CASE NO.: 23-60321

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff – Appellee,

V.

JAMARR SMITH, THOMAS AYODELE, GILBERT MCTHUNEL, II
Defendants – Appellants

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
OXFORD DIVISION

INITIAL BRIEF OF APPELLANT
CRIMINAL APPEAL

Goodloe T. Lewis
CJA-FPD for Smith
1305 Madison Avenue
Oxford, Mississippi 38655
(662) 234-4000 (telephone)
(662) 234-2000 (facsimile)
glewis@hickmanlaw.com
Mississippi Bar No.: 9889

Paul Chiniche
CJA-FPD for McThunel
265 N. Lamar Blvd., Ste. W
Oxford, Mississippi 38655
(662) 234-4319 (telephone)
(662) 259-8451 (facsimile)
pc@chinichelawfirm.com
Mississippi Bar No.: 101582

William F. Travis
CJA-FPD for Ayodele
8619 HWY 51 N.
Southaven, MS 38671
(662) 393-9295 (telephone)
bill@southavenlaw.com
Mississippi Bar No.: 8267

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

UNITED STATES OF AMERICA PLAINTIFF/APPELLEE

V. CASE NO.: 23-60321

JAMARR SMITH, ET AL DEFENDANTS/APPELLANTS

CERTIFICATE OF INTERESTED PERSONS

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judge of this court may evaluate possible disqualification or recusal.

1. Hon. Sharion Aycock, United States District Judge;

2. Jamarr Smith, Defendant/Appellant;

3. Thomas Ayodele, Defendant/Appellant;

4. Gilbert McThunel, II, Defendant/Appellant

5. Goodloe T. Lewis, CJA Counsel for Defendant/Appellant Jamarr Smith;

6. William F. Travis, CJA Counsel for Defendant/Appellant Thomas Iroko Ayodele;

7. Paul Chiniche, CJA Counsel for Defendant/Appellant Gilbert McThunel, II;

8. Robert J. Mims, Assistant United States Attorney, Northern District of Mississippi; and

9. Clyde McGee, IV Assistant United States Attorney, Northern District of Mississippi.

/s/ Goodloe T. Lewis
GOODLOE T. LEWIS, MSB #9889
Attorney of Record for Jamarr Smith
Defendant/Appellant

/s/ *Paul Chiniche*
PAUL CHINICHE, MSB #101582
Attorney of Record for Gilbert McThunel, II
Defendant/Appellant

/s/ *William F. Travis*
WILLIAM F. TRAVIS, MSB #8267
Attorney of Record for Thomas Ayodele
Defendant/Appellant

STATEMENT REGARDING ORAL ARGUMENT

Since geofence warrants are a novel and complex investigative method with substantial Constitutional implications, oral argument would be helpful and Defendants/Appellants hereby request same.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Pages**

Statutes

Rules

Other Authorities

STATEMENT OF JURISDICTION

1. Subject-Matter Jurisdiction in the District Court. This case arose from the prosecution of an offense against the laws of the United States of America. The district court had jurisdiction over this case under 18 U.S.C. §3231.

2. Jurisdiction in the Court of Appeals. This is a direct appeal from a final decision of the District Court for the Northern District of Mississippi, Oxford Division, entering judgments of conviction and imposing criminal sentences. This Court has appellate jurisdiction under 28 U.S.C. §1291 and 18 U.S.C. §3742.

The district court sentenced all three defendants on June 15, 2023. Jamarr Smith and Gilbert McThunel, II were sentenced to 121 months of imprisonment. (ROA.434, 2126; RE 8 & 9). Thomas Iroko Ayodele was sentenced to 136 months of imprisonment. (ROA.1992; RE 10). Appellant Jamarr Smith filed his Notice of Appeal of that Judgment on June 15, 2023, in compliance with Fed. R. App. P. 4. (ROA.440; RE 2). Appellant Gilbert McThunel filed his Notice of Appeal of that Judgment on June 20, 2023. (ROA.2132; RE 3). Appellant Thomas Iroko Ayodele filed his Notice of Appeal of that Judgment on June 21, 2023. (ROA.2002; RE 4).

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

1. False statement and omission of fact in warrant application. A warrant application must contain a truthful and complete factual showing of probable cause to permit the magistrate to make an independent determination as to its validity. Here, the affidavit contained a statement that a suspect was "possibly" using a cellular device (which was an artifact from the form or "go by" that the agent was using to draft the application). The application also failed to notify that the magistrate that the warrant required the search of 592 million Google accounts. Should the district court have invalidated this warrant?

2. Geofence warrants are unconstitutional. The Fourth Amendment requires that warrants state probable cause to search the place and seize the evidence therein; and particularize the data to be searched and seized. The warrant here did not identify a particular cellular device to search. Instead it required Google to search 592 million accounts looking for information of interest to the government. It was a general warrant. Is this a valid warrant and should the good faith exception apply?

3. *Daubert* Precludes government expert Moody's Testimony. In the first case in the country ever tried to a jury concerning Google location data, the government's expert on this subject was unaware of studies by anybody other than Google or the government that this theory was reliable. He was not aware of any

peer review studies of this theory. He did not know the error rate – or even if there was an error rate. He was not aware as to whether the theory had widespread acceptance in the greater scientific community – in fact, he did not believe that the scientific community would have reason to investigate the theory. The basis for his opinion was *ipse dixit* (without support). Should the district court have permitted this witness to testify?

STATEMENT OF THE CASE

I. FACTS RELEVANT TO ISSUES SUBMITTED FOR REVIEW

A. Underlying offense.

On February 5, 2018 at about 5:30 in the afternoon, the victim, Sylvester Cobbs, was working as a contractor for the United States Postal Service. His job on behalf of the Memphis distribution center was to deliver and pick up mail from five rural post offices in Desoto County and Tunica County, Mississippi. (ROA.1020). One of these post offices is in the small, unincorporated community of Lake Cormorant, Desoto County, Mississippi.[1]

Alone, Cobbs backed his box truck up to the rear of the post office building in Lake Cormorant, got out and went to unlock the back door to retrieve the mail

[1] Lying just east of the Mississippi River, Lake Cormorant is almost dead-center between Memphis, Tennessee and Tunica, Mississippi on Highway 61. If the Mississippi Delta begins in the lobby of the Peabody Hotel in Memphis, (*see* David L. Cohn, *God Shakes Creation* (Harper 1935)), then Lake Cormorant is in the very narrow top part of the Delta.

bags. (ROA.1028). At that point, an assailant wearing a mask sprayed Cobbs with pepper spray, tussled with him, hit him with a gun and took registered mail from the truck. (ROA.1028-30). Cobbs was unable to identify the assailant. (ROA.1029.). Cobbs also saw a red Hyundai automobile in the vicinity, but could not identify the driver. (ROA.1042, 1045-46).

Somewhat earlier that day, a resident of Lake Cormorant named Forrest Coffman saw the red Hyundai driving around and approached it to see what was going on. (ROA.1380-81). The driver asked for directions back to Highway 61. (ROA.1380). Coffman described the driver as a light skinned black man with reddish hair. (ROA.1396). After meeting with law enforcement on the day of the incident, Coffman had no further involvement with the matter for approximately 15 months. (ROA.1402-03).

Stephen Mathews of the United States Postal Inspection Service investigated the robbery. There was a video of the incident taken from a camera on a farm office across the street from the post office. (Trial Exhibit G-1) (ROA.1134). Based upon his examination of the video, Mathews determined that three suspects were involved, plus a white SUV and a red Hyundai. (ROA.1134). The government investigated the incident using a variety of techniques: studying the video, doing a tower dump, interviewing witnesses, checking for physical evidence

(fingerprints, DNA, etc.). Beyond that, the government had no suspects and no leads. (ROA.1139-41, 1197-1198).

The case was at a standstill for approximately nine months until November 2018, when Mathews learned of a new investigative technique, now called a "geofence warrant." (ROA.1198-1199).

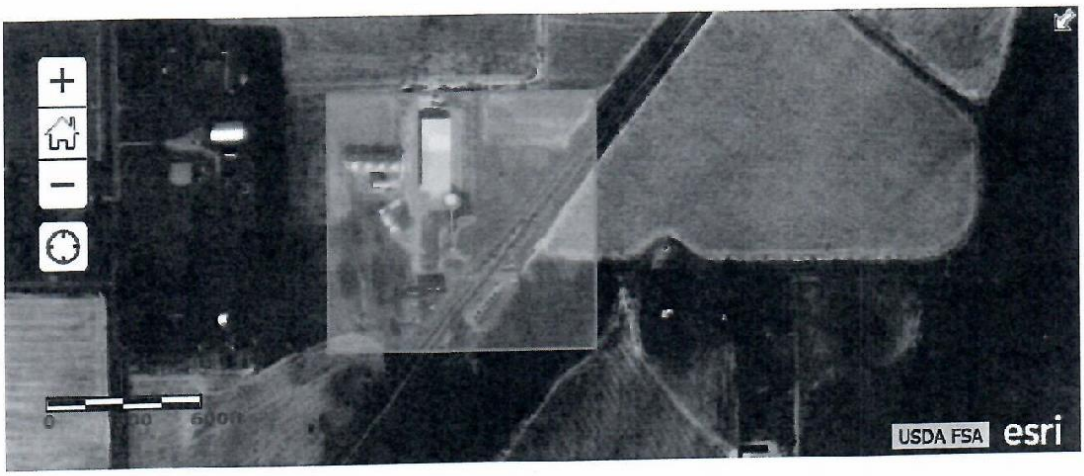
B. Bereft of suspects, the government sent a warrant to Google.

On November 8, 2018, Inspector Todd Matney of the United States Postal Inspection Service submitted an Application for a Search Warrant with attached affidavit to U.S. Magistrate Judge LeRoy Percy seeking help from Google in the form of a novel "geofence" warrant, forcing Google to search hundreds of millions of users to try and determine which devices were in the vicinity. (Application, ROA.104; Affidavit, ROA.105-112; RE 11). Postal Inspector Mathews drafted the warrant, and because he had never drafted or even been associated with a geofence warrant before, he used a form or several "go bys" provided to him by other law enforcement agents and then tried to tailor it to this case. (ROA.751-52, 794-95).

The affidavit stated that "there is probable cause to believe that certain unknown Google accounts associated with a particular specified location at a particular specified time, contain evidence, fruits and instrumentalities of a violation of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee." (ROA.106; RE 11). The attachment identified no specific Google

accounts of any particular individual; instead, attachment identified only a geographical box (i.e. a geofence) of coordinates around the Lake Cormorant Post Office as follows:

The highlighted area in the below map is the area represented by the coordinates listed above and the location pinned in the middle of the highlighted area is the location of the Lake Cormorant Post Office.



(ROA.112; RE 11). This box covered approximately 98,192 square meters, which is roughly the size of 18 football fields.[2]

The affidavit contained a Probable Cause Statement which generally described the crime and that a couple of vehicles appeared to be involved with it. (ROA.108-109; RE 11). None of those statements provided any specific probable cause to search a cell phone. Indeed, it is undisputed that no actual cell phone is

[2] For reference, a football field is slightly over 5,351 square meters. www.themeasureofthings.com

shown in the video. The affidavit then contained this critical statement:

> 16. Postal Inspectors conducted a detailed review of video surveillance and it appears the robbery suspect is **possibly using a cellular device** both before and after the robbery occurs.

(ROA.109; RE 11 (emphasis added)). Matney stated that this paragraph was included because, according to the persons with whom he and Mathews consulted, a geofence search warrant "required" that statement. (ROA.752). The affidavit also stated that, in the opinion of Matney, cell phones are used to plan crimes. (ROA.109; RE 11). That was the entire probable cause statement related to cellular devices.

The affidavit stated that the warrant would "identify which cellular devices were near the location where the robbery took place and may assist law enforcement in determining which persons were present or involved with the robbery under investigation." (ROA.110; RE 11). The affidavit stated that in response to the warrant, location data will:

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

(ROA.110; RE 11 (emphasis added)). It is undisputed that the government did not

undertake "further legal process" to obtain any additional data from Google.

C. What Google did with the geofence warrant.

Google collects location data from devices (typically cellphones, but not always) that (1) are either Android devices or other devices running a Google app; and (2) have location services activated. This is not a device-level permission – Google collects this data at the account-level. (ROA.818-819). The purpose for Google collecting this information is not to solve crimes, but rather to improve the "user experience" to, for example, optimize its map functions; e.g. when it knows the user likes to buy coffee in the morning, it will point out coffee shops in the area. (ROA.819-820).

The warrant on its face, which was granted on November 8, 2018, established a three-step process where Google and the government collaborated to decide what information to produce. (ROA.114).

II. Information to Be Provided by the Provider

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

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

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

Step 1

3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)

Step 2

4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

Step 3

(ROA.114).

1. Step 1

In Step 1, the warrant sought "all location data" in Google's possession for devices inside the geofence at the times in question. This data was to be produced

in an "anonymized" format that did not identify the specific accounts associated with the devices that showed up. (ROA.821, 826).

Because Google does not know which users have Location History enabled on their phones,[3] it is required to search all accounts with Location History enabled. (ROA.114, 821-24). In October, 2018 (the month before the warrant was applied for), "there were approximately 592 million daily active users of Location History worldwide." (ROA.822). Therefore, Google searched approximately 592 million accounts to determine whether they contained responsive data to the warrant, a search of breathtaking scope in response to Step 1 of the warrant. (ROA.826-27).

Notably, Google's search was much broader than that specifically sought by the warrant. Google actually produced data from a circular area that was approximately 378,278 square meters in area, not a 98,192 square meter box requested by the warrant. (ROA.823-24). This is an area almost four times larger than the area sought to be searched by the warrant.[4] (ROA.123 (stating "the effective range of the geofence was larger than directed in the warrant request due to the manner in which data was requested by the Government.")). Therefore, some

[3] Google estimated that "roughly one-third of active Google users (i.e., numerous tens of millions of Google users) had LH enabled on their accounts" at relevant times. (ROA.136).

[4] For reference, this area is about 1.65 times larger than the United States Capitol which as an area of approximately 230,000 square meters. www.themeasureofthings.com

devices identified may not have been in the actual geofence box sought by the warrant.

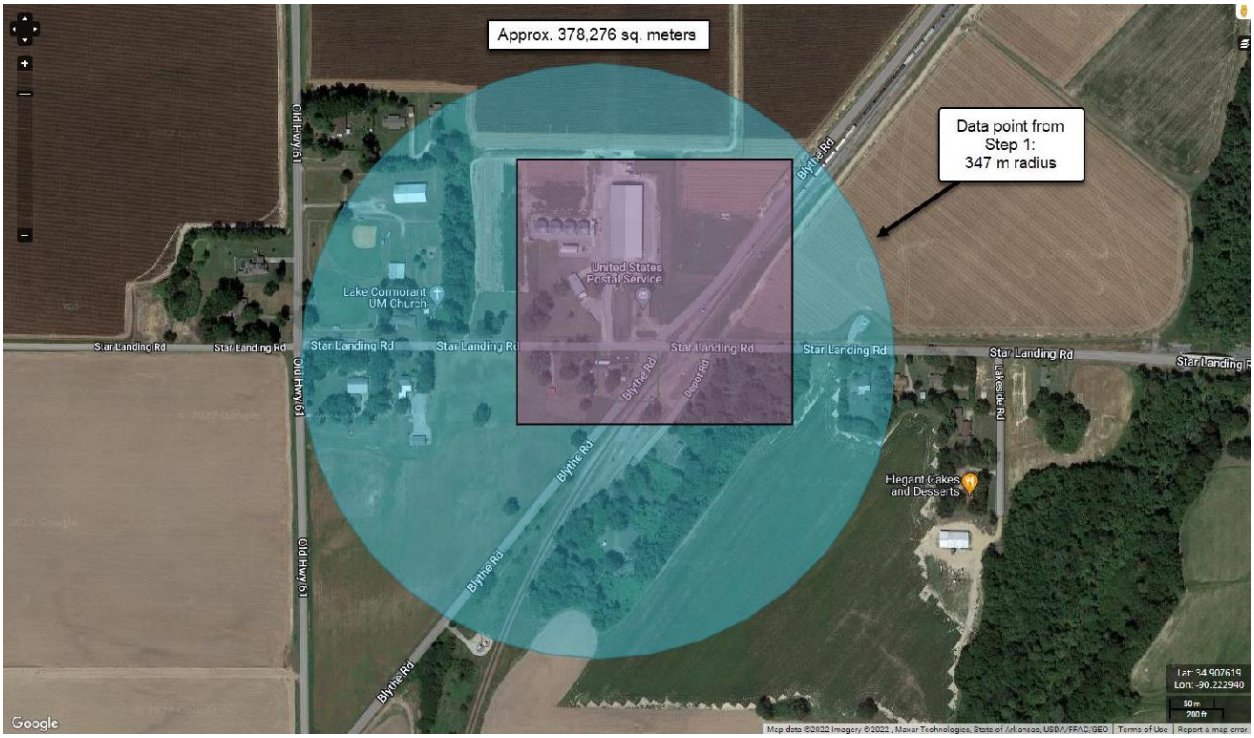
It is also important to note that just because a device is shown in the area of the search, it does not mean with certainty that the device was in fact within the radius of the search:

> 24. The location data points reflected in LH ["Location History"] are estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated LH data point. Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the saved coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. In other words, if a user opens Google Maps and looks at the blue dot indicating Google's estimate of his or her location, Google's goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.
>
> 25. Notwithstanding the confidence interval described above, if a user's estimated location (i.e., the stored coordinates in LH) falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request, even if the shaded circle defined by the 68% confidence interval falls partly outside the radius of the geofence request. As a result, it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius. To provide information about that,

> Google includes in the production to the government a radius (expressed as a value in meters) around a user's estimated location that shows the range of location points around the stored LH coordinates that are believed to contain, with 68% probability, the user's actual location.

(ROA.141).

So, Google provided data concerning at least one account with Location History enabled that could have been anywhere in the following circle:



and possibly outside that circle. (ROA.122). And in total, the search of 592 million accounts identified three devices.

This information was provided in an "anonymized" format which just provided a numerical identifier for the account, the type of account, time stamped location coordinates and the data source:

Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radius (m)
1091690859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091690859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091690859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091690859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091690859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

(ROA.120, 824).

The warrant specifically stated that any additional information obtained from Google after Step 1 would be with "further judicial process." (ROA.114).

2. Step 2

Step 2 of the process required by the warrant was as follows:

> 10. Second, the government reviews the de-identified production version to determine the device numbers of interest. If additional de-identified location information for a device in the production is necessary to eliminate false positives or otherwise determine whether that device is relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request (if authorized in that request).
>
> * * *
>
> 12. Finally, based on the de-identified data produced, the government can compel Google (if authorized in the request) to provide account-identifying information for the device numbers in the production that the government determines are relevant to the investigation. In response, Google provides account subscriber information such as the email address

> associated with the account and the name entered by the user on the account.

(ROA.146). In other words, the government (not a judge) analyzed the "provided records," and demanded that Google "provide additional location history outside of the predefined area for those accounts that the government deemed relevant to determine path of travel;" – all without any additional judicial scrutiny that was promised at the end of Step 1. (ROA.824). Step 2 also, without judicial involvement, increased the time frame for information sought to be produced by 60 minutes before and after the time period permitted by the initial request in Step 1. (ROA.114).

3. Step 3

In Step 3, "upon demand" by the government and not through issuance of an additional warrant, Google produced "de-anonymized" (i.e. specific user) subscriber information. Google produced four hits with the following account information: (1) "2165781.Key.csv", (2) "bleek2004.AccountInfo.txt", (3) "jamarrsmith33.AccountInfo.txt"and (4) permanentwavesrecords.AccountInfo.txt". (ROA.123). This was contrary to the averments in the Matney affidavit that the government would undertake "further legal process" to obtain this data. (ROA.114). Instead, the government, in its sole discretion, chose which accounts to search further and identify.

D. What the government did with the information provided by Google.

Based upon the four results above provided by Google, the government identified Gilbert McThunel and Jamarr Smith as suspects. (ROA.1047-48). The government then accessed the CLEAR database. (ROA.1048). Since the government now had phone numbers for certain suspects, it examined the tower dumps and sent warrants to phone companies for account information. (ROA.1049-51). The government identified defendant Thomas Iroko Ayodele because he was a friend of Smith on Facebook. (ROA.1050). Mathews testified in some detail as to the investigative efforts that flowed from the information provided by Google. (ROA.1056-1196).

In July, 2019, or fifteen (15) months after the crime, the government showed witness Forrest Coffman photo line-ups that included Smith, McThunel and Ayodele. (ROA.1387-90). Despite admitting that Smith did not match his original description as having light skin and reddish facial hair, Coffman identified Smith (but no other defendants) in the line-up. (ROA.1405-06).

In other words, all of the evidence in this case originated from information obtained from Google pursuant to this geofence warrant.

II. RELEVANT PROCEDURAL HISTORY

The government instituted this action by indictment filed on October 27, 2021. (ROA.18; RE 4). Count I of the indictment alleged conspiracy to rob the

Lake Cormorant Post Office by Smith, McThunel, and Ayodele. (ROA.18; RE 4). Count II of the indictment alleged actual robbery of the Lake Cormorant Post Office. (ROA.20; RE 4).

A. Motion to Suppress and ruling thereon.

On November 4, 2022, Smith filed a Motion to Suppress, joined by the other defendants. (ROA.100-159 (motion), 160-86 (memorandum), 187-88 (McThunel Joinder), 193-94 (Ayodele joinder)). The government responded to the Motion to Suppress on November 15, 2022. (ROA.207-36). The defendants filed a rebuttal on December 9, 2022. (ROA.243-57).

The district court conducted a hearing on the Motion to Suppress on January 17, 2023. The government called its two investigators, Matney and Mathews; the defendants called their expert, Spencer McInvaille. (ROA.605-678). From the defendants' perspective, the essential issues for consideration were three-fold: (1) the affidavit in support of the warrant contained a knowing and intentional false statement, or in the alternative, a statement made in reckless disregard of the truth, making it invalid pursuant to *Franks v. Delaware*, 438 U.S. 154, 164–65 (1978); (2) the government did not obtain additional warrants as required by the plain language of the original warrant before obtaining de-anonymized information from Google; thus the search was a warrantless search; and (3) the geofence warrant

simply violated the Fourth Amendment for a variety of reasons, and the good-faith exception did not apply.

McInvaille explained to the District Court, a traditional Google warrant (non-geofence) is used when law enforcement knows the suspect has a Google account and thus seeks information related to that specific suspect's account such as, location history, IP logs, emails, or whatever else relevant to the investigation. (ROA.613-616). However, the difference with a geofence warrant is that law enforcement does not have information about a suspect, but nevertheless seeks, through the geofence warrant, to search all of Google's large bucket of data (called the "Sensorvault") to obtain "anonomized" data. (ROA.613-616). Step 2, mentioned above, allows law enforcement to continue their search of Google data to obtain "contextual data." (ROA.617-618). Whether the geofence is big or small does not matter because Google must search every account to determine which devices fall within the parameters of the box. (ROA.616). McInvaille also explained Google has an error rate with its data. (ROA.616). In the last phase, or Step 3 mentioned above, law enforcement corresponds back with Google to obtain the "de-anonomized" data. (ROA.617-622). It was here that the government obtained four results, but determined that only two were relevant to their investigation.

The district court denied the motion to suppress on February 10, 2023. (ROA.269-293, *United States v. Smith*, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023). The court found that it did not need to resolve any issues concerning constitutionality of the warrant because it ultimately found that the good-faith exception applied. (ROA.279-83; *Smith*, 2023 WL 1930747 at *6-8). The district court did find that the government did not follow the narrowing measures set forth in Step Two of Google's process, and further violated the plain language of the warrant which required "further legal process" (i.e. an additional warrant) before seeking additional information from Google. (ROA.286-88, *Id.* at *10). Nonetheless, the court found that Matney and Mathews's violations were in good-faith. (ROA.288, *Id.*). Finally, the court noted:

> that in November 2018, the time law enforcement applied for the geofence warrant, there was no published case law on the constitutionality of geofence warrants. The Court find that fact – and the novelty of geofence warrants as a whole, particularly at the time of Inspector Matney and Mathews' relevant conduct – to be important in analyzing this case.

(ROA.288, *Id.*).

The district court ultimately applied the good-faith exception articulated in *United States v. Leon*, 468 U.S. 897 (1984). In considering the four *Leon* factors,[5]

[5] Those factors are: 1) the magistrate was misled by information that the affiant knew or should have known was false; 2) the magistrate abandoned his

the district court concluded that, based upon the court's review of the video, Matney had a good-faith basis to believe that a suspect was possibly using a cellular device. (ROA.291, *Smith*, 2023 WL 1930747 at* 11). Next, the warrant was sufficient and met the probable cause and particularity requirement. (ROA.291, *Id.* at *12). Finally, the court believed that Matney and Mathews's consultation with other members of law enforcement and the United States Attorney's office and good-faith belief that the warrant did not require additional court approval of next steps also met the good-faith requirement. (ROA.291-92, *Id.*). The district court found that the lack of published authority as to the validity of geofence warrants was persuasive. (ROA.292-93, *Id.*).

B. Trial

The case was tried to a jury beginning February 21, 2023.

The government called as witnesses Cobbs (the mail truck driver), postal inspector Mathews, three witnesses from various phone companies to authenticate cell phone records, Herbert Dewayne Martin (another postal inspector that performed a photo lineup for Coffman), Coffman (the witness who approached the red Hyundai), some fairly insignificant witnesses having to do with Ayodele's phone numbers and an expert, Christopher Moody.

---

judicial role; 3) the affidavit lacks substantial basis to determine probable cause; and 4) the warrant was facially deficient. *Leon*, 468 U.S. at 914-915.

Moody is employed as a technical surveillance coordinator for the United States Postal Service. (ROA.1432). He was tendered as an expert in the fields of (1) analysis of historical cell phone records for determining location (CSLI), and (2) Google location data for determining location. (ROA.1434-35). Though he had been accepted as an expert in the field of CSLI before, he had never been accepted as an expert in the field of Google location data, i.e. information provided by geofence warrants. (ROA.1437). In voir dire, Moody was unable to establish any of the basic elements of reliability for Google location data:

> Q. All right. So I'm going to turn now to the Google location data history. And you have never testified about that to a jury before?
>
> A. No.
>
> Q. To be even clearer, nobody has ever testified about that to a jury before?
>
> A. I do not know that that is accurate.
>
> Q. You don't know one way or the other?
>
> A. I don't know that your statement is accurate. So I cannot -
>
> * * *
>
> - answer one way or another.
>
> * * *
>
> Q. This is, assuredly, a novel theory about this Google location data; right? It hasn't been around very long?

A. Well, Google hasn't been around very long either. Technology continues to grow, and we keep getting new tools.

Q. Okay. So it -- you've given us your CV in this case; correct?

A. Correct.

Q. That's like your résumé, your qualifications; correct?
A. Correct.

Q. And your CV contains no mention of having Google geofence training; correct?

A. Correct.

Q. There have been no studies or analysis by somebody other than Google or the Government to state that this theory about geofence location is reliable or unreliable; right?

A. Not to my knowledge.

Q. You're not aware of any scientific studies that have tested this theory to determine if it's reliable?

A. Not to my knowledge.

Q. You're not aware of any peer review publications discussing this technology and validating its reliability?

A. Not to my knowledge.

Q. You do not know the error rate?

A. Don't know that there is a current error rate available, no, if that's what you're asking.

> Q. That was going to be my next question. The error rate has never been determined; correct?
>
> A. Neither has the positivity rate, for that matter.
>
> Q. Okay. And this theory has not attained widespread acceptance in the greater scientific community? I'm not talking about just the law enforcement community.
>
> A. Well, proximity analysis in targeted marketing does have widespread acceptance. So there are other communities out there, not necessarily scientific communities, that are using location history from these for targeted marketing.
>
> Q. Okay. I'm asking you about the greater scientific community, though. You're not aware of anything?
>
> A. Yeah.
>
> Q. You're not aware that it's obtained widespread acceptance in the greater scientific community?
>
> A. No. And I don't know what relevant -- or what reason the scientific community would be investigating either.

(ROA.1437-40).

The defendants then asserted a *Daubert* objection which was overruled after a brief bench conference, and Moody was allowed to testify about geofence technology. (ROA.1440-42). He testified in detail about Google's processes for storing data, specifically location data. (ROA.1447-49). He testified as to how Google responded to the geofence warrant (as described above), and how it eventually produced account information associated with Jamarr Smith and Gilbert

McThunel. (ROA.1456-60). He then presented an animation that collected and displayed the locations of the various devices identified by Google at relevant times in the Northwest Mississippi area. (ROA.1461-82; Trial Exhibit G-25).

On cross-examination, Moody admitted that he had not verified the information provided by Google or any of the phone companies, and could not vouch for their accuracy – only that the information was provided. (ROA.1482-83, 1508). He confirmed that Google does not collect location data to solve crimes, but mainly to sell ads provide user services like traffic data. (ROA.1503-04). He testified that Google location accuracy is correct about 60% of the time, and because a device showed up in the geofence did not mean that device was in the geofence – and that there could certainly be devices within the geofence that did not show up in Google's database. (ROA.1505-06).

On February 24, 2023, the jury returned a verdict of guilty as to both counts for all three defendants. (ROA.1640-41).

III. RULINGS PRESENTED FOR REVIEW

The defendants seek review of two rulings:

1. The district Court's denial of the Motion to Suppress. (ROA.269-293, *United States v. Smith*, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023).

2. The district Court's denial of the defendants' *Daubert* motion as to Moody. (ROA.1440-42).

SUMMARY OF ARGUMENT

First, the warrant should have been suppressed because it contained a knowing or reckless material false statement that a suspect in the video was "possibly" using a cellular device. It also contained a material omission of crucial information for the magistrate to make an informed decision: it called for the search of 592 million Google accounts.

In a broader sense, the geofence warrant in this case was so overbroad and unparticularlized that it constituted a modern-day general warrant. It failed to particularize the data to be searched and seized, explicitly granting law enforcement the discretion to choose who to target in Steps 2 and 3. Indeed, the geofence warrant was so overbroad and so unparticularized that it is a modern-day general warrant, to which the good-faith doctrine must not apply. The district court erred in finding that consultation with prosecutors could inoculate law enforcement officers' actions, and the court erred in not finding that suppression would produce deterrent benefits. Suppression is appropriate here to ensure that new technologies do not make an end run around the Fourth Amendment.

As to the government expert on Google location data, he was unaware of studies by anybody other that Google or the government that this theory was reliable. He was not aware of any peer review studies of this theory. He did not know the error rate – or even if there was an error rate. He was not aware that the

theory has widespread acceptance in the greater scientific community – in fact, he did not believe that the scientific community would have reason to investigate the theory. In short, he provided no basic requirements for expert testimony imposed by *Daubert* and should have been excluded.

ARGUMENT and AUTHORITIES

I. Issue I: The geofence warrant was unconstitutional and the good-faith exception does not apply.

A. Standard of review

When considering a district court's ruling on a motion to suppress, this Court reviews factual findings for clear error. *United States v. Davis*, 226 F.3d 346, 350–51 (5th Cir. 2000). This Court reviews legal conclusions regarding the constitutionality of law enforcement action, the sufficiency of the warrant, and the applicability of the good-faith exception *de novo*. *Id.*

B. The affidavit contained a knowing or reckless misrepresentation and omission of material facts.

As the Court is well aware, the Fourth Amendment states "that no warrants shall issue, but upon probable cause." U.S. Const. amend. IV. Law enforcement personnel seeking the issuance of a search warrant must present an affidavit containing facts sufficient to "provide the magistrate with a substantial basis for determining the existence of probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983). This factual showing for probable cause necessarily requires a truthful

showing. *Franks v. Delaware*, 438 U.S. 154, 164–65 (1978) ("when the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a truthful showing."). *Franks* noted that a magistrate will ordinarily have "no acquaintance with the information that may contradict the good-faith and reasonable basis of the affiant's allegation." *Id.* at 169. "Indeed," the Court in *Leon* explained, "it would be an unthinkable imposition upon the magistrate's authority if a warrant affidavit, revealed after the fact to contain a deliberately or recklessly false statement, were to stand beyond impeachment." *Leon*, 468 U.S. at 914 n. 12 (quoting *Franks*, 438 U.S. at 165). Therefore, it is well-established that a person's "Fourth Amendment rights are violated if (1) the affiant, in support of the warrant, includes a false statement knowingly and intentionally, or with reckless disregard for the truth, and (2) the allegedly false statement is necessary to the finding of probable cause." *Winfrey v. Rogers*, 901 F.3d 483, 494 (5th Cir. 2018).

1. The affidavit contained knowing and intentional false statements, or statements with reckless disregard for the truth – and further omitted material information.

The affidavit's most glaring defects were: (1) the false statement that suspects were "possibly" using a cellular device; and (2) the crucial omission that the warrant required Google to search 592 million user accounts.

First, the video used by the government does not show the "robbery suspect .

. . possibly using a cellular device both before and after the robbery occurs." (ROA.114). Further, Matney admitted under oath that he and Mathews included the statement concerning cellular device use in the affidavit because: (1) this language was contained in the form or "go by" that they were using; and (2) Matney believed that use of a cellular device by a suspect was essential for the probable cause showing. (ROA.751-52).

This Court has held that the intentional or reckless omission of exculpatory information from a warrant application may amount to a Fourth Amendment violation. *See Hale v. Fish*, 899 F.2d 390, 400 n. 3 (5th Cir. 1990). An accurate (and indeed exculpatory) statement in the affidavit would be: "Postal Inspectors conducted a detailed review of the video surveillance and it does not show the robbery suspect using a cellular device before or after the robbery occurs."

Matney also acted with reckless disregard for the truth by failing to disclose the true nature and scope of the geofence search – namely that it required the search of 592 million user accounts. These material omissions would have made it abundantly clear to a neutral magistrate that the government lacked probable cause to search anyone's Location History, let alone "numerous tens of millions" of accounts – or any of the defendants' accounts specifically.

The appellants acknowledge that Matney cannot be merely negligent in drafting his affidavit. *Brewer v. Haynie*, 860 F.3d 819, 825 (5th Cir. 2017). Though

an intentional misrepresentation or omission of material facts will certainly suffice, statements and omissions made with a reckless disregard for the truth will invalidate an affidavit and warrant. The Court may infer reckless disregard from circumstances evincing "obvious reasons to doubt the veracity" of the allegations. *St. Amant v. Thompson,* 390 U.S. 727, 731 (1968); *see also United States v. Tomblin*, 46 F.3d 1369, 1377 (5th Cir. 1995) (stating "recklessness can in some circumstances be inferred directly from the omission itself."). As demonstrated above, the statement concerning cellular device usage, and the omission concerning the scope of the search in the affidavit were reckless at best.

In *United States v. Namer*, this Court has held, in combination with the significance of an omission, the officer's mental state of recklessness can also be inferred from "other circumstances surrounding the investigation":

> This recognition that the analytical concepts of materiality and recklessness are often bound together is significant in this case. The misrepresentation was a material one. From that finding of vital materiality and other circumstances surrounding the investigation, we conclude that the misrepresentation was made, at the least, with reckless disregard for the truth.

United States v. Namer, 680 F.2d 1088, 1094 (5th Cir. 1982).

Namer provides a good illustration of what this Court means by "other circumstances surrounding the investigation." There, a state prosecutor and an economic crimes officer obtained a search warrant for the offices of an

unregistered loan broker suspected of offering securities. *Id.* at 1090-91. Before seeking the warrant, the affiants consulted the state's Deputy Commissioner of Securities, who said that the loan instruments, under a novel legal theory, "probably were securities." *Id.* at 1090–92. The search warrant affidavit, however, asserted that the instruments "are classified as securities" without commenting on the novelty of the legal theory used to reach that conclusion. *Id.* at 1091. Ultimately, based on the documents recovered, the broker was convicted of an unrelated federal fraud crime. *Id.*

On appeal, this Court considered whether the misrepresentation about the status of the offerings (securities or not) was material and reckless. This Court easily concluded that misstatement (are securities) and omission (novel legal theory) were material because it was the only part of the affidavit that suggested criminality. *Id.* at 1094. The more difficult question, according to this Court, was determining the affiant's mental state. *Id.* ("The more difficult issue is whether … the misrepresentation was made intentionally or with reckless disregard for the truth."). Based on the materiality of the misstatement and the circumstances surrounding the investigation, this Court inferred that the affiant made the misrepresentation "at the least, with reckless disregard for the truth." *Id.* Because the hypothetical corrected affidavit, purged of the misstatement, no longer

established probable cause, *id.* at 1094-95, this Court reversed and remanded. *Id.* at 1098.

Matney and Mathews included the statement about cellular phone usage *not* because they reasonably believed that a suspect was using a cellular device in conjunction with the crime. Indeed that statement could be made in essentially every criminal case in the era of proliferation of cell phones. It was made because they thought this statement was essential to achieving probable cause to search – and this is clearly reckless at best. Similarly, the omission of the scope of the search was crucial to their obtaining the warrant – and any magistrate would have to know that information to reasonably determine whether to issue the warrant.

2. The false statements/omissions were material.

The second prong of *Franks* requires the Court to examine the affidavit with the false material set to one side and determine "whether the reconstructed affidavit would still support a finding of probable cause." *Kohler v. Englade*, 470 F.3d 1104, 1113 (5th Cir. 2006). To be clear, and as will be discussed in more detail below, it is the defendants' position that the affidavit as originally submitted was completely lacking in probable cause to search the Google 592 million Google accounts at issue. The appellants are presenting this issue without conceding that the application and affidavit established probable cause in the first place.

Here is what the essential part of the reconstructed affidavit would look like

with the "possibly using a cellular device" information from paragraph 16 removed:

- Cellular telephones may be used to determine the location of a device when they have Location History enabled. (ROA.107).
- Google, Inc. collects this data. (ROA.107).
- A robbery occurred at the post office in Lake Cormorant on February 5, 2018 during which Sylvester Cobbs was injured, and where three registered mail sacks were taken. (ROA.108-09).
- A maroon Hyundai Elantra and a white GMC Yukon are believed to be involved in the robbery. (ROA.108-09).
- Matney believes, based upon his experience and training, that cell phones may have been used to plan the crime. (ROA.109).

The following information concerning the scope of the search should have been provided:

- Google does not know which account holders have Location History enabled on their devices. (ROA.117).
- Because this warrant is not identifying any specific user account to be searched, Google must search 592 million user accounts with Location History enabled to comply with this warrant. (ROA.117).

In fairness to the appellants, the Court should also add the following exculpatory fact:

- Postal Inspectors conducted a detailed review of the video surveillance and it does not show the robbery suspect using a cellular device before or after the robbery occurs.

The government may contend that the statement about cellular device usage

before and after the crime in question was supportive of a finding of probable cause to search cellular phones. Indeed, the above information (without the assertion that Matney observed cell phone use during the crime) further reinforces the fact that this was a "bare-bones" affidavit that is insufficient to support probable cause as a matter of law.[6]

In particular, the only assertion of a nexus between this crime and a cell phone is the single statement that Matney believes, based upon experience and training, that cell phones may be used to plan crimes. Similarly, Matney failed to establish a nexus between the robbery and a cellular device with Location History enabled. This is inadequate because the Supreme Court has held that probable cause must be based on individualized facts, not group probabilities. *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). The Fifth Circuit has specifically found that such an assertion, *without more*, is insufficient to establish probable cause. *United States v. Broussard*, 80 F.3d 1025, 1034-35 (5th Cir. 1996) (stating "The so-called 'boilerplate' assertions that [defendant] complains of, which are based on the affiant's extensive experience and training and involve generalizations about the types of evidence that may be found in drug dealers' residences, do not undermine the reasonableness of reliance on the warrant. We do not mean to suggest that these

[6] "'Bare bones' affidavits contain wholly conclusory statements, which lack the facts and circumstances from which a magistrate can independently determine probable cause." *United States v. Satterwhite*, 980 F.2d 317, 321 (5th Cir. 1992). That this was a "bare bones" affidavit in the first place is discussed further below.

types of generalizations, without more, are sufficient to render the officers' reliance objectively reasonable.").

Other jurisdictions have held on very similar facts that assertions that, based upon training and experience, persons tend to use cell phone to plan crimes is totally insufficient to support probable cause. In *United States v. Ramirez*, the court required that the Government make more specific allegations connecting the defendant, the cell phone searched, and the crime charged, instead of relying on generalizations that cell phones tend to contain evidence of crimes. *United States v. Ramirez*, 180 F. Supp. 3d 491 (W.D. Ky., 2016). The court noted that "[p]ossessing a cell phone during one's arrest for a drug-related conspiracy is insufficient by itself to establish a nexus between the cell phone and any alleged drug activity." *Id.* at 495. Similar reasoning should apply to the case at bar because law enforcement obtained data on the defendants' Google accounts where there was a lack of evidentiary nexus in this case, prior to the search," between the cell phone and any criminal activity. *Id.*, citing *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir.1994). In *Ramirez*, the court analyzed an affidavit very similar to the one currently before the Court.

> Detective Petter's statement regarding her training and experience lacks any specific reference to the crime of drug trafficking. It generalizes that 'an individual' may have information on his or her phone that connects him or her to a crime, co-defendants or victims, rather than specifically connecting Ramirez, the crime with which he

> was charged, or any known information about communications made using this particular phone.

Id.[7] The court proceeded to find that the generalizations in the affidavit were insufficient even to trigger the good-faith exception. *Id.* at 496; *see also Commonwealth v. Broom*, 474 Mass. 486, 52 N.E.3d 81 (2016) (search warrant affidavit assertion that the affiant knows from training and experience that "cellular telephones contain multiple modes used to store vast amounts of electronic data" and that, in his opinion, "there is probable cause to believe that the [defendant's] cell phone and its associated accounts … will likely contain information pertinent to this investigation" is a "general, conclusory statement" that "adds nothing to the probable cause calculus"). Here, Matney's affidavit omits a specific assertion or belief that a cell phone was used by a suspect as a tool in this robbery, as the Magistrate Judge typically sees when authorizing a wiretap or search warrant of a specific cell phone in a drug case. Here Matney uses the same generalizations assertion about cell phone use found by the Court in *United States v. Ramirez* to be insufficient to form the basis of probable cause.

In sum, the reconstructed warrant was bare bones, did not support a finding of probable cause, and was invalid at the time it was approved by the United States

[7] Of course, the Court will easily see the additional distinction between affidavits seeking access to a specific, identified person's cell phone and the affidavit at issue in this case: The government could not and did not identify a specific cell phone that it wanted to search – which only compounds the defectiveness of the application.

Magistrate.

C. The warrant was unconstitutional.

The crucial fact about this warrant was that it was not a search of people in the vicinity of the Lake Cormorant post office on the day and times in question; it was a search of all Google users with Location History enabled. Thus, the warrant required Google to conduct an epic dragnet of hundreds of millions of private accounts to determine if any one of them contained data of interest. This is prohibited by the Fourth Amendment.

1. Cell phones and the data contained in them are granted heightened protection by the Fourth Amendment.

The Supreme Court has stated: the "Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' ... [that] allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). Further, the Fourth Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd v. United States*, 116 U.S. 616, 630 (1886). Finally, a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

The Supreme Court has recognized that the "term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. The location records within

cell phones "hold for many Americans the 'privacies of life.' " *Riley*, 134 S.Ct., at 2494–2495 (quoting *Boyd*, 116 U.S. at 630). As such, a "cell phone search would typically expose to the government far more than the most exhaustive search of a house." *Riley*, *573* U.S. at 396–97 (emphasis in original); *see also United States v. Oglesby*, 2019 WL 1877228, at *5 (S.D. Tex. Apr. 26, 2019) (finding that "the protections given to a cell phone must be at least equal to, if not greater than, the protections set out for houses"). The Court in *Riley* found, in short, that cell phones "hold for many Americans the privacies of life" that the court in *Boyd* believed worthy of protection. *Id.* at 403.

There can be no serious contention that a person does not have an expectation of privacy as to their Location History contained in their cell phones, and the fact that this information may be held by a third-party like Google has no effect on that principle. *See Carpenter v. United States*, 138 S.Ct 2206, 2219, 2223 (2018) (holding that the government's access of GPS location information from cell phone providers invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements" and noting that there could soon be more sophisticated systems similarly protected.). *Carpenter* specifically rejected application of the third-party doctrine because cell phone users did not truly voluntarily share their cell phone data with their service provider because "carrying

[a cell phone] is indispensable to participation in modern society." *Id.* at 1220 (citing *Riley*, 573 U.S. at 384-85).

Accordingly, the information contained in and through cell phones can only be searched pursuant to a lawful search warrant, and probable cause receives a heightened level of scrutiny. *Riley*, 573 U.S. at 403.

2. The warrant lacked probable cause and was overbroad.

The Supreme Court defines "probable cause" as "a fair probability that contraband or evidence of a crime will be found in a particular place. *Gates*, 462 U.S. at 238. A warrant is overbroad if the government lacks probable cause to search. *United States v. Sanjar*, 876 F.3d 725, 735 (5th Cir. 2017). Thus, the two aspects of the Fourth Amendment require that (1) a warrant provide sufficient notice of what the agents may seize and (2) probable cause exist to justify listing those items as potential evidence subject to seizure. *Williams v. Kunze*, 806 F.2d 594, 598-99 (5th Cir. 1986).

Here, the warrant did not identify any person about whom it sought information from Google, nor did it only search devices around the Lake Cormorant post office on the date and time in question. It required Google to

search all accounts with Location History enabled (approximately 592 million – an epic dragnet),[8] and then the government decided what to seize.

There can be no doubt that the government did not have probable cause to search hundreds of millions of Google users' accounts. In fact, the government did not have probable cause to search one Google user's account because the government had no identifiable suspects, much less a suspect that it believed was using Location History on his or her phone. It is for this reason, that this new novel investigatory method of a geofence warrant deserves this Court's attention and analysis.

Ybarra requires that there be some evidence of a person's involvement in the suspected crime in order for the Fourth Amendment to allow the seizure of that person – or, by analogy the seizure of that person's things, such as Location History, in which the person has a constitutionally protected expectation of privacy. *Ybarra*, 444 U.S. at 91. So the government cannot simply rely on the generalized statement that "persons who commit crimes use cell phones" to establish probable cause. Probable cause must be based on individualized facts, not group probabilities. *Id.*

[8] This was truly a record-setting search, involving a number of persons that dwarfs the number of persons searched in any other reported criminal opinion. Even "tower dumps," which are the subject of controversy in their own right, impact no more than thousands of persons, and usually only hundreds. *See e.g. United States v. James*, 2019 WL 325231 at * 3 (D. Minn., Jan. 25, 2019) ("hundreds if not thousands" of cell phone users).

Ybarra, as demonstrated by the court in *United States v. Chatrie*, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022)[9] is particularly apposite here. In *Ybarra*, the government obtained a search warrant for any and all persons located in the Aurora Tap Tavern at the time of execution of the warrant because of the belief that somebody therein, plus the bartender "Greg," had narcotics on their person. *Ybarra*, 444 U.S. at 88. The Court found that "[t]here is no reason to suppose that, when the search warrant was issued on March 1, 1976, the authorities had probable cause to believe that any person found on the premises of the Aurora Tap Tavern, aside from 'Greg,' would be violating the law." *Id.* at 90. Nonetheless, Ybarra, a patron in the tavern, was found to have heroin on his person. The Court found that the police might have had probable cause to search the tavern itself, but certainly not Ybarra's person, stating "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." *Id.* at 91 (citing *Sibron v. New York*, 392 U.S. 40, 62–63 (1968)). Further,

> [w]here the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists

[9] *Chatrie* is instructive because it is, to the appellants' knowledge, the only other geofence case in any United States jurisdiction decided on a full record like the instant case.

> probable cause to search or seize another or to search the premises where the person may happen to be.

Id.

The court in *Chatrie* relied on *Ybarra* in finding that the warrant was based on "inverted probable cause:"

> 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. [*Ybarra*, 444 U.S. at 91.] This warrant therefore cannot stand.

Chatrie, 2022 WL 628905 at *24; see also *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 753 (invalidating the geofence warrant because it provided the government "unlimited 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) (citing *Ybarra*, 444 U.S. at 91). Thus, the importance of *Chatrie* is that the court ruled that the government must establish particularized probable cause to search each of the accounts returned (or "seized" in Fourth Amendment parlance) pursuant to Step 1 of the process – which the government could never do.

Indeed, it is difficult to imagine what probable cause could justify searching 592 million devices, but here there was no probable cause at all. The complete absence of probable cause makes the warrant fatally overbroad from the beginning. In other words, the government's effort to search all accounts with Location History enabled rendered the warrant an improper modern-day general warrant. *See Warden v. Hayden*, 387 U.S. 294, 313 (1967) (Douglas, J., dissenting). And the prevention of "dragnet" searches was the purpose of Fourth Amendment.

3. The warrant lacked particularity.

The Fourth Amendment requires that warrants "particularly describe[e]" the place to be searched and the things to be seized. The Supreme Court has interpreted this to require that the warrant particularly describe the place to be searched and the items to be seized so that nothing is left to the discretion of the officer in executing the warrant. *Marron v. United States*, 275 U.S. 192, 196 (1927); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

Here, and as mentioned above, the geofence warrant left it up to Google and the government to decide which users would have their account information searched – the hallmark of an unparticularized warrant. The warrant provided for a three-step process which permitted the government to use its discretion as to what it wanted to have.

Step One of the warrant did not provide clear information on what could be seized and ensnared people outside the geofence box in the warrant. Google did not search only the square geofence in the warrant – instead it searched an area in which it had only a 68% probability that a given device was in that area – meaning that there was a 32% chance that some data provided was not in the geofence at all. Therefore, Google and the government impermissibly used their discretion to decide what to search and which devices to identify as within the search area – all of which was well beyond what a particular warrant permits. No judge signed off on seizure of data for devices outside the square geofence.

Step Two and Step Three gave the government discretion as to which Google users would be the subject of further scrutiny – all without "further legal process" as required by the application and the warrant itself. First, the government required that Google provide additional information outside the scope of Step 1 of the warrant "location history outside of the predefined area . . . . [that] shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account" identified in Step 1. When Google produced the anonymous information regarding devices, the government decided what was "relevant" and then obtained de-anonymized information without returning to the court for an additional authorization. Other courts have denied geofence warrant applications on exactly

this basis as did the court in *Chatrie*. In *In Matter of Search of Info. Stored at Premises Controlled by Google*, the Court stated:

> This Court cannot agree that the particularity requirement is met here by virtue of the proposed geofences being narrowly tailored in a manner justified by the investigation. Attachment B to the proposed warrant, listing the items to be seized, does not identify any of the persons whose location information the government will obtain from Google. As such, the warrant puts no limit on the government'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. A warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize, *Stanford*, 379 U.S. at 485, 85 S.Ct. 506, but the warrant here gives the executing officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the identifying subscriber information, and thus, those persons' location histories.

Matter of Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d at 754.

Therefore, the warrant fails the particularity requirement because the government and Google decided what to seize, and no objective observer could look at the warrant and ascertain which specific accounts the government had authority to search and seize. Indeed, the warrant was useful *because* it was unparticularized – the government had no suspects. Valid warrants do not work that way.

D. The good-faith exception does not apply,

Without reaching the constitutional deficiencies in the warrant, the district court found that the good-faith exception applied. In order for the good-faith exception to the exclusionary rule to apply, "the officer's reliance on the magistrate's probable cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable," and "in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *See United States v. Leon*, 468 U.S. 897, 922–23 (1984). There are four situations in which an officer's reliance on a warrant cannot be objectively reasonable: (1) when the magistrate judge issuing the warrant is misled by information or an omission in an affidavit that the affiant knew, or should have known but for a reckless disregard of the truth, was false; (2) when the magistrate judge wholly abandons the role of neutral arbiter and acts as a rubber stamp to approve a warrant application; (3) when an affidavit supporting a warrant "is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) when the warrant is facially deficient, such as by failing to particularly describe the place to be searched or items to be seized. *Id.* at 914–15, 923, & n.24. The first, third, and fourth *Leon* exceptions apply here.

1. The magistrate was misled by incorrect information in the application.

This element is discussed extensively above. The Supreme Court emphasized in *Herring v. United States*, "an assessment of the flagrancy of the police misconduct constitutes an important step in the calculus of applying the exclusionary rule." *Herring*, 555 U.S. 135, 143 (2009) (quoting *Leon*, 468 U.S. at 911). To have deterrent value, the Court explained, the exclusionary rule should apply to "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* at 144. In other words, the good-faith exception excuses only isolated negligence. *Id.* at 147–48.

The district court erred when it found that Matney's "interpretation of the video could have led him to believe that the assailant's body language was consistent with using a cellphone." (ROA 291-92, *Smith*,2023 WL 1930747 at *11). As discussed above, this was not in fact what Matney and Mathews believed – he included this statement because it was contained in the form or "go by," and he believed that it had to be included to state probable cause. (ROA.752). This is by definition reckless at best. Further, Mathews and Matney did not disclose the scope of the search, and in fairness (particularly due to their extreme unfamiliarity with the nature of the warrant), they had no idea of such a scope.

2. The affidavit was bare bones, and there could be no reasonable belief that it was supported by probable cause.

The good-faith exception offers no refuge to the government where, as here, the warrant is "completely devoid" of probable cause. As discussed above the warrant here is a "bare bones" affidavit to which the good-faith doctrine does not apply. *See United States v. Craig*, 861F.2d 818, 821 (5th Cir. 1988) (referring to the third *Leon* exception as the "bare bones affidavit exception.").

The search of millions of Google users at once renders the warrant so overbroad that no reasonably objective officer could have thought it valid. Indeed, there was no probable cause to search Smith or McThunel's location history, much less *everyone's* location history. Indeed the government did not know Smith or McThunel were in the world (else they would have gotten a warrant for their Location History specifically).

3. The warrant was facially deficient.

The good-faith exception should not apply because the geofence warrant was so "facially deficient" that no objective officer could rely on it. *Leon*, 468 U.S. at 923. It lacked particularity because it sought "unbridled discretion" to search deeply private data of an unlimited number of people, and "the executing officers [could not have] reasonably presume[d] it to be valid." *Id.* Steps 2 and 3 of the warrant "lack[ed] any semblance of objective criteria to guide how officers would narrow the list of users." *Chatrie*, 590 F. Supp. 3d at 934. All law enforcement

officers know that particularity is a constitutional requirement – and unsupervised discretion of law enforcement in what to search clearly violates this requirement. As the Supreme Court stated in *Groh v. Ramirez*, "Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Groh v. Ramirez*, 540 U.S. 800, 563 (2004) (citing *Harlow v. Fitzgerald*, 457 U.S. 800, 818, 19 (1982)).

4. Reliance on review by the United States Attorney's Office does not cure blatant constitutional defects.

The district court placed some emphasis on the fact that Matney consulted with the United States Attorney's Office prior to submitting the warrant. (ROA.291-92, *Smith*, 2023 WL 1930747 at *12). The court erred in giving this weight in its analysis. In *Messerschmidt v. Millender*, the Supreme Court stated, "[B]ecause the officers' superior and the deputy district attorney are part of the prosecution team, their review also cannot be regarded as dispositive." *Messerschmidt v. Millender*, 565 U.S. 535, 554 (2012). Otherwise, each and every warrant could be immunized through attorney review, thereby displacing the need for a neutral and detached magistrate to independently assess the affidavit's probable cause.

Consulting with other officers regarding a warrant highlights "the competitive enterprise of ferreting out crime" and cannot be the single dispositive

factor. *Riley*, 573 U.S. at 382. Consultation with an attorney does not save Matney's and Mathews's unreasonable reliance on this general warrant.

5. Suppression would produce deterrent benefits

The purpose of the exclusionary rule "is to deter future Fourth Amendment violations" and that exclusion is appropriate only when "the deterrence benefits of suppression . . . outweigh its heavy costs." *Davis v. United* States, 564 U.S. 229, 237 (2011). The district court stated that it "struggle[ed] to see any wrongful conduct to deter." (ROA.292, *Smith*, 2023 WL 1930747 at *12).

A geofence warrant is like every other warrant in that it requires probable cause and particularity. Every law enforcement officer is trained to follow these constitutional requirements for obtaining a valid warrant. Both Matney and Mathews were veteran officers with experience obtaining countless warrants. They testified at length at the suppression hearing as to their familiarity with these concepts. (ROA.720-25, 764-68). Though law enforcement commonly tries new investigative techniques, they should not be allowed to mask constitutional shortcomings in the mere novelty of the technique.

Moreover, this was not an isolated instance of negligence – it was part of a troubling growing trend that is just now coming to light. *See Chatrie*, 590 F. Supp. 3d at 906 (finding that use of geofence warrants has grown "exponentially in recent years."). The exclusionary rule plays another important role in deterring

such "recurring or systemic negligence." *Herring,* 555 U.S. at 144. This Court has the power to send a strong message to law enforcement that the Fourth Amendment does not tolerate the proliferation of recurrent abuse of this investigative technique. Law enforcement's conduct in this case is culpable enough to yield "meaningful[l]" deterrence that would be "worth the price paid by the justice system." *Id.* This not "objectively reasonable law enforcement activity," and the Court should deter similar conduct by applying the exclusionary rule. *Leon,* 468 U.S. 919.

6. General warrants do not deserve good-faith protections.

There is no such thing as relying on a general warrant in good-faith. *See Groh,* 540 U.S. at 558. To hold otherwise would invite the kind of "systematic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring*, 555 U.S. at 144; *see also United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring) (finding that when a warrant is void, "potential questions of 'harmlessness'" do not matter); *United States v. Winn*¸ 79 F. Supp. 3d 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions.").

Should this Court find that this geofence warrant was an unconstitutional general warrant, then no balancing test is required. The good-faith doctrine does not apply. While the good-faith exception is relatively new, the prohibition on

general warrants is not. General warrants were a catalyst for the American Revolution and the inspiration behind the Fourth Amendment. And as a result, the Constitution forbids them. Because *Leon* was not decided until 1984—nearly 200 years after the Fourth Amendment outlawed general warrants in this country, fewer courts have had occasion to consider whether the good-faith rule has any bearing on a general warrant. But consistently, courts have found that the good-faith exception is inapplicable to general warrants. *See, e.g., Groh*, 540 U.S. at 558 (finding that a warrant "so obviously deficient" in particularity must be regarded as "warrantless" within the meaning of our case law); *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents ($92,422.57)*, 307 F.3d 137, 149 (3d Cir. 2002) (finding general warrants to be "so plainly in violation of the particularity requirement that the executing officers could not have reasonably trusted in its legality"); *United States v. George*, 975 F.2d 72, 77-78 (2d Cir. 1992); *United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988); *United States v. Crozier*, 777 F.2d 1376, 1381 (9th Cir. 1985); *see also United States v. Minnick*, 2016 WL 3461190, at *5 (D. Md. June 21, 2016) (considering the good-faith exception's applicability to suppression after rejecting the claim that what issued was a general warrant); *Winn*, 79 F. Supp. 3d at 926; *United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 445-46 (E.D. Pa. 2007) ("[W]e read Third Circuit precedent to prohibit the use of the good-faith exception in connection with general

warrants." (citing *United States v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982) ("It is beyond doubt that all evidence seized pursuant to a general warrant must be suppressed.")))).

The geofence warrant here was a general warrant. It "did not describe in 'specific and inclusive generic terms' what was to be seized," but rather "vest[ed] the executing officers with 'unbridled discretion' to search for and seize whatever they wished.'" *Fleet Mgmt. Ltd.*, 521 F. Supp. 2d at 443. It provided no particularized probable cause for the "all persons" search in Step 1, and it granted law enforcement "unbridled discretion" to search and seize more data in Step 2 and Step 3. (ROA.824). If the Fourth Amendment means anything, it is a safeguard against this type of dragnet search and discretionary seizure of private data. It does not contemplate this sort of general rummaging, even if conducted by computers. On the contrary, geofence warrants are the digital equivalent of the very thing the Fourth Amendment was designed to prevent.

E. Essentially all of the evidence against the defendants in this case is the fruit of the initial unconstitutional searches and must therefore be suppressed.

"Under the fruit-of-the-poisonous tree doctrine, all evidence derived from the exploitation of an illegal search or seizure must be suppressed, unless the government shows that there was a break in the chain of events sufficient to refute the inference that the evidence was a product of a Fourth Amendment violation."

United States v. Martinez, 486 F.3d 855, 864 (5th Cir. 2007) (quoting *United States v. Rivas*, 157 F.3d 364, 368 (5th Cir. 1998)) (internal quotation marks omitted). Here, the government did not have the identity of any of the defendants until after the geofence warrant was obtained; therefore, all of this derivative evidence must be suppressed. *See Segura v. United States*, 468 U.S. 796, 804 (1984) (holding that evidence later discovered and found to be derivative of an illegal search must be suppressed as fruit of the poisonous tree.).

It is indisputable in this case that the information provided by the geofence warrant was essential in the government's investigation of this robbery moving forward, particularly the identification of the defendants. Therefore, essentially all information in this case should be suppressed a fruit of the poisonous tree.

II. Issue II: Moody's testimony was inadmissible pursuant to *Daubert*.

A. Standard of review

The Court must "review the admission of expert testimony for an abuse of discretion," and it "will be upheld unless it was 'manifestly erroneous.'" *United States v. Hodge*, 933 F.3d 468, 477 (quoting *United States v. Valencia*, 600 F.3d 389, 423 (5th Cir. 2010)).

B. *Daubert* standards

The Court is well aware of the framework for determining the admissibility of expert testimony under Rule 702 of the Federal Rules of Evidence. *Daubert v.*

Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). A trial judge faced with a proffer of expert testimony must make a "preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue." *Id.* 592-93. Expert testimony is only admissible if it is both relevant and reliable. *Pipitone v. Biomatrix, Inc.*, 288 F.3d 239, 244 (5th Cir. 2002) (quoting *Daubert*, 509 U.S. at 597).

The party offering the expert testimony bears the burden of proof by a preponderance of the evidence as to the reliability and sufficiency of the opinion; here, the government. *Mathis v. Exxon Corp.*, 302 F.3d 448, 459-60 (5th Cir. 2002). Further, mere conclusory allegations do not satisfy the government's burden of proof. *Moore v. Ashland Chem., Inc.*, 151 F.3d 269, 277, 78 (5th Cir. 1998).

Further, "a district court must create a record of its *Daubert* inquiry and 'articulate its basis for admitting expert testimony.'" *Carlson v. Bioremedi Therapeutic Sys., Inc.*, 822 F.3d 194, 201 (5th Cir. 2016) (quoting *Rodriguez v. Riddell Sports, Inc.*, 242 F.3d 567, 581 (5th Cir. 2001)). District courts are to make a preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue. *Id.* at 199. That finding must be on the record. *Kuhmo Tire, Ltd. v. Carmichael*, 526 U.S. 137, 149 (1999).

Daubert provides a list of factors for judges to consider when evaluating the reliability of expert testimony. *Daubert*, 509 U.S. at 593-95. The factors include whether or not the expert's theory or technique: (1) has or can be tested; (2) has been subjected to peer review; (3) has a known or potential rate of error; and (4) has been generally accepted in the scientific community. *Pipitone*, 288 F.3d at 244 (quoting *Daubert*, 509 U.S. at 593-95). The test is a "flexible" one, and the list is illustrative and not exhaustive. *Kumho Tire*, 526 U.S. at 141. As such, the judge serves as a "gatekeeper" and this role requires judges "to make certain that an expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field." *Pipitone*, 288 F.3d at 244 (quoting *Kumho*, 526 U.S. at 152).

C. Moody's testimony

Moody was called to testify about two generally related, but significantly different areas: (1) historical cellular site analysis (commonly known as "CSLI");[10] and (2) Google location (a/k/a "geofence") analysis. (ROA 1268).

The defendants acknowledge that this Court has accepted historical cellular site analysis in the past as the subject of expert testimony. *United States v. Schaffer*, 439 F. App'x 344, 347 (5th Cir. 2011). However, this is not determinative

[10] "Cell Site Location Information."

of the admissibility of Moody's testimony – each expert must be subject to an independent judicial inquiry. *See United States v. Godinez*, 7 F.4th 628, 637-38 (7th Cir. 2021) (finding district court abused discretion by allowing expert to testify by relying on another court's acceptance of the expert in other cases and not conducting its own inquiry). Moody admitted that CSLI technology had not been validated outside of the law enforcement community by the greater scientific community (and that law enforcement had a vested interest in it being valid – i.e. law enforcement is not an independent and unbiased source of validation). (ROA.1261). This has been an ongoing criticism of this evidence. *See* Victoria Saxe, *Junk Evidence: A Call to Scrutinize Historical Cell Site Location Evidence*, 19 U.N.H.L. Rev. 133 (2020).

Google location analysis on the other hand has not been the subject of expert *trial* testimony in *any* court other than this case.[11] Indeed Moody had no Google

[11] Respectfully, the district court and the government were incorrect in citing *State v. Pierce*, 222 A.3d 582, 589 (Del. Super. Ct. 2019) for the proposition that "the Superior Court of Delaware has allowed expert testimony as to Google location data." *Smith*, 2023 WL 2703608 at *5. *State v. Pierce* was *not* a geofence case and did not involve the same methodology at issue in this case. That case involved downloading location data from the defendant's actual cellphone in possession of the government. *Pierce*, 222 A.3d 584-85. That did not occur here.

The difference is similar to that where an accident reconstructionist testifies that point of impact on a vehicle was to the rear by looking at damage to the rear of that vehicle; versus an accident reconstructionist coming up with a methodology for determining which of the over 300 million vehicles in North America sustained rear-end damage between 5pm and 6pm on February 5, 2018.

geofence training. (ROA.1269). He had never testified to this theory before, and never been accepted by an expert in any court as to this theory. He was unaware of studies by anybody other that Google or the government that this theory was reliable. He was not aware of any peer review studies of this theory. He did not know the error rate – or even if there was an error rate. (ROA.1272). He is not aware that the theory has widespread acceptance in the greater scientific community – in fact, he did not believe that the scientific community would have reason to investigate the theory. (ROA.1272-73).

D. Moody did not meet even the most basic *Daubert* requirements.

Though no single factor is dispositive of reliability and acceptance of a theory, here the government presented no basic evidence that satisfied a single *Daubert* factor as to the reliability and acceptance of geofence location data. Indeed, the only scientific support for the theory presented by Moody was that *he* said it was reliable – a classic case of *ipse dixit* of the expert, which is a well-established basis for excluding such evidence. *See Gen. Elec. Co. v. Joiner*, 522 U.S. 136, 146 (1997) (stating "nothing in either Daubert or the Federal Rules of Evidence requires a district court to admit opinion evidence that is connected to existing data only by the *ipse dixit* of the expert.").[12]

[12] The Court has to be concerned, and the district court should have recognized, that this was by all accounts *the first* time an expert was testifying in front of a jury concerning geofence Google location analysis – and the government

Moore v. Ashland Chemical is on point. There, the plaintiff presented Dr. Daniel E. Jenkins to testify that the plaintiff sustained pulmonary injuries from chemical exposure. However, the Court found:

> Dr. Jenkins cited no scientific support for this theory. None of *Daubert 's* factors to assess whether the opinion was based on sound scientific principles was met. Dr. Jenkins's theory had not been tested; the theory had not been subjected to peer review or publication; the potential rate of error had not been determined or applied; and the theory had not been generally accepted in the scientific community. In sum, Dr. Jenkins could cite no scientific support for his conclusion that exposure to any irritant at unknown levels triggers this asthmatic-type condition. Under the *Daubert* regime, trial courts are encouraged to exclude such speculative testimony as lacking any scientific validity.

Moore, 151 F.3d at 279. This is exactly the same situation as with Moody, and the district court should have excluded his testimony.[13]

In sum, the government did not satisfy even the most basic requirements of *Daubert* when presenting Moody, and the district court erred when it allowed him to testify.

---

knew it. The government' failure to do no more than it did to properly qualify Moody and validate his opinions, especially in a criminal case like this, is a real failure of the government's burden and should not be rewarded.

[13] As one treatise has stated: "Where the proffered expert offers no tests or testable theory to support his or her stated conclusion, personal opinion, not science, is testifying, and the proffered testimony is inadmissible as a matter of law under Fed. R. Evid. 702. *33A Fed. Proc., L. Ed.* Theory can or has been tested, § 80:217 (2023).

CONCLUSION

For the reasons stated above, this Court should reverse the judgment of the district court denying the motion to suppress, and order that the district court dismiss the indictment. Additionally, the Court should reverse the decision of the district court permitting Moody to testify, and render judgment in favor of the defendants/appellants.

Respectfully submitted,

JAMARR SMITH

/s/ Goodloe T. Lewis
GOODLOE T. LEWIS, MSB #9889
CJA appointed Federal Public Defender
1305 Madison Avenue
Post Office Drawer 668
Oxford, Mississippi 38655
(662) 234-4000 (telephone)
glewis@hickmanlaw.com

GILBERT MCTHUNEL

/s/ Paul Chiniche
PAUL CHINICHE, MSB #101582
CJA appointed Federal Public Defender
265 N Lamar Blvd., Suite W
Oxford, Mississippi 38655
(662) 234-4319 (telephone)
pc@chinichelawfirm.com

THOMAS AYODELE

/s/ William F. Travis
WILLIAM F. TRAVIS, MSB #8267
CJA appointed Federal Public Defender
8619 Highway 51 N.
Southaven, Mississippi 38671
(662) 393-9295 (telephone)
bill@southavenlaw.com

CERTIFICATE OF SERVICE

I, Goodloe T. Lewis, hereby certify that on November 21, 2023, the Appellant's Brief was served via ECF to lead trial counsel for Plaintiff/Appellee, Assistant U.S. Attorney Robert Mims at robert.mims@usdoj.gov. I also certify that: 1) all privacy redactions have been made pursuant to 5th Cir. Rule 25.2.13; 2) the electronic submission is an exact copy of the paper documents pursuant to 5th Cir. Rule 25.2.1; and 3) the document has been scanned for viruses with the most recent version of Norton Anti-virus and is free of viruses. Further, I certify that I sent a paper copy via regular mail to Defendants/Appellants Jamarr Smith, Gilbert McThunel and Thomas Iroko Ayodele and District Judge Sharion Aycock.

/s/ *Goodloe T. Lewis*
GOODLOE T. LEWIS

CERTIFICATE OF COMPLIANCE

Pursuant to 5th Cir. R. 32.2.7(c), the undersigned certifies this brief complies with the type-volume limitations of 5th Cir. R. 32.2.7(b).

1. Exclusive of the exempted portion in 5th Cir. R. 32.2.7(b)(3), this brief contains 12,937 words.

2. This brief has been prepared in proportionally spaced typeface using Microsoft Word 2010 in Times New Roman typeface and 14 point font size.

3. The undersigned understands a material misrepresentation in completing this certificate, or circumvention of the type-volume limits in 5th Cir. R. 32.2.7, may result in the Court's striking the brief and imposing sanctions against the person signing the brief.

/s/ *Goodloe T. Lewis*
GOODLOE T. LEWIS