IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA

v. **Criminal Case No. 3:19cr130**

OKELLO T. CHATRIE,

Defendant.

MEMORANDUM OPINION

I. Introduction

Ratified in 1791, the Fourth Amendment to the United States Constitution guarantees to the people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To that end, the Framers prohibited the issuance of a warrant, unless that warrant was based "upon probable cause" and unless it "particularly describ[ed] the place to be searched, and the persons or things to be seized." *Id.* The Supreme Court of the United States has since applied the principles embodied in this language to constantly evolving technology—from recording devices in public telephone booths, *Katz v. United States*, 389 U.S. 347 (1967); to thermal-imaging equipment, *Kyllo v. United States*, 533 U.S. 27 (2001); and, most recently, to cell-site location data, *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

This case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods. In recent years, technology giant Google (and others) have begun collecting detailed swaths of location data from their users. Law enforcement has seized upon the opportunity presented by this informational stockpile, crafting "geofence" warrants that seek location data for every user

within a particular area over a particular span of time. In the coming years, further case law will refine precisely whether and to what extent geofence warrants are permissible under the Fourth Amendment. In the instant case, although the Motion to Suppress must ultimately be denied, the Court concludes that this particular geofence warrant plainly violates the rights enshrined in that Amendment.

II. Findings of Fact and Procedural History

A. Findings of Fact[1]

1. The Robbery at the Call Federal Credit Union

On May 20, 2019, at approximately 4:52 p.m., a bank robbery occurred at the Call Federal Credit Union (the "Bank") in Midlothian, Virginia. The suspect held a firearm over the course of the robbery and took $195,000 from the Bank.

During the robbery, the suspect presented a teller working at the Bank a handwritten note that stated:

> I've been watching you for sometime [sic] now. I got your family as hostage and I know where you live, [i]f you or your coworker alert the cops or anyone your family and you are going to be hurt. I got my boys on the lookout out side [sic]. The first cop car they see am going to start hurting everyone in sight, hand over all the cash, I need at least 100k and nobody will get hurt and your family will be set free. Think smartly everyone['s] safety is depending and you and your coworker[']s action so I hope they don't try nothing stupid.

[1] A "presumption of validity" exists "with respect to the affidavit supporting the search warrant." *Franks v. Delaware*, 438 U.S. 154, 171 (1978). Because Chatrie does not allege that the statements in the affidavits supporting the search warrants are untrue statements, but instead says that these statements do not provide enough information or that they do not contain the proper information to support the search warrants, the Court in part makes its findings of fact based on the statements made in the affidavits. *Id.* (describing the circumstances in which the Court must hold an evidentiary hearing on a defendant's motion to suppress).

(ECF No. 54-1, at 6.)[2] The teller told the suspect that she did not have access to that amount of money, and the suspect then displayed a silver and black firearm. While openly holding the gun, the suspect directed the teller, other Bank employees, and the Bank customers to move to the center of the lobby and get on the floor. The suspect then led these individuals behind the teller counter to an area that contained the Bank's safe. Once behind the counter, the suspect forced the Bank's manager to open the safe and place $195,000 into a bag he brought with him. After acquiring the money, the suspect left the Bank on foot, "towards an adjacent business, west of the [B]ank." (ECF No. 54-1, at 6.)

During its investigation, law enforcement obtained the instant Geofence Warrant (hereinafter "Geofence Warrant" or "Warrant")—a novel application of search technology whose use has grown exponentially in recent years. Google produced certain location information pursuant to the Warrant, which led the police to Okello Chatrie. Chatrie was eventually charged with two crimes related to the robbery.[3] He then filed a Motion to Suppress the Geofence Warrant that forms the basis of this Opinion.

---

[2] The Court employs the pagination assigned by the CM/ECF docketing system for citations to the parties' submissions. Where a document was not filed through CM/ECF (for example, an exhibit introduced at a hearing), the Court will cite to the pages that would have been assigned through CM/ECF had they been filed through the system.

In addition, the Court acknowledges that its findings of fact differ between this Memorandum Opinion and a later issued Memorandum Opinion addressing the validity of four other warrants. In that Opinion, the warrants set forth a lengthier, more detailed narrative explaining the officers' investigatory steps than the instant Geofence Warrant. In determining the validity of a warrant, the "magistrate [or magistrate judge], and a reviewing court, will restrict their inquiries on probable cause to the facts set forth in the four corners of the officers' sworn affidavit." *United States v. Lipscomb*, 368 F. Supp. 3d 680, 684 (E.D. Va. 2019). Thus, because the facts in the Geofence Warrant differ from those set out in the four other warrants, the Court's findings of fact accordingly differ as well.

[3] More precisely, (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A).

2. The Record Presented to the Court by the Parties

There is a relative dearth of case law addressing geofence warrants.[4] In this case, the parties, especially the defense, pursued a thorough and deep record. This Court was aided by Amicus Google's provision of detailed information, including in-person testimony regarding the company's acquisition, retention, and use of users' location data. In what may be a first, Google filed an Amicus Brief.[5] Mr. Marlo McGriff, a Location History Manager at Google since 2016, submitted three declarations over the course of this matter. Ms. Sarah Rodriguez, a Team Lead for Legal Investigations Specialists ("LIS")[6] at Google since 2018, provided one declaration. During a hearing on March 4–5, 2021, (one of many in this case), the Court heard live testimony from both Mr. McGriff and Ms. Rodriguez.[7]

---

[4] Specifically, this Court has identified only five other federal opinions on the subject, but all assessed the validity of the warrants *before* they were issued: *In re Search of Information That is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021); *In re Search of Information that is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153 (D. Kan. 2021); *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); and, *In re Search of Information Stored at Premises Controlled by Google*, No. 20M297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

[5] Among other things, Google argued in its brief that Location History is not a business record, but is a journal stored primarily for the user's benefit and is controlled by the user. Google states that LH information "can often reveal a user's location and movements with a much higher degree of precision than [Cell Site Location Information]." (ECF No. 59-1, at 8.) Google argues that a geofence is certainly a "'search' within the meaning of the Fourth Amendment," because "[u]sers have a reasonable expectation of privacy in the LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail." (ECF No. 59-1, at 9.)

[6] Legal Investigations Specialists are the Google employees who receive warrants and send the returns.

[7] This testimony was delayed at the request of defense counsel during an extensive period of time because the COVID pandemic prevented live testimony.

The parties to this case also brought their own experts. Spencer McInvaille, an expert in digital forensic examinations, forensics, and cellular location testified for the defense, and FBI Special Agent Jeremy D'Errico, a part of the cellular analysis survey team ("CAST") spoke for the Government. Multiple rounds of briefing occurred before, during, and after the hearings held by the Court.

In order to establish as thorough a record as possible with respect to this new technology, the Court will first discuss Google's location services, as well as Google's typical response to geofence warrants.[8]

3. Google's Collection and Production of Location Data

a. Google's Suite of Location Services

Google collects detailed location data on "numerous tens of millions" of its users. (ECF No. 96-1, at ¶ 13; ECF No. 201, at 205.) It acquires and stores this data through one of at least three services: (1) Location History, (2) Web and App Activity ("WAA"), and (3) Google Location Accuracy ("GLA"). Google only searches Location History when it receives a geofence warrant.

i. Location History

Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data. Google developed Location History to allow users to view their Location History data through its "Timeline" feature, a depiction of a user's collected Location History points over time. (ECF No. 96-1, at ¶ 5; *see* ECF No. 202, at 79.) According to Google, this permits Google account holders to

[8] Other companies such as Amazon and Apple invariably retain users' location data as well. But Google, whose services function across Apple *and* Android devices (as opposed to Apple Maps for example, which functions only on iPhones), seems to be subject to more geofence requests than other companies.

"choose to keep track of locations they have visited while in possession" of their mobile device. (ECF No. 96-1, at ¶ 4.) Importantly, Location History also supports Google's advertising revenue.[9] For instance, McGriff testified that Location History data serves Google's advertising business by providing "store visit conversions" or "ads measurement" to businesses based on user location. (ECF 201, at 196–97.) Without identifying any individual user, this "store conversion" data can follow a particular ad campaign and identify "how many users who saw a particular ad campaign actually went to one of those stores." (ECF No. 201, at 197.) Google's "radius targeting" also allows—again without identifying any user—"a business to target ads to users that are within a certain distance of that business." (ECF No. 201, at 198.)

Location History is powerful: it has the potential to draw from Global Positioning System ("GPS") information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol ("IP") address information, and the signal strength of nearby Wi-Fi networks. According to Agent D'Errico, Location History logs a device's location, on average, every two minutes.[10] Indeed, Location History even allows Google to "estimat[e] . . . where a device is in terms of elevation." (ECF No. 202, at 95.) McGriff testified that this capability helps locate someone in an emergency, or try to "determine if you are on the second [or first] floor of the mall" if the Google Maps directory has launched to help a user navigate indoors. (ECF No. 202, at 95–96.)

---

[9] Using 10K filings from Google's parent company Alphabet, FBI Agent D'Errico noted that Google's advertising revenue constituted 85.4% and 83.9% of its *entire* revenue in 2018 and 2019, respectively.

[10] Defense Expert McInvaille evaluated a sample set of data and found that, for that data, Location History logged a device's location every six minutes. Under McInvaille's estimate, a user's movement is logged 240 times a day. D'Errico's estimate would raise that to 720 times a day. And Google Expert McGriff confirmed that Location History can track a user "hundreds" of times a day. (ECF No. 202, at 159.)

Google stores this data in a repository known as the "Sensorvault" and associates each data point with a unique user account. (ECF No. 201, at 130.) The Sensorvault contains a substantial amount of information. McGriff testified that the Sensorvault assigns each device a unique device ID—as opposed to a personally identifiable Google ID—and receives and stores *all* location history data in the Sensorvault to be used in ads marketing. Google then builds aggregate models within the Sensorvault with data that is transformed so that it no longer looks like user data, and then uses the data to, for instance, assist decision-making in Google Maps. As another example, Google uses this data to depict whether certain locations are busy during particular hours. Both McGriff and Rodriguez declared that, to identify users within the relevant timeframe of a geofence, Google has to compare *all* the data in the Sensorvault in order to identify users within the relevant timeframe of a geofence. (ECF No. 96-1, at ¶ 23 ("Google must search across *all* [Location History] data," and "run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant."); ECF No. 96-2, at ¶ 7 ("Google must conduct the search across *all* [Location History] data.").) Clearly, however, Google can alter the data back to identify users in response to a geofence warrant.

Still, Location history is off by default. A user can initiate, or opt into, Location History either at the "Settings" Level, or when installing applications such as Google Assistant, Google Maps, or Google Photos. Although the specific software pathway each user sees at any given moment can differ based on numerous factors, McGriff acknowledged that it was "possible that a user would have seen the option" to opt into Location History multiple times across multiple apps. (ECF No. 202, at 77–78.) For instance, Google may prompt the user to enable Location

History first in Google Maps, then again when he or she opens Google Photos and Google Assistant for the first time.[11]

Once a user opts into Location History, Google is "always collecting" data and storing *all* of that data in its vast Sensorvault, even "if the person is not doing anything at all with [his or her] phone." (ECF No. 201, at 114–15; *see* ECF No. 201, at 115 ("Once enabled, [Google is] now collecting [the user's] location history all the time.").) Even if a user enables Location History through an application and later deletes that app, Location History will "still collect[]" data on the user because Location History is tied to an individual's Google *account*, not to a *specific app*. (ECF No. 201, at 123–24.) Thus, after a user opts into the service, Location History tracks a user's location across every *app* and every *device* associated with the user's account. Approximately one-third of all active Google users have Location History enabled on their accounts.

In certain circumstances, Google can estimate a device's location down to three meters. Location History cannot, however, pinpoint an individual's location with absolute precision. Instead, Google *estimates* a phone's coordinates. When Google, through Location History, reports a device's estimated location by placing a point on a map, it also depicts around that point a "confidence interval"—a circle of varying sizes—which indicates Google's confidence in its estimation. (ECF No. 201, at 38, 212; ECF No. 202, at 253–54.) The smaller the circle around a phone's estimated location, the more confident Google is in that phone's exact location, and *vice versa*. In general, "Google aims to accurately capture roughly 68 percent of users"

[11] In a highly critical 2018 evaluation of tracking through Location History and Web & App Activity, the Norwegian Consumer Council (funded by the Norwegian government) characterized this as one of an identifiable set of problematic practices, dubbing it "repeated nudging" to encourage a user to enable the app. (Mar. 4–5 Hr'g Def. Ex. 27, at 28.)

within its confidence intervals. (ECF No. 201, at 213.) "[I]n other words, there[is] a 68 percent likelihood that a user is somewhere inside" the confidence interval. (ECF No. 201, at 213.)

ii. Web and App Activity

Web and App Activity collects a wider variety of information than Location History. If a user opts into WAA and has authorized all other requisite device permissions, WAA collects certain data points when a user *affirmatively engages* in certain activities.[12] For example, when a user performs a Google search, Google may, through WAA, keep a record of that search so that it can "automatically suggest[]" that search to the user at a later time. (ECF No. 96-1, at ¶ 16.) Google maintains that WAA allows a user to "experience faster searches and more helpful app and content recommendations." (ECF No. 96-1, at ¶ 16.) "Some of [the data obtained through WAA] can include location information, although the source of the location information will vary depending on the activity, the device, and the user's other settings." (ECF No. 96-1, at ¶ 16.) Location History "and WAA are separate services that store data in separate databases." (ECF No. 96-1, at ¶ 16.) That is, "WAA data is not used to calculate the locations that are stored in [Location History], and completing a search across [Location History] data does not search or draw on WAA data in any way." (ECF No. 96-1, at ¶ 16.)

iii. Google Location Accuracy

Lastly, Google Location Accuracy—only available on Android devices[13]—allows a user's phone to draw in location data from sources other than GPS information. "If a user has the GLA setting on, the Android[device's] location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors[] to estimate the device's location." (ECF

[12] This stands in contrast to Location History, which constantly and *passively* logs a user's location.

[13] At the time of the robbery, Chatrie used an Android device.

No. 96-1, at ¶ 17.) Thus, "the device 's location information that is sent to and stored in [Location History] . . . may be calculated using not only GPS-sourced data, but also [more detailed] WiFi- or cell-sourced data from the GLA database." (ECF No. 96-1, at ¶ 17.) "In other words, GLA data might be used by the device to calculate a [more precise] location data point that is then stored in [Location History]." (ECF No. 96-1, at ¶ 17.) Like WAA, Google generally stores GLA data separate from Location History information.

Again, as a general matter, Google appears to draw only from Location History to produce records for geofence requests, as WAA and GLA do not collect enough data points to pinpoint "devices within a certain period of time within a certain radius." (ECF No. 202, at 138; *see* ECF No. 201, at 211; ECF No. 96-1, at ¶¶ 20–22.) In keeping with this principle, here, Google only produced to law enforcement information from its Location History database.

b. Enabling Location History

The Court reports its understanding of the software pathways necessary to enable Location History based on two sets of sources. All sources agree that Chatrie enabled his Location History on July 9, 2018. However, even with input from two knowledgeable witnesses, the record as to how users can and do—and how Chatrie in particular could and did—enable Location History is not definitive on this record.

First, Defense Expert Spencer McInvaille testified in Court using a video of a device employing what was likely the same software used by Chatrie's phone to demonstrate how one might activate Location History through the Google account setup or through an app such as Google Maps. (Jan. 21 Hr'g Def. Ex. 4 ("Opt-In Video").) McInvaille also offered a written report explaining how Chatrie may have enabled location history. In that report, McInvaille

reported that Chatrie most likely enabled LH using Google Assistant, and that it was enabled on July 9, 2018.

Second, Google Location History Product Manager Marlo McGriff filed three declarations that explain how Google collects, stores, and turns over Location History data. He also testified in person during the March 4–5 Suppression Hearing. In his second declaration, McGriff concedes that McInvaille's video exhibit depicts largely accurate pathways to enable Location History. But McGriff states that McInvaille's video is incomplete. McGriff notes that "[b]y 2017 at the latest, it was not possible for a user to unable [Location History] solely by tapping on 'YES, I'M IN' as depicted on the final screen in the McInvaille Video." (ECF No. 110-1, at ¶ 7.) Instead, "a user who tapped on 'YES, I'M IN' . . . would be presented with a second opt-in screen" described above. (ECF No. 110-1, at ¶ 7.) McGriff presents the Court with the exact text of the second opt-in screen in his Third Declaration.[14] (ECF No. 147, at ¶¶ 7–8; *see* ECF No. 147, at ¶ 10 ("The text quoted in ¶¶ 7–8 is the same text that [Chatrie] would have seen on July 9, 2018.").

No expert could say *exactly* which software pathway Chatrie would have seen when he enabled Location History, nor could Google determine which app he used to turn the service on. Google does, however, accept that Chatrie would have seen the informational text in Part II.A.3.b.ii ("Through an App") in *some* form.

i. Through Phone Setup

As mentioned, a user must affirmatively enable Location History before Google uses the service to log the user's whereabouts. Google first allows users to enable Location History

[14] McGriff complicated this seemingly straightforward proposition by acknowledging that any "device that has been sitting on a shelf for three years [would use start up language] dated to when it was baked into the device." (ECF No. 202, at 18.)

during the initial Google account setup process. After a new user connects the phone to the internet, agrees to the phone manufacturer's terms and conditions, and inputs the necessary information to create a Google account, the interface displays Google's terms of service. (*See* ECF No. 110-1, at ¶ 5 (acknowledging that the Opt-In Video exhibit was accurate but incomplete).) To move past this screen, the user must scroll through a summary of Google's privacy terms until the user reaches the bottom of the page. This page "does [not] . . . say anything about [L]ocation [H]istory." (ECF No. 81, at 51.) Near the bottom, the screen displays blue text that reads, "MORE OPTIONS," with a downward-facing arrow next to the text. (Opt-In Video 3:00.) If the user taps on "MORE OPTIONS," the interface displays additional information about Google's location services. (ECF No. 81, at 51.) This additional information informs the user that WAA and GLA are enabled by default. Although Location History is *not* enabled by default, the user can opt into it from this screen by checking a box.

ii. Through an App

If a user does not enable Location History while setting up his or her Google account, Google will also prompt the user to turn the service on as soon as he or she sets up an app "that has [Location History]-powered features." (ECF No. 110-1, at ¶ 5; *accord* ECF No. 96-1, at ¶¶ 3–6; ECF No. 201, at 221; ECF No. 202, at 8–9.) Such apps include Google Maps, Google Photos, and Google Assistant. When a user opens one of these apps for the first time, the phone immediately directs the user to a bright blue screen that reads: "Get the most from Google Maps." (Opt-In Video 4:36.) This screen informs the user that "Google needs to periodically store [his or her] location to improve route recommendations, search suggestions, and more." (Opt-In Video 4:36.) Below that, the interface offers the user the option to "LEARN MORE." (Opt-In Video 4:36.) If the user taps "LEARN MORE," the page redirects to "[a]ll of [Google's]

terms and conditions"—but these terms and conditions include no information specifically tailored to location information. (ECF No. 81, at 57.)

Back at the initial blue page, the user can either select "YES, I'M IN" or "SKIP." (Opt-In Video 4:36.) As of July 2018, once the user selects "YES, I'M IN," the interface redirects the user to another page that displays the following text:

> **Location History**
>
> Saves where you go with your devices ∨ [15]
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

(ECF No. 147, at ¶ 7 (bold in original).) Next to "Location History: Saves where you go with your devices," the interface includes an "expansion arrow," depicted in the above text with a downward-facing caret. (ECF No. 147, at ¶ 8.) If a user "tap[s] on [this] expansion arrow," the interface "present[s the user] with additional information about" Location History. (ECF No. 147, at ¶ 8.) The screen then reads:

[15] Although the testimony is unclear on the matter, prior to 2018, this line appears to have read: "[C]reates a private map of where you go with your signed in devices." (ECF No. 201, at 266.) Google changed this language in response to European regulation.

Location History

Saves where you go with your devices

Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.

If you use your device without an internet connection, your data may be saved to your account once you return online.

Not all Google services save this data to your account.

This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.

This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.

NO THANKS TURN ON

(ECF No. 147, at ¶ 8 (bold in original).) If the user selects "TURN ON"—either in the original screen or this expanded version—Location History is enabled. (ECF No. 147, at ¶ 9.) Importantly, a user need not interface with or employ the expansion arrow to enable Location History. In other words, a user could activate the service without knowing any of the further details of the service as explained in the above expanded version.

As noted, Chatrie enabled Location History on his device on July 9, 2018 at 12:09 a.m. Eastern Standard Time, and he appears to have done so through Google Assistant.

c. "Pausing" and Trying to Delete Location History

After a user opts in, he or she has two mechanisms to manage Google's collection and retention of his or her Location History data: "pausing" the service, or deleting the information it collected.

i. Pausing

As Google Location History Product Manager Marlo McGriff explained, when a user "*pauses*" his or her Location History, it merely "halts the collection of future data;" *it does not delete* information Google has already obtained. (ECF No. 202, at 84.) And deleting an app through which the user enabled Location History will not pause the service.

A user may pause Location History on an Android device in one of three locations. First, the user can pause it "through the settings on any particular app that uses Location History." (ECF No. 202, at 63.) Second, he or she can pause it by navigating "through the device level settings." (ECF No. 202, at 63.) Finally, the user can log into myactivity.google.com and change his or her location settings. For each of these options, "a user [must] actively, intentionally navigate" through each interface. (ECF No. 202, at 64.)

When a user attempts to pause Location History, the device will present a pop-up screen containing text called the "pause copy." (Mar. 4–5 Hr'g Def. Ex. 27, at 23.) The pause copy warns users that pausing Location History will "limit[] functionality of some Google products over time, such as Google Maps and Google Now." (Mar. 4–5 Hr'g Def. Ex. 27, at 23; *accord* ECF No. 202, at 66.) Yet the record suggests that apps such as Google Assistant *will* continue to function with Location History paused. For instance, McInvaille noted that, despite prompts from Google to initiate Location History because apps like Google Assistant "depen[d] on these

settings in order to work correctly," the user does not "need Location History for [Google Assistant] to work." (ECF. No. 201, at 111, 113.)

The pause copy also does not specifically detail how app functionality might be limited. Nor does Google inform users of the fact that the app will, indeed, continue to function without Location History enabled, either when setting up the application or when displaying the pause copy. McGriff confirmed that when a user "pauses" the service, it halts only the collection of future data, and it does not (if a user has opted in) pause other location services such as Web & App Activity. (ECF No. 202, at 84, 90.)

ii. Trying to Delete

In 2018, when Chatrie enabled his Location History, a user had only one option to *delete* his or her Location History: by visiting myactivity.google.com and viewing his or her Timeline. Through the Timeline, a user "can review, edit, or delete [his or] her [Location History data] at will." (ECF No. 96-1, at ¶ 15.) But in response to an article from the Associated Press criticizing Google's acquisition of location data, one Google employee apparently remarked through an email: "The current [User Interface as of August 13, 2018] *feels* like it is designed to make things *possible*, yet *difficult* enough that people won't figure . . . out" how to turn Location History off.[16] (Mar. 4–5 Hr'g Def. Ex. 30, at 6 (emphasis added).) Whether the substance of this remark is true or not, the sentiment it expresses is certainly not inconsistent with the record before the Court.

[16] On May 11, 2018, two Senators launched an investigation into Google's acquisition of location data. During the March 4–5 Suppression Hearing, Chatrie tried to suggest that this investigation—in conjunction with a critical article from news website Quartz—*caused* Google to issue an update to its privacy policy on May 25, 2018. Google's expert McGriff testified credibly, however, that the investigation and policy changes were unrelated, because "there[was] no way Google updated its privacy policy in two weeks." (ECF No. 201, at 259.)

The effort to clarify this interface obviously is ongoing at Google.[17] In May 2019, McGriff formally heralded the "autodelete" controls that made it easier for users to manage their data. (*See* Mar. 4–5 Hr'g Def. Ex. 46.) And in December of 2019, McGriff introduced, on behalf of Google, "Incognito mode" and "Bulk delete in Timeline." (*See* Mar. 4–5 Hr'g Def. Ex. 47.)

d. Google's Process in Answering a Geofence Warrant

Geofence warrants represent "a novel but rapidly growing [investigatory] technique." (ECF No. 59-1, at 8.) When law enforcement seeks a geofence warrant from Google, it (1) identifies a geographic area (also known as the "geofence," often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time. (*See* ECF No. 96-2, at ¶ 4.) The requested time windows for these warrants "might span a few minutes or a few hours." (ECF No. 96-2, at ¶ 4.)

In recent years, the number of geofence warrants received by Google has increased exponentially. Google received its first in 2016. After that, Google "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the

---

[17] Since 2018, Google has added another feature to increase user control over Location History data. It now allows a user to set an "auto delete function" that limits how long Location History information remains with Google. (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) The auto delete function now enables a user to "[c]hoose a time limit" for how long he or she wants Google to save activity data and "any data older than that will be automatically deleted from [the] account on an ongoing basis." (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) McGriff testified that Google has also now developed a practice whereby Google sends monthly or annual emails about how to change settings. Google has no record that these emails were ever sent to Chatrie.

Still, concern about the user interface seemed to persist over time. Chatrie presented what purported to be emails from Google employees (garnered for other litigation) noting the confusing nature of various location products. One, in April 2019, reads: "Speaking as a user, WTF? More specifically I **thought** I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google-[software engineer]. That's not good." (Mar. 4–5 Hr'g Def. Ex. 37, at 5). The Norwegian report called this phenomenon "[d]eceptive click-flow." (Mar. 4–5 Hr'g Def. Ex. 27, at 27).

rate . . . increased over 500% from 2018 to 2019." (ECF No. 59-1, at 8.) In 2019, Google received "around 9,000 total geofence requests."[18] And Google now reports that geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States. Google, *Supplemental Information on Geofence Warrants in the United States* (last visited Mar. 1, 2022), https://bit.ly/3o7Znqc.

Google began to take issue with certain early geofence warrants because the requests were too broad. As related by Legal Investigations Specialist Rodriguez, the warrants "sought [Location History] data that would identify *all* Google users who were in a geographical area in a given time frame." (ECF No. 96-2, at ¶ 5 (emphasis added).) Thus, in 2018, Google held both internal discussions with its counsel and external discussions with law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice ("CCIPS"), to develop internal procedures on how to respond to geofence warrants. "To ensure privacy protections for Google users, . . . Google instituted a policy of objecting to any warrant that failed to include de[-]identification and narrowing measures." (ECF No. 96-2, at ¶ 5.) Seemingly developed as a result of Google's collaboration with CCIPS, this de-identification and narrowing "protocol typically . . . entails a three-step process." (ECF No. 96-2, at ¶ 5; *see* ECF No. 202, at 553.) As noted earlier, the Court draws its understanding of this process from an amalgam of in-person testimony and a declaration submitted by current Google Tooling and Programs Lead and former Legal Specialist Sarah Rodriguez.

[18] To clarify, a geofence *request* is not identical to a geofence *warrant*. "[I]n some cases, law enforcement is[not] aware that [it] need[s] to submit a warrant" to obtain Location History. (ECF No. 202, at 173.) Google still considers this communication from law enforcement a "geofence request," even when not accompanied by a warrant. (ECF No. 202, at 173.)

i. Step 1

First, at Step 1, law enforcement receives a warrant "compelling Google to disclose a *de-identified* list of all Google user[s]" whose Location History data indicates were within the geofence during a specified timeframe. (ECF No. 96-2, at ¶ 6 (emphasis added).) In response to the warrant, Google must "search . . . *all* [Location History] data to identify users" whose devices were present within the geofence during the defined timeframe. (ECF No. 96-2, at ¶ 7; ECF No. 96-1, at ¶ 23.) "Google does not know which users may have . . . saved [Location History] data before conducting th[is] search." (ECF No. 96-2, at ¶ 7.)

Rodriguez stated that, as part of this first step, Google provides the Government with responsive user records identified in the Sensorvault. Google deems a record "responsive" if a user's estimated location (*i.e.*, the stored coordinates of the phone in Location History) falls within the boundaries of the geofence. (ECF No. 96-1, at ¶ 25.) Rodriguez confirmed that, for every device whose "stored latitude/longitude coordinates fall within the radius described in the warrant," Google turns over a "'production version' of the [users'] data." (ECF No. 96-2, at ¶ 8.) This production version "includes a [de-identified] device number,[19] the latitude/longitude coordinates and timestamp of the stored [Location History] information, the map's [confidence

---

[19] When responding to geofence warrants, Google:

> de[-]identifies the data produced to the [G]overnment at this [first] step by removing the [user's distinct] Google Account ID . . . , leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting [Location History] to a user's account . . .

(ECF No. 96-2, at ¶ 9.) Unlike a Google Account ID, a Location History device number does not by itself identify which account is associated with certain location points. However, as discussed in Part II.A.6.b ("The Three Paths Video"), *infra*, piecing together an "anonymous" user's location data could reveal that user's identity.

interval], and the source of the stored [Location History]," (*i.e.*, "whether the location was generated via Wi-Fi, GPS, or a cell tower"). (ECF No. 96-2, at ¶ 8.)

According to Rodriguez, the sizes and timeframes of geofences "vary considerably from one request to another." (ECF No. 96-2, at ¶ 8.) Because Google produces *all* location points captured within the geofence over the timeframe, "[t]he volume of data produced at [Step 1] depends on the size and nature of the geographic area and length of time covered by the geofence request." (ECF No. 96-2, at ¶ 8.) Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data.

Indeed, Google places significant discretion on the LIS employee who initially reviews a particular geofence warrant. This "specialist" will first process and review the warrant. (ECF No. 202, at 178–79.) If the specialist believes the warrant "needs further review"—for example, if the geofence seems too large or the timeframe too long—he or she may first "engage with [the requesting] law enforcement officer to collect more information about the investigation." (ECF No. 202, at 179, 182.) From there, the specialist will "consult with [Google's] legal counsel." (ECF No. 202, at 179.) If Google's counsel objects to the warrant, Google may have a "conversation" with law enforcement to alleviate Google's concerns, or it may "require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue." (ECF No. 202, at 187.) Assuming law enforcement eventually assuages Google's concerns with the warrant, Google then provides the Government with the de-identified geofence data.

ii. Step 2

Second, according to Rodriguez, at Step 2, the Government "reviews the de[-]identified [data] to determine the [Sensorvault] device numbers of interest." (ECF No. 96-1, at ¶ 10.) 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, at this step, "can compel Google to provide additional . . . location coordinates *beyond* the time and geographic scope of the original request."[20] (ECF No. 96-2, at ¶ 10 (emphasis added).) These additional location points "can assist law enforcement in eliminating devices" from the investigation that were, 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."[21] (ECF No. 96-2, at ¶ 11.) Notably, Google imposes "no geographical limits" on this Step 2 data. (ECF No. 202, at 184.) Thus, if a user's location fell within the geofence at Step 1, law enforcement can obtain *all* location points for identified users over an expanded timeframe at Step 2. This means that, at Step 2, no geographic barrier confines the information searched.

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 not simply seek geographically unrestricted data for *all* users within the geofence. Google has no firm policy as to precisely *when* a Step 2 request is sufficiently narrow. But if law enforcement requests "a lower number of devices from St[ep] 1 to St[ep] 2," this, to some extent, demonstrates to Google that law enforcement has tailored the data it seeks. (ECF No. 202, at 190.) Again, assuming Google has no further objections to law enforcement's Step 2 request, Google provides law enforcement with de-identified but geographically unrestricted data.

---

[20] At Step 2, for law enforcement to expand the timeframe from which to obtain Location History data, Google generally requires that the warrant explicitly expand that timeframe *in the warrant's text*. Otherwise, Google will object to that request.

[21] If law enforcement requests this additional data, it must typically do so within sixty days.

iii. Step 3

Finally, at Step 3, drawing from the de-identified data Google has produced so far, "the [G]overnment can compel Google . . . to provide *account-identifying information*" for the users "the [G]overnment determines are relevant to the investigation." (ECF No. 96-2, at ¶ 12 (emphasis added).)[22] This "account-identifying information" includes the name and email address associated with the account. (ECF No. 96-2, at ¶ 12; ECF No. 202, at 192.) Google seems to prefer that law enforcement request Step 3 data on fewer users than requested in Step 2, although it is "[p]ossibl[e]" that Google would approve a Step 3 request that is not narrowed after Step 2 at all. (ECF No. 202, at 194.)

4. The Instant Geofence Warrant and Its Justifications

a. Det. Hylton's Investigation[23]

When Det. Hylton responded to the scene of the bank robbery on May 20, 2019, he "interviewed witnesses" and "reviewed surveillance camera video from . . . the Call Federal Credit Union Bank." (ECF No. 202, at 330.) Through this initial investigation, he "learned that [the] suspect had come from the southwestern corner of the Journey Christian Church [the 'Church'], . . . a building adjacent and to the east of the Call Federal Credit Union, at approximately 4:50 in the afternoon." (ECF No. 202, at 330–31.) He also learned of the core

[22] Law enforcement has sixty days from the time Google turns over Step 2 data to request Step 3 information.

[23] Although the subsequent warrants evaluated in a separate Opinion, explain officers' investigatory efforts to identify a suspect beyond reviewing security camera footage, the Geofence Warrant contains no information about those efforts. Because the Geofence Warrant does not expressly incorporate these subsequent warrants—and indeed, it could not have because officers obtained them after drafting the Geofence Warrant—the Court will consider only the following facts in its analysis. *See United States v. Hurwitz*, 459 F.3d 463, 470 (4th Cir. 2006) (requiring that a warrant either incorporate a supporting document by reference or attach the document to warrant itself in order for a court to read the document alongside the warrant).

facts that underlie this case—that the suspect walked into the Bank wearing a fisherman's hat and traffic vest, presented the teller with a note demanding $100,000, forced the manager at gunpoint to open the Bank's vault, took $195,000, and may have left in a blue Buick Lacrosse. Critically, through security footage, Det. Hylton observed that when the suspect first walked into Bank, he was "holding what appeared to be . . . a cell phone to the side of his face." (ECF No. 202, at 331.) To Det. Hylton, this use of a phone suggested "that [the suspect] could have possibly been speaking with a coconspirator." (ECF No. 202, at 333.)

After Det. Hylton completed his on-site investigation, he pursued at least two other leads. First, a purportedly estranged romantic partner called the police and told them that she "kn[e]w who did th[e] robbery," and that the suspect was her "ex-boyfriend." (ECF No. 202, at 334.) Law enforcement found this ex-boyfriend, interviewed him, examined his cell phone, and ultimately determined that he was not the suspect. Next, an employee at another branch of the Bank alerted the police about an individual who drove a blue Buick Lacrosse and wore a traffic vest. Det. Hylton ultimately determined that this individual was likewise not the suspect.

Having unearthed no further leads from his investigation, Det. Hylton then turned to geofence technology. He had sought three other geofence warrants in the past. Before seeking those warrants, he had consulted with prosecutors, who approved them. Magistrates—including one federal magistrate judge—approved all three as well. Those warrants were, according to Det. Hylton, "mostly similar" to the one at bar. (ECF No. 202, at 328; *compare* Mar. 4–5 Hr'g Def. Ex. 18 ("Prior Federal Geofence Warrant") *and* Mar. 4–5 Hr'g Def. Ex. 19 ("Prior State Geofence Warrant") *with* ECF No. 54-1.) Indeed, all but one adopted a roughly 150-meter radius, although a "few of them had more locations because [there were] more robberies to

investigate." (ECF No. 202, at 328; *see* Prior Federal Geofence Warrant; Prior State Geofence Warrant.)

On June 14, 2019, roughly three weeks after the robbery, Det. Hylton applied for and obtained the instant Geofence Warrant from Chesterfield County Magistrate David Bishop.

b. Magistrate Bishop

Chatrie contests the sufficiency of Magistrate Bishop's qualifications. Although the Court will address that issue more fully later in this Opinion, the Court briefly notes that Chesterfield County Magistrate "David Bishop graduated from Pensacola Christian College with a Bachelor's of Science in Criminal Justice in May 2016."[24] (ECF No. 156, at 1.) Around two years later, on June 12, 2018, the Executive Secretary of the Supreme Court of Virginia appointed Bishop as a magistrate. Magistrate Bishop completed his statutorily required probationary period on March 12, 2019. He was released for service on October 24, 2018.

Three months after Magistrate Bishop finished his probationary period, Det. Hylton presented Magistrate Bishop with the instant Geofence Warrant. When Magistrate Bishop reviewed the Warrant, he asked no questions of Det. Hylton, nor did he "seek to modify anything in the affidavit." (ECF No. 202, at 362.) Based on Det. Hylton's understanding, Magistrate Bishop simply "read [the Warrant] and signed it."[25] (ECF No. 202, at 362.) The record suggests that this was the first geofence warrant Magistrate Bishop had signed.

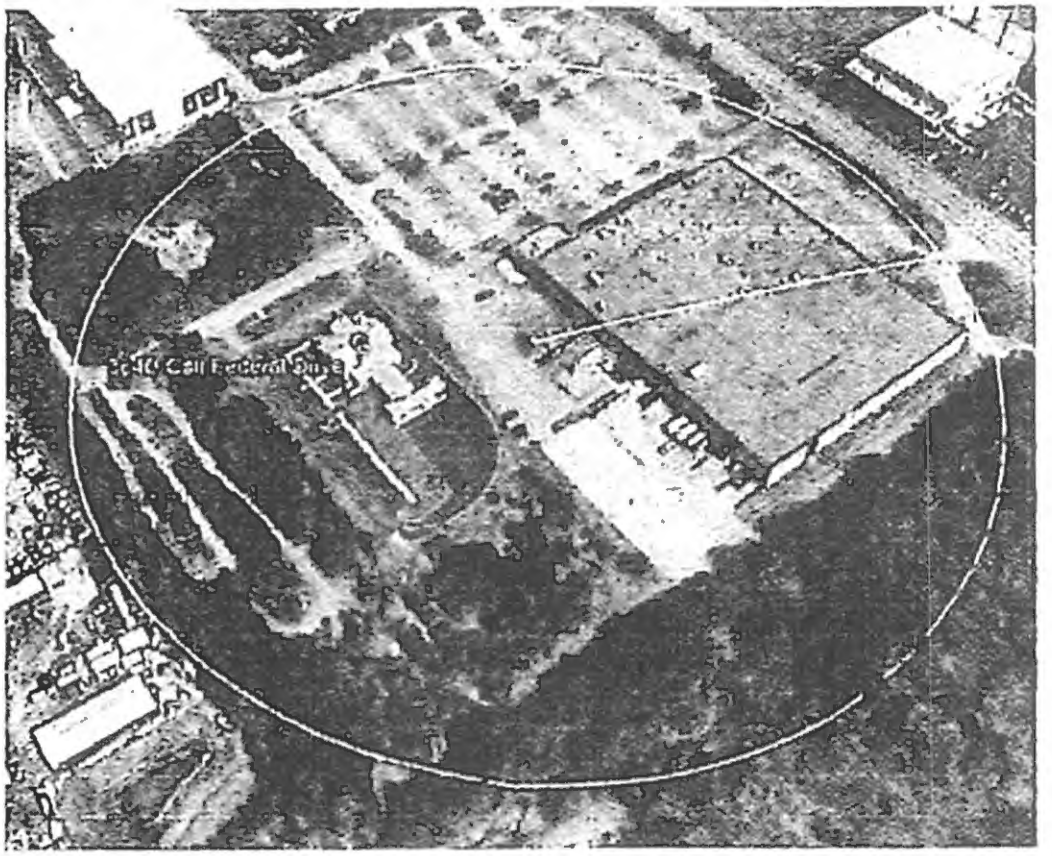
---

[24] The Virginia Code imposes one educational requirement on the Commonwealth's magistrates: they must possess a bachelor's degree "from an accredited institution of higher education." Va. Code § 19.2-37. The Code does not further define what qualifies as an "accredited institution" for the purpose of magistrates. Chatrie disputes whether Magistrate Bishop's alma mater, Pensacola Christian College, is sufficiently "accredited" under the Virginia Code. (ECF No. 135, at 6–9.) The Court will speak to this later in the Opinion.

[25] Det. Hylton did note, however, that because Magistrate Bishop did not read the Warrant in front of him, Magistrate Bishop "*could* have consulted with someone" about it. (ECF No. 202, at 362 (emphasis added).)

c. The Instant Geofence Warrant

The Warrant drew a geofence with a 150-meter radius—with a *diameter* of 300 meters, longer than three football fields—in an urban environment which included the Bank and the nearby Journey Christian Church.[26] All told, the geofence encompassed 17.5 acres. The eastern side of the geofence abutted but did not include Price Club Boulevard. The southern side encompassed a wooded area behind the Bank. The northern side encircled the Church's parking lot, and the western side captured a wooded area to the west of the Bank. The Warrant included the following photograph of the area with the geofence superimposed over it:



[26] Thus, the total area of the geofence is 70,686 square meters—about three and a half times the *footprint* of a New York city block. Michael Kolomatsky, *How Big Is an Acre, Anyway?* N.Y. Times (July 26, 2018), https://nyti.ms/345CjS7. Of course, this portion of suburban Richmond, Virginia does not have the density (or height) comparable to that of seven New York City blocks.

The Warrant sought location data for every device present within the geofence from 4:20 p.m. to 5:20 p.m. on the day of the robbery. In keeping with Google's established approach, the Geofence Warrant described a three-step process by which law enforcement would "attempt to narrow down" the list of users for which the Government would obtain the most invasive information. (ECF No. 54-1, at 4.)

At Step 1, "Google w[ould] provide 'anonymized information' regarding the Accounts that are associated with a device that was inside the described geographical area" from 4:20 p.m. to 5:20 p.m. (ECF No. 54-1, at 4.) At Step 2, "Law enforcement w[ould] return a list [of accounts] that they ha[d] attempted to narrow down." (ECF No. 54-1, at 4.) Google would then "produce contextual data points with points of travel outside of the geographical area." (ECF No. 54-1, at 4.) During Step 2, the warrant expanded the timeframe to include thirty minutes before and thirty minutes after the initial hour-long window, so that the Step 2 window was two hours long in total. (ECF No. 54-1, at 4.) Finally, at Step 3, after Government review, Google would "provide identifying account information/CSI[27] for the accounts requested" by law enforcement. (ECF No. 54-1, at 4–5.)

In explaining why "Google [should] provide Geo[f]encing data," Det. Hylton noted in the warrant's accompanying affidavit that:

---

[27] The warrant included in the definition of "identifying account information/CSI" the following:

> user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phones numbers associated with the account.

(ECF No. 54-1, at 4.)

> when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the [crime].

(ECF No. 54-1, at 6.) Specifically, he noted that when reviewing the Bank's surveillance footage, he observed that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) He further explained that:

> Google has . . . developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.
>
> Based on [his] training and experience, [he has learned] that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled.

ECF No. 54-1, at 7.) Therefore, he explained, "the requested data/information would have been captured by Google during the requested time." (ECF No. 54-1, at 6.) Det. Hylton noted several ways law enforcement could use this information. For example, "location data . . . may tend to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) In turn, this geographic and timeline information may tend to "inculpat[e] or exculpate[e] persons of interest." (ECF No. 54-1, at 7.)

Inexplicably, on June 19, 2019—*the day before he sent the Warrant to Google*—Det. Hylton submitted his return for the Warrant to the Chesterfield County Circuit Court. A search warrant return "notifies the Court when [an officer] *execute*[*s*] a search warrant," and the officer "report[s] back to the Court what items [he or she] gathered during the search." (ECF No. 202, at 366–68 (emphasis added).) In the return, he stated that he had executed the warrant on June 14, 2019. Yet he had not yet sent the Warrant to Google. Moreover, in describing the items

already seized under the Warrant—again, he had not yet executed it—Det. Hylton wrote for what would be a sizable amount of precise location information on at least nineteen device users: "Data." (Mar. 4–5 Hr'g Gov't Ex. 2, at 9; *see* ECF No. 202, at 367, 369); *see also United States v. Williams*, 592 F.3d 511, 520 (4th Cir. 2010) ("While the [Fourth Amendment's] protection cannot demand perfection, any tolerance of imperfection does not give officers free reign to ransack and take what they like." (citation and quotation marks omitted)).

5. Google Receives the Geofence Warrant

The next day, on June 20, 2019, Det. Hylton sent Google the Warrant that Magistrate Bishop had approved. Pursuant to Step 1, Google produced anonymized Location History data for all accounts associated with phones present within the geofence from 4:20 p.m. to 5:20 p.m.—nineteen users in total.[28] Associated with these nineteen users were 210 individual location points, along with the confidence interval for each point. In this case, law enforcement ran this information through a program to produce a visual representation of the data. *See* Part II.A.6.a, *infra*.

A few days after Google provided him the Step 1 information, Det. Hylton emailed Google. The record then strongly suggests that he did not "attempt to narrow down" the list of devices for which he requested further data. In contravention to Google's policy, and without consulting Magistrate Bishop, Det. Hylton requested "additional location data" (Step 2 data) *and* "subscriber information" (Step 3 data) "for *all* 19 device numbers produced in [S]tep 1." (ECF

[28] Google provides this information in a table, sorted into seven columns: "Device ID," "Date," "Time," "Latitude," "Longitude," "Source," and "Maps [Confidence Interval]." (*See, e.g.*, Mar. 4–5 Hr'g Def. Ex. 3, at 7.) Google LIS Rodriguez testified that the Device ID is not an identifier for "any other specific Google account." (ECF No. 202, at 176.) It is not cross-referenced by Google outside of Location History, but if an individual device were responsive to two different geofence warrants, the ID would be the same in both. Law enforcement does not return this information to Google nor, in this case, did it return the data to the Chesterfield County Court.

No. 48-1, at 1; *accord* ECF No. 96-2, at ¶ 15; ECF No. 202, at 195, 345.) He noted that, because "the sought Google devices [were] fairly low in number," he requested Step 2 and 3 data for *all* nineteen users "in an effort to rule out possible co-conspirators." (ECF No. 48-1, at 1; *see* ECF No. 202, at 195.) He admitted, however, that "device numbers 1–9 may fit the more likely profile of [the] parties involved." (ECF No. 48-1.) Six days after sending the email, Det. Hylton called Google and left two voicemails seeking a response.

A Google specialist then called Det. Hylton. As described by Rodriguez, the LIS "explained the issues" with Det. Hylton's request—namely, that the request "did not appear to follow the three sequential steps or the narrowing required by the search warrant." (ECF No. 96-2, at ¶ 16; *see* Mar. 4–5 Hr'g Tr. 189, 197.) "Det. Hylton asked . . . what information would be produced in [S]tep 2 and . . . [S]tep 3." (ECF No. 96-2, at ¶ 16.) The Google specialist explained the nature of the data to be turned over during these steps and emphasized to Det. Hylton "the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16; *see* ECF No. 202, at 197.) The specialist, however, does not appear to have provided Det. Hylton with any "specific directive[s] . . . about how much [Det. Hylton] had to narrow" his request. (ECF No. 202, at 197.) On July 9, 2019, Det. Hylton emailed Google, requesting Step 2 data on the *nine* users identified in his prior email. Google then provided him that information in the same format as Step 1 data had been returned. It does not appear that Det. Hylton explained to Google precisely why he requested Step 2 data for these nine particular accounts. Neither Det. Hylton nor Google consulted with a magistrate or judge before Google disclosed this data.

"On or about July 10, 2019, and July 11, 2019, Google received emails from [Det.] Hylton requesting [Step 3] information . . . on [three] device numbers." (ECF No. 96-2, at ¶ 19.) Google provided him with this information—"the account subscriber information associated with

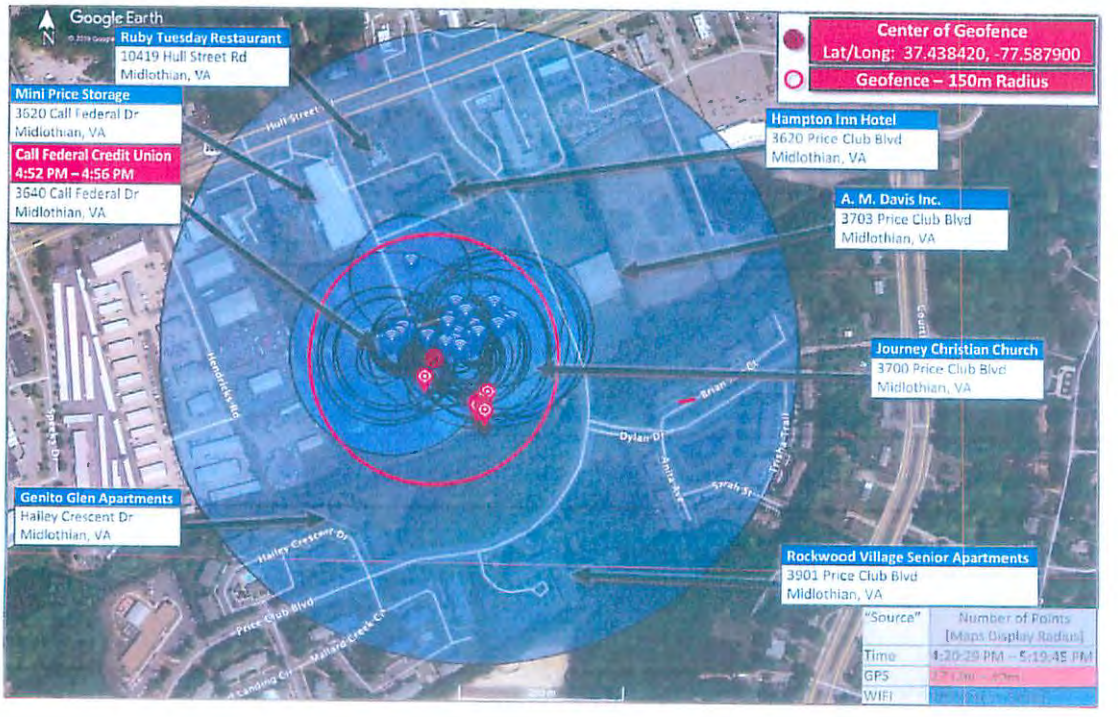
the 3 device numbers"—on July 11. (ECF No. 96-2, at ¶ 20.) Again, it is not apparent from the record whether Det. Hylton demonstrated to Google why he requested Step 3 data for these three accounts, nor did he seek the magistrate's approval before obtaining the data.

Finally, "[o]n or about July 12, 2019," Det. Hylton emailed Google "requesting *additional* device or phone number information that could be associated with one of the accounts" for which Google had produced Step 3 data. (ECF No. 96-2, at ¶ 21 (emphasis added).) This would have been an unauthorized Step 4. A Legal Investigations Specialist called Det. Hylton, that day and told him that "no further information was produced under" the Geofence Warrant. (ECF No. 96-2, at ¶ 21.)

6. Data Derived from the Warrant

a. Law Enforcement's Demonstrative

Upon receipt of the geofence data, law enforcement "imported [the Step 1 information] into mapping software" so that law enforcement could visualize the data points. (Mar. 4–5 Hr'g Gov. Ex. 1, at 15.) That program rendered the following depiction:



The visualization, created by Agent D'Errico, plots each point's confidence interval—the area in which Google is 68 percent confident a given individual is located—with a blue shaded circle.

Here, the largest confidence interval for a user located within the geofence had a radius of roughly 387 meters (longer than four football fields)—more than twice as large as the original geofence.[29] Thus, the Geofence Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence. Within this confidence interval—in addition to the Bank and the Church—are several buildings (with an unknown number of floors), including a Ruby Tuesday restaurant, a Hampton Inn Hotel, several units of the Genito Glen apartment complex, a self-storage business, a senior living facility, two busy streets (Hull Street and Price Club Boulevard), and what appear to be several residences near the southeast edge of the confidence interval. Near the time of the robbery, the individual whose account produced this large confidence interval could have been present at any of these locations instead of within the geofence.

Indeed, given that Google returns locations via these estimated location points, both McInvaille and D'Errico confirmed geofences can return both false positives (someone who is not in the geofence reported as being there) and false negatives (someone in the geofence not

[29] The Court acknowledges that as a matter of fact, it is unlikely that this user would have been located far outside the geofence. As FBI Agent D'Errico testified during the March 4–5 Suppression Hearing, this user first reported a location point within the geofence with a confidence interval of around 84 meters. The next location point, reported only thirty seconds later, was the point with the 387-meter confidence interval—but the user's reported location was in exactly the same spot as the prior point. It is thus unlikely that the user would have traveled from an area in or near the geofence to a location significantly outside of it within thirty seconds. FBI Agent D'Errico did note, however, that these location points were "indicative . . . that the device [was] moving," and that "for some reason, . . . a new center coordinate was not obtained by that phone." (ECF No. 202, at 255.) Nevertheless, the notion that geofences *can* capture information from users who are not even in the vicinity of the relevant area troubles the Court and evinces how broad a sweep these warrants may have.

reported). Chatrie created a video based on the returns of this geofence warrant suggesting that a false positive was returned here.

b. The Three Paths Video

Chatrie's video depicting the movement of three phones was based on the data obtained through the Warrant at Step 2. At the March 4–5 Suppression Hearing, Chatrie introduced a video that plotted the locations of three anonymous individuals whose location data Google turned over at Step 2— "Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63, 67; *see* Mar. 4–5 Hr'g Def. Ex. 5 ("Three Paths Video").)

At the beginning of the two-hour, geographically unlimited, window for which the Government requested Step 2 location data, a cluster of location points for Mr. Blue appeared at a nearby apartment complex. At 4:34 p.m., Mr. Blue seemed to leave the apartment complex, and at 4:35 p.m., Mr. Blue's location estimate appeared inside the geofence, roughly seventeen minutes before the robbery occurred. However, at 4:36 p.m.—twenty-seven seconds later—Mr. Blue appeared outside the geofence on Price Club Boulevard, and by 4:37 p.m., Mr. Blue appeared to be driving down Hull Street. Mr. Blue then drove south and stopped at another residence—clustering location data for five minutes—and eventually drove back toward the original apartment complex, where he remained for the rest of the two-hour window. Because Mr. Blue appeared within the geofence for such a brief period of time—and because he appeared within the fence just as he appeared to drive on a nearby street—Defense Expert McInvaille testified that Mr. Blue may have been a "false positive"—he may not have actually stepped foot within the geofence. (ECF No. 201, at 43–44, 65.)

Mr. Green's location points initially clustered at a hospital for a period of about thirty-five minutes. Eventually, Mr. Green drove south along Old Courthouse Road, ultimately

appearing inside the geofence at 4:41 p.m. Around two minutes later—and nine minutes before the robbery—Mr. Green's estimated location appeared in a residential neighborhood, clustering around one home for the remainder of the two-hour window.

Finally, Ms. Yellow clustered location points at a house from 3:51 p.m. to 4:11 p.m. At 4:18 p.m., she clustered several points near a school, and by 4:26 p.m., she appeared to drive toward the Bank. At 4:31 p.m., she first appeared in the geofence, her location estimate surfacing inside the Bank. She reported two more location points inside the Bank, and by 4:36—eighteen minutes before the robbery—appeared to be driving away from the Bank. She drove south, arrived at the house from which she started, and remained there for the rest of the two-hour window.

Defense Expert McInvaille testified that he was able to access publicly available information such as tax records related to the homes in which Mr. Blue, Mr. Green, and Ms. Yellow appeared to spend significant time. He explained that these records, in conjunction with other publicly available information such as social media accounts, would have allowed him to determine these individuals' likely identities with only a few data points. Law enforcement would, of course, have similar or enhanced research capabilities to identify users based on these "de-identified" location points.

* * *

Ultimately, the Step 3 information law enforcement obtained led the authorities to Chatrie.

B. Procedural History

On September 17, 2019, a grand jury indicted Chatrie on two counts: (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d),

and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A). The police issued a warrant, and a magistrate judge signed a Petition and Order for Writ of Habeas Corpus ad Prosequendum ordering that Chatrie, then an inmate at Riverside Regional Jail, appear in the United States District Court for the Eastern District of Virginia to answer for the charges.

On October 1, 2019, Chatrie appeared before the magistrate judge and waived his right to a detention hearing. The magistrate judge ordered Chatrie detained pending trial. On that same day, Chatrie appeared for an arraignment and pleaded not guilty to the charged offenses.

On October 29, 2019, Chatrie filed the instant Geofence Motion to Suppress. (ECF No. 29.) The United States responded, (ECF No. 41), and Chatrie replied, (ECF No. 48). On December 23, 2019, the Court granted Google leave to file an amicus brief. (ECF No. 73.) In response to Chatrie's Federal Rule of Civil Procedure 17(c) subpoenas, Google also filed a total of four declarations by two Google employees: three by Marlo McGriff, and (2) one by Sarah Rodriguez. (ECF Nos. 96-1, 96-2, 110-1,[30] 147.)

On November 9, 2020, around one week before the scheduled Suppression Hearing, Google filed a Motion for Leave to Present Remote Testimony. On November 11, 2020, Chatrie responded in opposition. In this response, Chatrie argued that "[i]n person testimony from the Google employees [was] critical to the Court's resolution of Mr. Chatrie's geofence warrant," and that "Google's continued intrusion into this case warrants a finding from this Court that the

[30] On June 17, 2020, Google sought leave to file a Supplemental Declaration of Marlo McGriff (the "Motion for Leave"). The Court granted the Motion for Leave over Chatrie's objection. Given the close proximity in time, the Court continued the then-scheduled July 2, 2020 geofence hearing. The Court found that "the ends of justice [were] best served by granting a short continuance" because "the Geofence Motion to Suppress presents substantial issues of first impression that require the Court to consider a full and accurate record concerning the technology at issue." (ECF No. 115, at 4.) The Court continued the hearing to November 17, 2020.

Google witnesses are hostile/adverse witnesses." (ECF No. 166, at 1, 6.) After the Court held a status conference on the Motion for Leave to Present Remote Testimony, Chatrie filed a Motion to Continue the November 17, 2020 hearing, seeking to continue the hearing to a time when Google would be able to attend in person. On December 18, 2020, the Court granted Chatrie's Motion to Continue and scheduled the Suppression Hearing for March 4, 2021.

Considering the novel and complex questions of law at issue, the Court allowed the parties to provide supplemental briefing on discovery provided by Google and the March 4–5, 2021 Suppression Hearing. Among others, witnesses from Google—McGriff and Rodriguez—provided the Court with a relatively exhaustive picture of Google's typical response to geofence warrants. Now, after careful consideration of the issues and with the aid of the parties' thorough briefing, the Court concludes that, although this warrant is invalid for lack of particularized probable cause, the Court cannot suppress the resulting evidence because the *Leon* good faith exception applies.

III. Analysis

Chatrie seeks to suppress evidence obtained from the June 14, 2019 Geofence Warrant that covered 70,686 square meters of land around the Bank, located in a busy part of the Richmond metro area. Despite the Court's concerns about the validity of this warrant and the adoption of unsupervised geofence warrants more broadly, the Court will deny Chatrie's Motion to Suppress because the officers sought the warrant in good faith.

A. The Court Will Briefly Address Fourth Amendment Standing

Because the Court will independently deny Chatrie's motion to suppress by considering the validity of the Geofence Warrant, the Court "need not wade into the murky waters of standing," *i.e.*, whether Chatrie has a reasonable expectation of privacy in the data sought by the

warrant. *United States v. James*, No. 18cr216, 2018 WL 6566000, at *4 (D. Minn. Nov. 26, 2018); *see Byrd v. United States*, 138 S. Ct. 1518, 1530 (2018) (Fourth Amendment standing "is not a jurisdictional question and hence need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim.").

Nonetheless, the Court notes its deep concern (underlying both Fourth Amendment standing, and the third-party doctrine discussed below) that current Fourth Amendment doctrine may be materially lagging behind technological innovations. As Fourth Amendment law develops in a slow drip, "technology [continues to] enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018). Relevant here, although *law enforcement* limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in. *See* Part II.A.3.a, *supra*. The Government thus has an almost unlimited pool from which to seek location data, and "'[w]hoever the suspect turns out to be,' they have 'effectively been tailed'" since they enabled Location History. *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (quoting *Carpenter*, 138 S. Ct. at 2218).

Indeed, the "'retrospective quality of [geofence] data' enables police to 'retrace a person's whereabouts,'" and "[p]olice need not even know in advance whether they want to follow a particular individual, or when." *Id.* at 342 (quoting *Carpenter*, 138 S. Ct. at 2218). Until recently, the ease with which law enforcement might access such precise and essentially real-time location data was unimaginable. And it is this expansive, detailed, and retrospective nature of Google location data that is unlike, for example, surveillance footage, and that perhaps

causes such data to "cross[] the line from merely augmenting [law enforcement's investigative capabilities] to impermissibly enhancing" them. *Id.* at 341.

What is more, the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights. Consider, for example, a geofence encompassing a bank, a church, a nearby residence, and a hotel. Ordinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank. *See United States v. Knotts*, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). He or she thus may not be able to establish Fourth Amendment standing to challenge a time-limited acquisition of his location data at the bank.

But the individual in his or her residence likely *would* have a heightened expectation of privacy. *Silverman v. United States*, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his [or her] own home and there be free form unreasonable government intrusion."). Yet because that individual would not have been alerted that law enforcement obtained his or her private location information, and because the criminal defendant could not assert that individual's privacy rights in his or her criminal case, *United States v. Rumley*, 588 F.3d 202, 206 n.2 (4th Cir. 2009), that innocent individual would seemingly have no realistic method to assert his or her own privacy rights tangled within the warrant. Geofence warrants thus present the marked potential to implicate a "right without a remedy." *Hawkins v. Barney's Lessee*, 30 U.S. 457, 463 (1831) ("There can be no right without a remedy to secure it.").

As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing "reasonable expectation of privacy" doctrine as it relates to technology. That run of cases primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (considering the validity of using thermal imaging on one's home); *United States v. Jones*, 565 U.S. 400, 402–03 (2012) (construing "the attachment of a [GPS] tracking device to an individual's vehicle" for twenty-eight days); *Carpenter*, 138 S. Ct. at 2217 n.3 (considering whether "accessing seven days of [an individual's cell site location information] constitutes a Fourth Amendment search").

At base, these matters are best left to legislatures. *See* Zach Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TechCrunch (Jan. 13, 2022), https://tcrn.ch/35mLHkP (discussing a recently introduced New York bill that would ban the use of geofence warrants statewide). This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data. And, as discussed below, despite its ongoing efforts to improve, Google appears to do so under the guise of consent few people understand how to disable. Even with consent, it seems clear that most Google users do not know how the consent flow to control their collection of data works, nor do they know Google is logging their location 240 times a day. It is not within this Court's purview to decide such issues, but it urges legislative action. Thoughtful legislation could not only protect the privacy of citizens, but also could relieve companies of the burden to police law enforcement requests for the data they lawfully have.

B. Because the Government Lacked Particularized Probable Cause as to Every Google User in the Geofence, the Warrant Violates the Fourth Amendment

At base, this particular Geofence Warrant is invalid. The Fourth Circuit has clearly articulated that warrants, like this one, that authorize the search of every person within a

particular area must establish probable cause to search every one of those persons. Here, however, the warrant lacked any semblance of such particularized probable cause to search each of its nineteen targets, and the magistrate thus lacked a substantial basis to conclude that the requisite probable cause existed. And to the extent the Government would argue that Steps 2 and 3 cure the warrant's defects as to probable cause, such an argument is unavailing here. The Government itself contends that law enforcement demonstrated probable cause to obtain *all* the data sought without any narrowing measures (*i.e.*, de-anonymized and geographically unlimited data from everyone within the geofence). In any event, Steps 2 and 3—undertaken with no judicial review whatsoever—improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions. These steps therefore cannot buttress the rest of the warrant, as they fail independently under the Fourth Amendment's particularity prong.

1. Legal Standard: The Warrant Requirement

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Stated another way, the Fourth Amendment requires that a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and, (3) be issued by a neutral, disinterested magistrate.[31] *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotations and citations omitted). If a warrant is invalid, the proper remedy in a criminal action is "ordinarily" to suppress the evidence derived from it. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018).

[31] Because this third prong intersects with the Court's good faith analysis, the Court discusses it more fully in Part III.C.2, *infra*.

a. Probable Cause

Whether probable cause for a search exists is a "practical, common-sense" question, asking whether "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). It requires only "the kind of fair probability on which reasonable and prudent people, not legal technicians," would rely. *United States v. Jones*, 952 F.3d 153, 158 (4th Cir. 2020) (citing *Florida v. Harris*, 568 U.S. 237, 244 (2013)). Officers must present sufficient information to the magistrate judge[32] to allow him or her to exercise independent judgment. *Gates*, 462 U.S. at 239. The magistrate cannot simply ratify the bare conclusions of others. *Id.* "When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant." *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citations omitted). "[T]he duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004).

More specifically, a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Indeed, the United States Court of Appeals for the Fourth Circuit has established that warrants that authorize the search of "all persons on [a] premise[s]" must show probable cause "to believe that *all* persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (emphasis added) (second alteration in original), *overturned on other grounds by Pearson v. Callahan*, 129 S. Ct. 808 (2009). In other words, these warrants must demonstrate

[32] In the federal system, the magistrates who review and sign search warrants are judges who must have law degrees. This is not necessarily the case in state judicial systems.

"good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant in the criminal activity." *Owens*, 372 F.3d at 276 (internal quotation marks omitted).

At base, probable cause demands that law enforcement possess "a reasonable ground for belief of guilt . . . *particularized* with respect to the person to be searched or seized." *Maryland v. Pringle*, 124 S. Ct. 795, 800 (2003) (emphasis added); *see Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) ("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.") 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." *Ybarra*, 444 U.S. at 91.

b. Particularity

A warrant must also be sufficiently "particular[]." *Hurwitz*, 459 F.3d at 470. Thus, a warrant must "confine the executing [officers'] discretion by allowing them to seize only evidence of a particular crime." *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)). The warrant must therefore "identif[y] the items to be seized by their relation to designated crimes," and the "description of the items [must] leave[] nothing to the discretion of the officer executing the warrant." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (citation omitted). "So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not . . . the particularity standard is met." *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted).[33]

[33] The Framers included the particularity requirement to "end the practice, abhorred by the colonists, of issuing general warrants," which authorized officers to carry out an "exploratory rummaging in a person's belongings." *United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013) (internal citation and quotations omitted). Such "general warrants" placed "the liberty of

2. The Geofence Warrant Fails to Establish Particularized Probable Cause to Search Every Google User Within the Geofence

Although cloaked by the complexities of novel technology, when stripped of those complexities, this *particular* Geofence Warrant lacks sufficient probable cause.[34] The United States Supreme Court has explained that warrants must establish probable cause that is "particularized with respect to the person to be searched or seized." *Pringle*, 124 S. Ct. at 800. This warrant did no such thing. It first sought location information for *all* Google account owners who entered the geofence over the span of an hour.[35] For those Google accounts, the warrant further sought "contextual data points with points of travel outside of the" Geofence for yet another hour—and those data points retained *no* geographical restriction. (ECF No. 54-1, at 4.) Astoundingly, the Government claims that law enforcement established probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the geofence without any

---

every [person] in the hands of every petty officer" and were therefore denounced as "the worst instrument of arbitrary power." *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

[34] In considering whether the Geofence Warrant is valid, the Court assumes for the sake of analysis that the Government's collection of data here is a "search." *See In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 736 (noting that by obtaining a warrant and arguing for the validity of that warrant, "the [G]overnment is treating its proposed capture of information as a search"). Indeed, this is the position Google advances in its amicus brief.

[35] To be clear, the Court sees individuals from whose accounts the Government obtained data as functional subjects of the search, even though the warrant authorized officers to obtain data only from Google's servers. In the same way that users' devices generate IP address information and typically share that information with a third party, so too do users' phones generate Location History data and share that information with Google. *See, e.g.*, *United States v. Broy*, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016) (treating the defendant's IP address as if it is were defendant's property that he disclosed to a third party).

In other words, regardless of which entity's files the Government looked through, the users ultimately retain at least some joint interest in the location data their phones generate. As discussed in Part III.B.4, *infra*, however, because the Court ultimately finds that Det. Hylton acted in good faith, whether these individuals have an expectation of *privacy* in that data must be decided another day. *Cf., e.g.*, *Broy*, 209 F. Supp. 3d at 1053 (finding no reasonable expectation of privacy because the defendant disclosed his IP address to a third party).

narrowing measures.[36] Yet the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals.

Law enforcement attempted to justify the warrant by claiming that such a sweeping search "may [have] tend[ed] to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) Even if this Court were to assume that a warrant would be justified on the grounds that a search would yield *witnesses* (some of whom had already been interviewed) instead of perpetrators, the Geofence Warrant is completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime. *Cf. Owens*, 372 F.3d at 276. To be sure, a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information.[37] However, the warrant, on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.

Indeed, it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing. Law enforcement knew only that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) After the police failed to located the suspect via reviewing camera footage, speaking with witnesses, and pursuing two leads, law enforcement simply drew

---

[36] Instead, it appears that law enforcement implemented narrowing measures in this Warrant at the behest of Google. (*See* ECF No. 202, at 275–76 (discussing "go bys," template documents that outline "specific information that [Google] need[s] in order to process the search warrant").)

[37] For instance, Det. Hylton stated in his affidavit that: (1) surveillance tapes revealed that the suspect used a phone; (2) in the officer's "training and experience, when people act in concert . . . they frequently utilize cellular telephones;" (3) Google "provides electronic communication services to subscribers, including email services;" (4) Google "has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android;" and, (5) studies show that "91% of American adults own a cellular phone with 56% being smartphones." (ECF No. 54-1, at 6–7.)

a circle with a 150-meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot.[38] The Government then requested location information for *every device* within that area. *See Carpenter*, 138 S. Ct. 2206, 2216 (2018) (describing cell phone location information as "encyclopedic").

What is more, in one instance, this Geofence Warrant captured location data for a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery. Because the radius of one of the users' confidence intervals stretched to around 387 meters, the Geofence Warrant might have reported that user's location data to the Government, notwithstanding the fact that he may have simply been present in any number of nearby locations. For example, that person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard. Yet the Government obtained the person's location data just the same. The Government claims that footage depicting the perpetrator holding a phone to his ear—and nothing else—justified this sweeping warrant. That, however, is simply not "[]reasonable." U.S. Const. amend. IV.

To further underscore the breadth of this search, Chatrie's expert Spencer McInvaille pointed out a likely "false positive" from the warrant—"Mr. Blue." McInvaille testified that this

---

[38] The Government has made passing references to "several [additional] pieces of evidence" that might have guided the contours of the Geofence Warrant. (*E.g.*, ECF No. 202, at 272.) But neither the warrant nor its supporting affidavit referred to this evidence. It is therefore irrelevant to the validity of the warrant. *See Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004) (declining to consider material contained in a warrant's *application* where the warrant did not incorporate the application by reference).

"false positive" individual may not have ever stepped within the geofence—he may have simply driven "outside of the original geofence" on a nearby road, but could have nonetheless appeared "as if [he] were inside the geofence." (ECF No. 201, at 43–44, 65.) Because Google's location estimate for that person could have been "incorrect," Google may have *thought* the person had stepped foot in the target area. (ECF No. 201, at 43–44.) The Government therefore obtained two hours of unrestricted location data for an individual who perhaps had only driven within the outer vicinity of the crime scene.[39]

This Geofence Warrant therefore suffers from the same probable cause defect as that at issue in *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020). In that case, the Government sought "to erect three geofences." *Id.* 732. Two encompassed the same location during different timeframes, and the other captured a second location. *Id.* Each geofence lasted for forty-five minutes. *Id.* The court remarked that "the proposed warrant would admittedly capture the device IDs . . . for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone – other than the Unknown Subject – entering those locations is involved in the subject offense or in any other crime." *Id.* at 752. There, just as here, the warrant provided the Government "unlimited

---

[39] The fact that data points obtained during Steps 1 and 2 are anonymized when Google reports them does not completely quell this Court's concerns about the invasiveness of this warrant. Even "anonymized" location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one or two hour period. As noted above, during the March hearing, McInvaille identified three anonymous accounts captured within the geofence—"Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63–71.)

McInvaille testified that, using two hours of only "anonymized" data obtained through the warrant, he could observe each account's reported location, track each account to his or her home, and pinpoint each account's personal identity using publicly available resources even without any Step 3 information. *See* Herbert B. Dixon Jr., *Your Cell Phone is a Spy!*, Am. Bar Ass'n (July 29, 2020), https://bit.ly/3nRuCVq ("Although user data are anonymized, users' identities can nonetheless be determined by following their movements back to their homes and other places.").

discretion to obtain from Google the device IDs . . . of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on nothing more than the 'propinquity' of these persons to the Unknown Subject at or near the time" of the criminal activity. *Id.* at 753. As that court (and the Supreme Court in *Ybarra*) recognized—and as this Court now concludes—the Fourth Amendment's probable cause requirement demands more than "mere propinquity" to a crime. *Id.* at 752; *Ybarra*, 444 U.S. at 91.

Despite the Government's reliance on *United States v. McLamb*, that case is inapposite. There, the Fourth Circuit upheld a warrant that allowed law enforcement to obtain identifying information of "any user entering a username and password into" an internet-based dark website where users could download or upload child pornography. *United States v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018). But there, a user's "mere propinquity" to the website *did* necessarily establish probable cause: any user visiting the site likely participated in the criminal conduct of viewing or sharing child pornography. *Id.* Here, on the other hand, a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime. *McLamb* therefore does not inform this case.[40]

Nor does the Government's reliance on *United States v. James* persuade. The *James* court considered a warrant to collect cell tower information (so-called "tower dumps") to determine whether "a particular cellular phone number (ostensibly held by the robber) could be identified during the timeframes of each of the respective robberies." 2018 WL 6566000, at *1.

---

[40] But one can readily imagine other instances when one's "mere propinquity" to a location, as in *McLamb*, likely *would* provide probable cause to obtain location data for each individual within a geofence. This would *not* necessarily involve improper use of location data. For example, the FBI appears to have employed geofence technology to locate participants in the January 6 Capitol riots. Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, Wired (Sept. 30, 2021), https://bit.ly/3HktvWU. In that situation, one's presence within the Capitol *would* perhaps, by itself, provide probable cause that an individual was present without permission and was therefore committing a crime.

Law enforcement sought the cell tower data based on the notion that a cell phone number present at the location and time of all six robberies created sufficient probable cause that the number belonged to the robber. *Id.* Ultimately, the court concluded that "there was a fair probability that data from the cellular towers" would contain identifying information about the perpetrator and that therefore the warrants sufficed to allege probable cause. *Id.* at *4. As another court has noted however, *James* did not account for whether probable cause existed to search through the *other* individuals' location information. *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751; *see also id.* at 752 (distinguishing another tower dump decision from the geofence context because the court discussing the tower dump "stopped the analysis once the court found probable cause in the 'nexus' between the offense and *all* the requested cell phone records, without analyzing whether probable cause existed to obtain all of those records." (quoting *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769 (S.D. Tex. 2013)). *James* therefore stopped short of considering whether "particularized" probable cause existed, and it is precisely that lack of narrowly-tailored probable cause that is fatal to this Geofence Warrant.[41]

The Court cautions that it declines to consider today whether a geofence warrant may *ever* satisfy the Fourth Amendment's strictures. *See In re Search Warrant Application for*

---

[41] Throughout this litigation, the parties—and Google—drew or resisted analogies to tower dumps. As explained above, however, the lead tower dump cases like *James* do not persuade this Court. Those decisions either decide that individuals' proximity to certain towers *alone* creates probable cause to search them, or altogether neglect to consider such particularity concerns. *James*, 2018 WL 6566000, at *4; *see also United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021) (affirming the district court's adoption of the magistrate judge's original opinion on the same grounds). Indeed, the Eighth Circuit in *James* expressly warned that in holding valid the warrants at issue—which connected a robber to a *series* of crimes—was *not* holding "that it is now fair game to search the records from 'cell phone towers near the location of *every* crime.'" *Id.* at 1106. The Court similarly concludes here that the commission of a single crime—by itself, and with no narrowing measures or guardrails—is not sufficient to search geofence records "near the location of *every* crime." *Id.*

Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020) ("[I]t is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are implicated."). Consider, for example, one of the few other federal court opinions to address a geofence warrant—*In re Search of Information That Is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021) [hereinafter "DDC Opinion"]. There, law enforcement devised a two-step process to narrow the list of individuals whose data they would obtain. *Id.* at *5–6. At Step 1, Google would identify all accounts who entered the geofence within the relevant time periods. *Id.* For each of these accounts, Google would turn over only anonymized data. *Id.*

The Government would then review that data, identify likely suspects based on the "mov[ement]" of the users' devices through the geofence, and, crucially, identify to the *court* the devices the Government believed belonged to the perpetrator. *Id.* The *court* could then, at its discretion, order Google to disclose to the Government personally identifying information for devices that belonged to likely suspects. *Id.* In essence, to obtain a warrant authorizing disclosure of de-anonymized data, the Government was required to demonstrate that location data for a *particular* user or set of users would provide evidence of the crime. And crucially, the warrant left ultimate discretion as to which users' information to disclose to the reviewing court, not to Google or law enforcement.

In certain situations, then, law enforcement likely *could* develop initial probable cause to acquire from Google *only* anonymous data from devices within a narrowly circumscribed geofence at Step 1. *See Hurwitz*, 459 F.3d at 473 (a warrant must be "no broader than the probable cause on which it is based"). From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly,

officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information. Although the *instant* warrant is invalid, where law enforcement establishes such narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional.[42]

At bottom however, particularized probable cause "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91. The Court finds unpersuasive the United States' inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby. In essence, the Government's argument rests on precisely the same "mere propinquity to others" rationale the Supreme Court has already rejected as an appropriate basis for a warrant. *Id.* This warrant therefore cannot stand.

---

[42] The warrant in the DDC Opinion differed in additional ways. For instance, that warrant appears to have sought only location data that fell *within* the geofence across time periods notably shorter than the geofence at bar. *See* DDC Op. at *12 ("[T]he geofence only provides cell phone user's whereabouts in a single area for a handful of minutes on the days in question, not the sum-total of their daily movements."). Here, by contrast, the Government sought two hours of location data *not* bound within the geofence. *Cf.* DDC Op. *12 ("[T]he warrant does not seek location data for days or even hours to track the whereabouts of the perpetrators, but rather location data that is tailored and specific to the time of the [alleged crimes] only." (second alteration in original) (quotation marks and citation omitted)).

In addition to restricting officers' discretion when selecting which accounts for which to obtain personally identifying information, limiting the pool of data returned to only location points *within* the geofence helps assuage this Court's concerns with respect to particularized probable cause, and, more broadly, concerns that broad swaths of anonymous data can be used to pinpoint numerous individuals' identities.

3. This Geofence Warrant's Three-Step Process Does Not Cure Its Defects

To the extent the Government would attempt to argue in the alternative that this warrant's three-step process cures any defects with the warrant's particularized probable cause, such an argument is unavailing.[43] Even if this narrowing process cured any of the warrant's shortcomings as to particularized probable cause, this process cannot independently buttress the warrant for an entirely separate reason: clear lack of particularity. Warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In other words, "[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as what to seize." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). But Steps 2 and 3 of this warrant leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users.

This warrant, for instance, contains no language objectively identifying *which* accounts for which officers would obtain further identifying information. Nor does the warrant provide objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny. Nor does the warrant even simply limit the *number* of devices for which agents could obtain identifying information. Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval.

[43] The Court recognizes that the Government primarily argues that it possessed probable cause to obtain *all* data sought regardless of the three-step process.

The facts here underscore the breadth of discretion law enforcement possessed under this warrant.[44] After receiving anonymized information on the nineteen targeted users at Step 1, Det. Hylton requested the additional location information (Step 2) and subscriber information (Step 3) "for all 19 device numbers produced in [S]tep 1." (ECF No. 96-2, at ¶ 15.) In response, a Google specialist "called Detective Hylton and explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant."[45] (ECF No. 96-2, at ¶ 16.) During that call, "[t]he LIS specialist also explained the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16.) Det. Hylton eventually narrowed his requests. Yet he did not specify to Google why he was choosing these particular users.

Google's insistence on narrowing the list does not render this warrant sufficiently particular. For one thing, this warrant's clear text does not specifically allow Google to limit the group of accounts that would be subject to further scrutiny. (*See* ECF No. 54-1, at 4–5 (noting only that Google "shall produce" further information).) But even if it did, Fourth Amendment discretion must be confined to the signing magistrate, not the executing officers or a third party. *United States v. Chadwick*, 433 U.S. 1, 9 (1977) ("The judicial warrant has a significant role to play in that it provides the detached scrutiny of a neutral magistrate . . . ."), *abrogated on other*

---

[44] The facts also raise a concern about how even good faith effort by law enforcement can impinge upon constitutional boundaries through a lack of understanding as to what this warrant actually produces and how it does so. While all performed in good faith—especially given this novel and complex process—Det. Hylton returned the warrant before it was served, improperly requested Step 2 and 3 information simultaneously, failed at first to narrow his request at Step 2, and incorrectly tried to add a Step 4 to the process. While the Google LIS allowed only what was permitted under the warrant (which Det. Hylton did not resist), Fourth Amendment protections should not be left in the hands of a private actor.

[45] Det. Hylton received this remonstration despite having executed three geofence warrants prior to this one.

grounds by California v. Acevedo, 500 U.S. 565 (1991). Stated plainly, Steps 2 and 3 "put[] no limit on the [G]overnment's discretion 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." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 754. These Steps accordingly fail to provide the executing officer with clear standards from which he or she could "reasonably . . . ascertain and identify . . . the place to be searched [or] the items to be seized." *Blakeney*, 949 F.3d at 861. The Government therefore cannot rely on Steps 2 and 3 to supply this warrant with particularized probable cause, as these steps independently fail under the Fourth Amendment's particularity requirement.

4. The Third-Party Doctrine

Lastly, the Court simply cannot determine whether Chatrie "voluntarily" agreed to disclose his Location History data based on this murky, indeterminate record. But the Court expresses its skepticism about the application of the third-party doctrine to geofence technology. Under this doctrine, "a person [generally] has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). However, in *Carpenter v. United States*, the Supreme Court refined this principle and held than an individual *does* possess an expectation of privacy in seven days of cell-site location information collected by a wireless carrier. 138 S. Ct. at 2217 & n.3. Here, the Government argues that Chatrie cannot claim a reasonable expectation of privacy in his Location History data because (1) he "voluntarily disclosed" the information to Google; and, (2) the two hours of location data sought here do not implicate the same privacy concerns as the seven days obtained in *Carpenter*. (ECF No. 41, at 11; *see* ECF No. 41, at 9–13.)

The Court thinks otherwise. Common sense underscores Supreme Court Justice Sonia Sotomayor's observation in *United States v. Jones* about "voluntary" collection of electronic information unbeknownst to the subject of the warrant. As to the third-party doctrine, Justice Sotomayor observed that:

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.

Jones, 565 U.S. at 417–18 (Sotomayor, J., concurring). At base, the topic is complex. And considering the messiness of the current record as to how and when Chatrie "gave consent," the Court cannot—and need not—reach a firm decision on the issue. But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data, even for "just" two hours. Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216; *see id.* at 2219 ("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."). Although, unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day.

This is especially so given the limited and partially hidden warnings provided by Google. In the Google Assistant set-up process, the device likely provided Chatrie a single pop-up screen informing him that "[t]his data may be saved and used in any Google service where [he was] signed in to give [him] more personalized experiences," and that he "can see [his] data, delete it

and change [his] settings at account.google.com." (ECF No. 147, at ¶ 7; *see* ECF No. 96-1, at ¶ 7; ECF No. 201, at 102; ECF No. 202, at 21.) However, the consent flow did not detail, for example, how frequently Google would record Chatrie's location (every two to six minutes); the amount of data Location History collects (essentially *all* location information); that even if he "stopped" location tracking it was only "paused," meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (*i.e.*, down to twenty or so meters).[46] (ECF No. 201, at 122, 136; ECF No. 202, at 71.)

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. The record here makes plain that these "descriptive texts" are less than pellucid. Although the Court cannot reach a final decision on the issue today based on the current record here, Chatrie likely could not have, in a "meaningful sense, . . . voluntarily 'assumed the risk' of turning over a comprehensive dossier of his physical movements" to law enforcement. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745); *see id.* at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

[46] As Google's expert Marlo McGriff testified, Location History also allows Google to estimate a device's *elevation*. Thus, if New York City law enforcement obtained a geofence warrant with a roughly 150-meter radius (similar in size to the one at issue here) that encircled the Empire State Building, even if it were not fully precise, the police might be able to obtain location data for many thousands of people.

C. Because Det. Hylton Consulted with Government Attorneys in the Face of Novel Technology and Obtained Similar Warrants in the Past, and Because the Warrant Was Not Otherwise "So Facially Deficient," the Good-Faith Exception Applies

Despite the warrant's defects, the Court ultimately cannot find that excluding the instant evidence would serve to deter future improper law enforcement conduct. This is particularly so in light of rapidly advancing technology and lack of judicial guidance on this novel investigatory technique, and where, as here, prosecutors and magistrates approved three similar warrants.

1. Legal Standard

The exclusionary rule "is neither 'a personal constitutional right' nor is it 'designed to redress the injury occasioned by an unconstitutional search.'" *United States v. Manafort*, 323 F. Supp. 3d 795, 805 (E.D. Va. 2018) (quoting *Davis v. United States*, 564 U.S. 229, 236 (2011)). Rather, the exclusionary rule "is a prudential doctrine created . . . to compel respect for" constitutional rights. *Davis*, 564 U.S. at 236–37 (2011). "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *McLamb*, 880 F.3d at 690 (internal quotation marks and citation omitted). Where suppression would not produce deterrent benefits, the exclusionary rule does not apply. *United States v. Leon*, 468 U.S. 897, 909 (1984).

For that reason, evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was "objectively reasonable." *Id.* at 922–23. Generally, the fact that a neutral magistrate has issued a warrant "suffices to establish" that a law enforcement officer has "acted in good faith in conducting the search." *Id.* at 922. Therefore, searches carried out pursuant to a warrant "rarely require any deep inquiry into reasonableness." *Id.*

The Fourth Circuit has nonetheless set out four categories of cases in which the good-faith exception will not apply:

> (1) if the magistrate or judge in issuing a 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 of the truth; (2) if the issuing magistrate wholly abandoned his [or her] judicial role[;] . . . (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the 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.

United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotation marks and citations omitted). When considering a motion to suppress the fruits of a novel investigative technique, courts generally decline to hold a warrant "facially deficient where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. Further, "consultation [with Government attorneys prior to seeking a warrant] is a relevant consideration in determining whether the warrant was facially deficient." *United States v. Matthews*, 12 F.4th 647, 657 (7th Cir. 2021).

2. Because Det. Hylton Relied on the Approval of Prior Warrants in the Face of Novel Technology, the Good-Faith Exception Applies

a. Det. Hylton

Despite the warrant failing under Fourth Amendment scrutiny, the *Leon* good faith exception shields the resulting evidence from suppression. The warrant lacked particularized probable cause, but it was not "*so* lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923 (emphasis added). This is particularly so because "the legality of [this] investigative technique [was] unclear," and Det. Hylton sought "advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. When Det. Hylton applied for the Geofence Warrant, no court had yet ruled on the

legality of such a technique. And as this Court's preceding analysis demonstrates, the permissibility of geofence warrants is a complex topic, requiring a detailed, nuanced understanding and application of Fourth Amendment principles, which police officers are not and cannot be expected to possess. *See* Part III.B.2, *supra*.[47]

In the face of this legal uncertainty, Det. Hylton relied on his past experience seeking geofence warrants—he had sought three before applying for this one. Magistrates and prosecutors had approved all three. *See Matthews*, 12 F.4th at 656 (noting the "general principle that attorney involvement supports a finding of good faith"). Det. Hylton testified that these prior warrants were "mostly similar" to the one at bar—all but one incorporated a roughly 150-meter radius, although a "few of them had more locations because of the more robberies to investigate." (ECF No. 202, at 328.) Even accounting for his miscues, in light of the complexities of this case, Det. Hylton's prior acquisition of three similar warrants, and his consultation with Government attorneys before obtaining those warrants, the Court cannot say that Det. Hylton's reliance on the instant warrant was objectively unreasonable. *See McLamb*, 880 F.3d at 691. While magistrate approval and consultation with the prosecution alone cannot and should not mechanically trigger the good-faith exception, exclusion here likely would not "meaningfully deter" improper law enforcement conduct. *Herring v. United States*, 555 U.S. 135, 144 (2009).[48]

---

[47] The Court therefore rejects Chatrie's argument that "one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements" would know that this warrant was insufficient. (ECF No. 205, at 42.)

[48] This is particularly so because Det. Hylton's "consultation with [G]overnment attorneys [in the face of untested investigatory techniques] is precisely what *Leon*'s 'good faith' expects of law enforcement." *McLamb*, 880 F.3d at 691.

b. Magistrate Bishop

Nor can this Court conclude that Magistrate Bishop wholly abandoned his role as a detached magistrate as Chatrie argues. *See Doyle*, 650 F.3d at 470. This exception to good faith primarily looks to whether the magistrate "overstep[ped] his [or her] judicial responsibilities and compromise[d] his judicial neutrality," *United States v. Gary*, 420 F. Supp. 2d 470, 486 (E.D. Va. 2006) (quoting *United States v. Servance*, 394 F.3d 222, 231 (4th Cir. 2005), *vacated on other grounds by Servance v. United States*, 544 U.S. 1047 (2005)), by, for example, actively participating in an investigation, *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327 (1979); retaining a pecuniary interest in issuing the warrant, *Connally v. Georgia*, 429 U.S. 245, 249–51 (1977) (per curiam); "rubber stamp[ing]" a warrant that contained a "bare bones" affidavit, *Wilhelm*, 80 F.3d at 121 (4th Cir. 1996); or, failing to make an independent assessment as to the validity of the warrant, *United States v. McKneely*, 810 F. Supp. 1537, 1547 (D. Utah 1993), *rev'd on other grounds by United States v. McKneely*, 6 F.3d 1447 (10th Cir. 1993).

Chatrie has, perhaps, shown that Magistrate Bishop *should have* considered the implications of the Warrant more carefully. But ultimately, he has "produced no evidence to show that the magistrate did not read the affidavit or that he read it so cursorily as to have wholly abandoned his neutral and detached role." *Gary*, 420 F. Supp. 2d at 487; (*see* ECF No. 202, at 361–62 (noting that the magistrate reviewed the warrant for around fifteen or thirty minutes).) Nor did he "suggest that the magistrate acted in a partisan manner or aligned himself with the police. Consequently, . . . the second [*Leon* exception] does not bar application of the good-faith exception." *Gary*, 420 F. Supp. 2d at 487. Chatrie further argues that "[t]he magistrate's utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as . . . neutral arbiter." (ECF No. 205, at 41.) But the Fourth Circuit has instructed

that such "an allegation that a search warrant application contained grossly insufficient information is best analyzed under the third *Leon* exception." *United States v. Wellman*, 663 F.3d 224, 229 (4th Cir. 2011). And for the reasons explained above, that exception does not warrant suppression either.

Finally, the Court must address Chatrie's challenge to Magistrate Bishop's qualifications. Chatrie contends that Magistrate Bishop did not possess the requisite statutory qualifications to make the instant probable cause determination. The Court first observes that, in Virginia, any United States citizen who is a resident of the Commonwealth is eligible to be appointed as a magistrate with certain limitations not relevant here. Va. Code § 19.2-37. To qualify today, a magistrate need only have "a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B). And "[a] person initially appointed as a magistrate prior to July 1, 2008, who continues in office without a break in service is *not* required to have a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B) (emphasis added). No law degree is required. Indeed, "[n]o person appointed as a magistrate on or after July 1, 2008, *may* engage in the practice of law." Va. Code § 19.2-37(F) (emphasis added).

Magistrate Bishop graduated from Pensacola Christian College with a Bachelor of Science Degree in Criminal Justice in May of 2016. He was appointed as a Virginia magistrate roughly two years later in June 2018, began certification school in July 2018, and was formally appointed and "released for independent service on October 24, 2018." (ECF No. 156, at ¶ 3.) His nine-month probationary period pursuant to Virginia Code § 19.2-38 ended on March 12, 2019. In other words, Magistrate Bishop had been serving as a non-probationary magistrate just

three months before he signed this sweeping and powerfully intrusive Geofence Warrant on June 14. And he had graduated from college just three years earlier.

Chatrie does not rest on Magistrate Bishop's lack of a law degree. He instead avers that Magistrate Bishop's undergraduate degree was not sufficiently "accredited" under Virginia law. (ECF No. 135, at 6–9.) As noted, Pensacola Christian College does not appear to be officially licensed in Florida. (*See* Ex. B 24, ECF No. 135-2 ("Pensacola Christian College operates in the state of Florida as an independent institution of higher learning that is exempt from state commission oversight as per Florida statutes.").) Further, it does not appear to be accredited by a regional higher-education accrediting agency. *See, e.g.*, Southern Association of Colleges and Schools Commission on Colleges, *Accredited and Candidate List January 2022* (last visited Mar. 1, 2022), https://bit.ly/3cb3ICF. Yet the Transnational Association of Christian Colleges and Schools ("TRACS")[49] accredited the college in 2013. *Pensacola Christian College*, TRACS (last visited Mar. 1, 2022), https://bit.ly/3C22S5j.

Chatrie contends that the TRACS accreditation means little, as "[t]he most widely respected agencies are regional [accrediting] bodies," while "national accrediting agencies are significantly less prestigious." (ECF No. 135, at 7.) He points out that elsewhere, the Virginia Code and Virginia Administrative Code specify that certain professionals receive degrees accredited by specific agencies (typically distinguishing between regional and national entities), and that professionals with similar levels of expertise are typically required to obtain a degree from a regionally accredited school. *See* Va. Code § 54.1-4400; 18 Va. Admin. Code 115-40-22, 160-40-280. If the Court is to read anything into this, however, it is precisely the opposite

[49] TRACS is a national agency recognized by the Council for Higher Education Accreditation and the United States Department of Education. *CHEA- and USDE- Recognized Accrediting Organizations*, CHEA (last visited Mar. 1, 2022), https://bit.ly/3og0sLw.

conclusion from Chatrie's. The notion that Virginia lawmakers narrow the permissive group of accrediting agencies *elsewhere* merely signals that the lawmakers know how to limit the pool of accrediting bodies but chose not to do so here. *Cf. Alexis v. Barr*, 960 F.3d 722, 735 n.1 (5th Cir. 2020) (Dennis, J., dissenting) (noting that where a statute defined a term more specifically in one place but not the other, lawmakers had "intentionally omitted" that more specific definition in the other usage). Under Virginia Code § 19.2-37 then, Magistrate Bishop's degree likely suffices.

To the extent Chatrie also attacks Magistrate Bishop's decision because he "would have had, at most, only a few months of experience evaluating warrant applications on his own when he signed the geofence warrant," that argument cannot prevail given Virginia's statutory scheme. (ECF No. 135, at 9.) Virginia magistrates must complete a training program, pass a certification examination, and serve a nine-month probationary period before hearing cases without supervision. Va. Code § 19.2-38. Magistrate Bishop had done this, and he had been certified by the Commonwealth of Virginia's Office of Executive Secretary. As a general principle, "[s]tates are entitled to some flexibility and leeway in their designation of magistrates, so long as all are neutral and detached and capable of the probable-cause determination required of them." *Shadwick v. City of Tampa*, 407 U.S. 345, 354 (1972). In the ordinary course then, Virginia sufficiently trains its magistrates to determine probable cause.

Frankly, however, it is not clear to the Court that *any* person just three years out of college should be burdened with the responsibility of approving or rejecting a warrant of this complexity and magnitude. The Court certainly does not impute any bad faith or improper action by Magistrate Bishop (or the Commonwealth). This case has shown, however, the myriad ways that geofencing instigates a massive intrusion into individual rights, and it does so without

notice to potentially thousands of persons with phones within it. It seems less than evident that all law enforcement officers have a clear understanding of the invasive scope of these warrants either. Nor do most magistrates, with or without a law degree. Ultimately, it is for the General Assembly to review or change its magistrate practice given this new technology, and one hopes they would.

In any event, even if Magistrate Bishop's degree or lack of experience did not qualify him to make this consequential finding, the good faith exception would still apply. The Fourth Circuit recently concluded in *McLamb* that the good faith exception is not categorically inapplicable even if the instant "warrant . . . reache[s] beyond the boundaries of a magistrate judge's jurisdiction" where suppression would not "produce an appreciable deterrence on law enforcement." 880 F.3d at 691 (internal quotation marks omitted). The Court finds that suppression based on a technical defect of the magistrate's credentials would not serve to deter improper law enforcement conduct. In a typical investigation, officers simply cannot be required to consult a magistrate's resume before approaching that magistrate to obtain a warrant.

IV. Conclusion

Despite the Court finding good faith here, the Court nonetheless strongly cautions that this exception may not carry the day in the future. This Court will not simply rubber stamp geofence warrants. If the Government is to continue to employ these warrants, it must take care to establish particularized probable cause. As the legal landscape confronts newly developed technology and further illuminates Fourth Amendment rights in the face of geofence practices, future geofence warrants may require additional efforts to seek court approval in between Steps, or to limit the geographic and temporal information sought. But in light of the complex legal issues that lead to this Court's conclusion, the Court cannot say that Det. Hylton's reliance on the

Geofence Warrant was objectively unreasonable. Accordingly, the *Leon* good faith exception applies, and the Court will deny Chatrie's motion to suppress evidence obtained as a result of the Geofence Warrant.

For the foregoing reasons, the Court will deny the Motion to Suppress. (ECF No. 29.) An appropriate Order shall issue.

Date: 3-3-2022
Richmond, Virginia

/s/
M. Hannah Lauck
United States District Judge