IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

23-60321

UNITED STATES OF AMERICA,
Plaintiff-Appellee

v.

JAMARR SMITH, THOMAS IROKO AYODELE,
GILBERT MCTHUNEL, II
Defendants-Appellants

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
NDMS CRIMINAL NO. 3:21-CR-107

BRIEF OF APPELLEE

CLAY JOYNER
United States Attorney

ROBERT J. MIMS
MS Bar No. 9913
Assistant United States Attorney

CLYDE MCGEE
MS BAR No. 102229
Assistant United States Attorney
Northern District of Mississippi
900 Jefferson Avenue
Oxford, Mississippi 38655
662-234-3351

CERTIFICATE OF INTERESTED PERSONS

The undersigned counsel of record certifies that the Government is unaware of any persons who might have an interest in the outcome of this case other than:

1. Honorable Sharion Aycock, United States District Court Judge, Northern District of Mississippi;
2. Clay Joyner, United States Attorney for the Northern District of Mississippi;
3. Robert J. Mims, Assistant United States Attorney, Attorney for Plaintiff-Appellee;
4. Clyde McGee IV, Assistant United States Attorney, Attorney for Plaintiff-Appellee;
5. Defendant-Appellant Jamarr Smith;
6. Goodloe T. Lewis, CJA Counsel for Defendant-Appellant Jamarr Smith;
7. Defendant-Appellant Gilbert McThunel, II;
8. Paul Chiniche, CJA Counsel for Defendant-Appellant Gilbert McThunel, II;
9. Defendant-Appellant Thomas Iroko Ayodele;
10. William F. Travis, CJA Counsel for Defendant-Appellant Thomas Iroko Ayodele.

These representations are made so that the judges of this Court may evaluate possible disqualification or recusal.

/s/*Robert J. Mims*
ROBERT J. MIMS, MSB No. 9913
Assistant United States Attorney
Attorney for Plaintiff-Appellee

/s/*Clyde McGee IV*
CLYDE McGEE IV, MSB No. 102229
Assistant United States Attorney
Attorney for Plaintiff-Appellee

STATEMENT REGARDING ORAL ARGUMENT

Although the facts and legal arguments are adequately presented in the briefs and record, given the novel nature of geofence warrants, the government does not oppose the appellants' request for oral argument.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

JURISDICTIONAL STATEMENT

The Fifth Circuit Court of Appeals has jurisdiction over final orders of the United States District Court for the Northern District of Mississippi, pursuant to Title 28, United States Code, Section 1291.

STATEMENT OF THE ISSUES

The District Court properly denied the appellants' Motion to Suppress the geofence warrant. The warrant was constitutional, there were no false statements or omissions in the application for the warrant, and agents relied upon the warrant in good faith.

Furthermore, the District Court did not abuse its discretion nor err, manifestly or otherwise, in allowing the expert testimony of Christopher Moody. The appellants' *Daubert* challenge was properly denied.

STATEMENT OF THE CASE

On February 5, 2018, three individuals, acting together, robbed Sylvester Cobbs of U.S. Mail matter, money, and property at the Lake Cormorant Post Office in Lake Cormorant, Mississippi. (ROA.483-484, 560, 1027-1030, 1133-1134) The Lake Cormorant Post Office is open mornings, closing at noon. (ROA.1026, 1125) Cobbs is a contract carrier for the Postal Service who ran an afternoon route collecting mail from post offices in Tunica and DeSoto Counties to take to the distribution center in Memphis. (ROA.1021-1022) Lake Cormorant was the fourth of five stops he would make along his route. (ROA.1022)

The mail collected by Cobbs included registered mail bags (ROA.1022-1023) which contain the cash receipts collected by the Postal Service from the sale of items such as money orders and stamps. (ROA.1127-1128) When Cobbs stopped at Lake Cormorant, he had already collected registered mail bags from three other post offices along his route. (ROA.1027, 1041)

On February 5, 2018, at approximately 5:20 p.m., Cobbs arrived at the Lake Cormorant Post Office in a U.S. Mail truck and backed up to the back door, where he would retrieve mail bags waiting for him inside the post office. (ROA.1024, 1026-1028) Before he could open the back door to the post office, an unknown individual, later determined to be Gilbert McThunel, came out from hiding to rob Cobbs of the registered mail bags that Cobbs had already collected. (ROA.1028-1030) When

Cobbs did not cooperate, McThunel struck Cobbs multiple times with a handgun, threatened to kill him, then grabbed the registered mail bags from Cobbs' truck. (ROA.1028-1030) Cobbs pulled the truck to the front of the building and called for help. (ROA.1030) The loss to the Postal Service was $60,706. (ROA.1132)

When the Postal Inspection Service began investigating, agents found a security camera on a farmer's shop across the street, which had recorded the attack.[1] (ROA.479, 558) From a review of the footage, agents began to understand the events of the robbery. (ROA.482-484) Prior to the robbery, the video depicts a white SUV driving past the side of the post office opposite the attack. (Exhibit "G-1," 5:45 minute mark to 6:01 minute mark) (ROA.487, 560) The SUV leaves the picture then returns a short time later, stopping briefly to let McThunel out of the vehicle. (Exhibit "G-1," 6:39 - 6:56) (ROA.487, 560) The SUV drives off and McThunel walks behind the post office where he hides behind the building. (Exhibit "G-1," 6:39 - 9:50) While waiting, video footage shows McThunel with his left arm and hand held up to his ear for multiple minutes, consistent with talking on a phone. (Exhibit "G-1," 6:50 - 9:50) (ROA.488, 563-564) Phone records confirmed that McThunel was indeed on the phone. (ROA.574, 576) McThunel received a call at 5:16 p.m. from Jamarr Smith, another participant in the robbery, who was acting as

[1] The security camera footage is trial exhibit "G-1." The timer on the security footage starts at 00:00, so that references to times on the security footage are not to the specific time of the robbery, but rather to a time frame on the footage itself.

a lookout, and the two engaged in a 5 minute, 42 second phone call.[2] (ROA.574, 576-577)

When Cobbs arrived, McThunel attacked Cobbs as described above, then grabbed the registered mail bags from Cobbs' truck. (Exhibit "G-1," 11:15 - 13:10) Part of the confrontation between McThunel and Cobbs is obscured by Cobbs' truck, but it is clear from the video that McThunel struck Cobbs multiple times, driving him to the ground. (Exhibit "G-1," 12:20 - 13:05) As Cobbs pulled the truck to the front of the building, McThunel paced behind the building for a short time, eventually exiting the camera's view to the left. (Exhibit "G-1," 13:10 - 13:40) Before leaving the camera's view, McThunel set the registered mail bags down and appearred to reach briefly into his pocket. (Exhibit "G-1," 13:25 - 13:38) While it is difficult to see exactly what he is doing, it appears McThunel is possibly pulling out a phone to check for a text message or to see who is calling. (Exhibit "G-1," 13:34) McThunel walked out of view for several seconds, then returned to the back of the post office. (Exhibit "G-1," 13:38 - 13:57) (ROA.499) McThunel placed the registered mail bags on the ground and squatted down, and while it is again difficult

[2] Appellants state that the video does not show the assailant using a phone. Appellants aver that an accurate statement in the affidavit would have been that "a detailed review of the video…does not show the robbery suspect using a cellular device…." To the contrary, the video, before and after the robbery, shows the assailant "possibly using a cellular device" as stated in the search warrant affidavit. For the portion before the robbery, there is no other explanation for why the assailant held his hand to his ear for multiple minutes. Phone records confirmed the affiant's assertion to be correct.

to see what he is doing as he is squatting, it appears that he was checking or texting on his phone. (Exhibit "G-1," 13:57 - 14:07) (ROA.499-500, 563-564) McThunel then stood and walked out of view again. (Exhibit "G-1," 14:07 - 14:21) (ROA.500) Shortly thereafter, the white SUV returns, driving in the direction that McThunel was last seen walking. (Exhibit "G-1," 18:30 - 18:45) (ROA.502) After presumably picking up McThunel, the white SUV drives back past the post office, leaving the scene for good. (Exhibit "G-1," 20:43 - 20:55)

Agents noticed another vehicle of interest on camera during the robbery. (ROA.495-496, 560) Shortly after Cobbs pulled into the post office lot, a red Hyundai Sonata, following from the same direction as Cobbs' truck, approached the intersection in front of the post office, slowed to a brief, but noticeable stop in the intersection, then completed a right hand turn, travelling across the railroad tracks before making a u-turn and returning in the direction from which it had come. (Exhibit "G-1," 10:27 - 11:05) (ROA.495-496, 560) A little over a minute later, as the attack on Cobbs is occurring, the same car approached the intersection in front of the post office, stopped in the intersection again, before making a u-turn in the intersection and pulling in front of a building across the street from the front of the post office. (Exhibit "G-1," 12:20 - 12:40) (ROA.497) The car stopped for several seconds in front of the building, then backed up towards the post office, where it sat throughout the remainder of the attack. (Exhibit "G-1," 12:40 - 13:20) (ROA.497)

As Cobbs pulled to the front of the building, the car pulled forward and left the scene. (Exhibit "G-1," 13:15 - 13:20) (ROA.497-498)

An eyewitness in the area had seen the red Hyundai Sonata sitting in the area near the post office at the time of the robbery[3] and approached the driver to ask if he needed assistance. (ROA.1380) This witness later identified the driver of the red Sonata as Jamarr Smith, both during a photo lineup (after agents had developed Smith, McThunel, and Ayodele as subjects of the investigation) and while testifying at trial. (ROA.1363-1366, 1388-1389, 1390-1391)

Agents were unable to identify any suspects from the video, so in November 2018, Todd Matney of the Postal Inspection Service prepared an affidavit seeking a geofence search warrant, with assistance from Postal Inspector Stephen Mathews. (ROA.480-481, 560) The geofence warrant, directed to Google, sought information pertaining to any Google accounts located within a described geographical "box" between 5:00 pm and 6:00 pm, central time, on February 5, 2018. (ROA.112) The "box," drawn with specific latitude and longitude coordinates, encompassed the Lake Cormorant Post Office and a portion of the road to the front and side where the

[3] In their brief, appellants mistakenly assert that the eyewitness saw the red Hyundai "driving around" "somewhat earlier in the day." This is incorrect. The eyewitness saw the Hyundai at the time the robbery was occurring, sitting in front of an abandoned store across the intersection from the post office. (ROA.1380) Appellants also said the eyewitness initially described the driver as having "reddish hair," when actually, the eyewitness described the driver as having a "reddish goatee." (1400-1401) Regardless, the eyewitness later clearly identified Jamaar Smith as the driver of the Hyundai. (ROA.1363-1366, 1388-1389, 1390-1391)

vehicles of interest were seen travelling. (ROA.112) The warrant set forth a three-step process for obtaining information from Google, which was consistent with Google's requirements at that time.[4] (ROA.114) Google would first provide agents a list of Google accounts found within the "box" during the specified time frame, with the devices only identified by an anonymous numerical identifier, without any content concerning the user of the device (Step One). (ROA.114) For those accounts that agents determined relevant to the investigation, Google would provide additional location history outside of the "box" to determine path of travel (Step Two). (ROA.114) This additional location information would not exceed 60 minutes either side of the first and last timestamp associated with the account in the initial dataset. (ROA.114) Finally, for those accounts deemed relevant following Step Two, Google would provide subscriber information to the agents (Step Three). (ROA.114)

The affidavit and application for a warrant were submitted to Magistrate Judge Roy Percy (ROA.503), who issued the warrant on November 8, 2018. (ROA.113) The agents followed the steps set forth in the warrant. (ROA.503-506) In response to Step One, Google provided information showing that three devices[5] had been located within the "box" during the specified time. (ROA.504, 568) Two of the devices, identifiers ending in 859 and 768, registered multiple times between 5:22

[4] Google policy required extra steps or layers that are not actually required by law.
[5] Appellants inadvertently state multiple times in their brief that Google returned four devices in Step One, but it was actually only three devices, as described herein.

and 5:30. (ROA.568-569) One of the devices, identifier ending in 479, only registered once, at 5:58. (ROA.8-9) Agents determined that devices 859 and 768 were relevant and that device 479 was not. (ROA.569-573) Agents followed the process set forth in the warrant for steps two and three, eventually finding out that devices 859 and 768 belonged to Smith and McThunel. (ROA.505, 570-573) Agents later obtained additional court-authorized search warrants for Smith's and McThunel's Google accounts, seeking location and other information pertaining to their accounts between January 1, 2018, and April 30, 2018. (ROA.573) Further investigation, including phone records pertaining to Smith and McThunel, revealed Thomas Iroko Ayodele as a potential suspect. (ROA.574) Agents determined that Ayodele owned a white SUV that appeared to match the SUV seen on camera. (ROA.575) Agents further determined that McThunel owned a red Hyundai Sonata that appeared to match the red Sonata seen on camera and in which Smith was identified by an eyewitness as being in the vicinity of the post office at the time of the robbery. (ROA.575) Other location information obtained through warrants issued to phone companies showed the three appellants travelling from Batesville (their hometown) to Lake Cormorant and back on the afternoon of the robbery and phone records further confirmed multiple communications between appellants throughout the time immediately before, during, and after the robbery. (ROA.573-574)

Prior to trial, appellants filed a Motion to Suppress all evidence obtained through the geofence warrant. (ROA.100-159) Following a lengthy hearing on January 31, 2023, the district court denied appellants' motion in an extensive memorandum opinion that held the agents acted in good faith reliance on the issued geofence search warrant. (ROA.263, 268-293)

During the suppression hearing, appellants called Spencer McInvaille as an expert in the field of digital forensics and geolocation analysis (including Google location data). (ROA.609-610) McInvaille provided expert testimony to the court on Google location data, though he provided no studies or peer reviewed documents. (ROA.610-624)

McInvaille, appellants' own Google geolocation expert, admitted that the Google data proved that two devices were on scene around the Lake Cormorant Post Office on the date and time in question:

> Mr. Mims: …So you don't disagree that Smith and McThunel were present at the Lake Cormorant post office at 5:30 p.m. that evening, do you?
>
> Mr. McInvaille: I can't say them physically, but an account that you have associated with them, yes.
>
> Mr. Mims: Okay. Their devices were present, weren't they?
>
> Mr. McInvaille: The devices with those accounts, yes.

(ROA.857)

On March 10, 2022, the Government designated Christopher Moody as an expert and provided notice to appellants that Moody would be used to show "the location of defendants and their cellular phones before, during and after the time of the subject robbery." (ROA.404) His curriculum vitae was also provided. (ROA.405-406)

On February 3, 2023, the Government provided a supplemental expert disclosure in compliance with recently revised Rule 16 of the Federal Rules of Criminal Procedure which stated in detail Moody's anticipated testimony. (ROA.407-410) Though appellants were noticed about Moody as early as March 2022, during the 11 months prior to trial, appellants did not file a *Daubert* motion to exclude Moody's testimony.

Trial commenced on February 21, 2023. (ROA.330) During the trial, the government called Moody as an expert witness in the field of cell site and geolocation/historical location records, who presented testimony to the jury, along with animated maps, showing the location and movement of the appellants' cell phones before, during, and after the robbery, utilizing information obtained from the geofence warrant and historical cell site data. (ROA.1276-1313) When Moody was offered as an expert witness, appellants raised a *Daubert* objection. (ROA.1273-1275) The objection was overruled and Moody was accepted as an expert witness. (ROA.1276)

Before being tendered as an expert, Moody offered testimony as to his qualifications. Moody is a technical surveillance coordinator for the Postal Inspection Service. (ROA.1265) Moody testified about his expertise in GIS mapping and communications intercept, having worked with phone records and geolocation records from Google and other social media platforms for the last 13 years. (ROA.1265) Moody discussed his training from the FBI Task Team, NATIA, PenLink, CellHawk and other providers in phone analytics, noting that he receives training yearly. (ROA.1265-1266) Moody also listed his extensive educational background. (ROA1266) Moody further testified that he had previously been accepted and testified as an expert in the Western District of Tennessee. (ROA.1267) Appellants questioned Moody concerning his qualifications and asked Moody about cell phone technology, Google location history, and the recency of its use. (ROA.1268-1273) Appellants' subsequent *Daubert* objection was overruled. (ROA.1273-75)

Following his acceptance as an expert witness, Moody testified about cell phone data including cell sites and cell tower sectors, giving detailed testimony about azimuth degrees in phone records and how phones communicate with the towers. (ROA.1276-1279) Moody also discussed Google geolocation data and how Google geolocation data is collected from customers of Google. (ROA.1281-1284) Moody explained how Google collects WIFI, GPS, and cell site data on customers

and how Google provides this data to law enforcement through search warrants. (ROA.1281-1284)

Moody then offered testimony concerning the PLX and CellHawk programs. (ROA.1286) Moody loaded the cell phone records into PLX which resulted in the creation of maps of what cell site the phones hit at certain times. (ROA.1286-1289) Moody further testified that he received Google records, including GPS coordinates and accuracy radii, and loaded them into the CellHawk mapping program. (ROA.1289-1290) Moody explained that he received the full historical location information records, for two of the accounts, from Google in this case (through a separate search warrant). (ROA.1291) Moody, through maps and phone records from the phone companies, showed the jury how all three appellants' cell phones were located in the immediate vicinity of the Lake Cormorant Post Office at the time of the robbery and also showed the appellants' path of travel from Batesville to Lake Cormorant and back. (ROA.1295-1309)

Moody, again utilizing maps, showed the jury the results of the historical location data from Google for Smith's and McThunel's devices. (ROA.1295-1297) Moody explained how the Google location data, like the cell site data, also depicted appellants' devices in the immediate vicinity of the Lake Cormorant Post Office at the time of the robbery, as well as their travel from Batesville to Lake Cormorant

and back. (ROA.1295-1309) Moody explained to the jury that the phone data and the Google data matched and appeared to be the same devices. (ROA.1302, 1309)

Appellants cross-examined Moody extensively on the issue that Moody was not vouching for the reliability or accuracy of the Google records and phone records, specifically cell sites, cell towers and GPS data. (ROA.1315-1316) Appellants' counsel pointed out that the phone did not have to be in the cell site cones provided in the maps, but rather, the phone could be beyond the outer arc of the cone. (ROA.1327) Moody clarified that the shaded area cell site cones were used to identify who was using that sector of the towers. (ROA.1327) Appellants' counsel further examined Moody about potential inaccuracies such as weather and terrain features. (ROA. 1327-1330) Finally, appellants' counel questioned Moody about the accuracy of Google records and how Google wants to be accurate 68 percent of the time. (ROA.1338)

Following a four-day trial, the jury returned a verdict of guilty against all three appellants. (ROA.330-331) Appellants were sentenced on June 13, 2023, to terms of imprisonment ranging from 121 to 136 months. (ROA.434, 1992, 2126)

Following trial, appellants filed a Motion for New Trial and Motion for Judgment of Acquittal. (ROA.383-386) The district court denied the motion. (ROA.415-424) In its order and opinion denying appellants' motion, the district court discussed Moody's "extensive" and "considerable amount of" training in the

field of geolocations data, stating, "It is clear from Moody's testimony during trial and after reviewing his Curriculum Vitae that he was qualified to testify as an expert and his testimony was reliable." (ROA.423) The court found that not all of the *Daubert* factors have to apply and that the methodology Moody used went to the weight rather than the admissibility of the testimony. (ROA.424) Ultimately, the court held that Moody's testimony was reliable and relevant to help the jury in deciding the facts of the case. (ROA.424)

Following denial of the Motion for New Trial and Motion for Judgment of Acquittal, each appellant filed a timely notice of appeal. (ROA.440, 2002, 2132)

SUMMARY OF THE ARGUMENT

I. The District Court Properly Denied the Defendants' Motion to Suppress the Geofence Warrant.

Geofence warrants are constitutional when supported by an affidavit establishing probable cause. There were no false statements or omissions in the application for the warrant, and agents relied upon the warrant in good faith.

II. The District Court Did Not Abuse its Discretion nor Err, Manifestly or Otherwise, in Allowing the Expert Testimony of Christopher Moody.

The District Court properly accepted Christopher Moody, a technical surveillance coordinator for the Postal Service, as an expert in the field of cell site and geolocation/historical location records over the objection of appellants. The District Court also properly overruled appellants' Motion for New Trial/Acquittal. (ROA.424) The District Court, noting that Moody has received "extensive training and experience in cell site analysis," and his testimony regarding the phone and Google records and the maps and animations that he created correctly found that Moody was qualified to testify as an expert and that his testimony was reliable. (ROA.423) Ultimately, the Court correctly determined that the methodology Moody used went to the weight rather than the admissibility of his testimony and that the testimony was reliable and relevant to the jury. (ROA.424)

ARGUMENT

I. The District Court Properly Denied the Appellants' Motion to Suppress the Geofence Warrant.

A. Standard of Review

Upon denial of a Motion to Suppress, the Fifth Circuit reviews the factual findings of the District Court for clear error and its legal conclusions *de novo*. *United States v. Gomez*, 623 F.3d 265, 268 (5th Cir. 2010). The evidence is to be viewed in the light most favorable to the government as the prevailing party. *United States v. Macias*, 658 F.3d 509, 517 (5th Cir. 2011).

B. Analysis

Geofence warrants in general are a valid investigatory tool of law enforcement and this warrant in particular was a lawful warrant supported by probable cause. Furthermore, even if the District Court had determined that the magistrate judge erred in issuing the warrant, the good faith exception would apply so that appellants' Motion to Suppress was properly denied.

i. The Geofence Warrant Satisfied the Fourth Amendment

The geofence warrant at issue here authorized the government to obtain from Google limited and specified information directly tied to a particular robbery at a particular place and time.[6] The facts of this case illustrate why a warrant that requires

[6] Appellants make reference in their memorandum to general warrants, but the warrant at issue did not remotely resemble a general warrant. A general warrant "specified only an offense—typically

disclosure of information about devices in a particular place at a particular time is not a general warrant. When law enforcement officers sought the warrant, they were investigating a serious violent crime, wherein the victim, Sylvester Cobbs, had been beaten with a handgun and threatened with death. The geofence warrant allowed them to solve the crime and protect the public by examining a remarkably limited and focused set of records from Google.

a. The Geofence Affidavit Established Probable Cause

Probable cause requires only 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). Probable cause is not a high bar. *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). The duty of a reviewing court is simply to ensure that the magistrate judge had a substantial basis for concluding that probable cause existed. *Gates*, 462 U.S. at 238–39.

Here, the affidavit established an ample basis for the magistrate judge to find probable cause. The affidavit established that an unknown subject, aided and abetted by two other unknown subjects, robbed Sylvester Cobbs of money and property belonging to the Postal Service. (ROA.573-574) It further established that the

seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). In contrast, the warrant at issue here was limited to specified information directly tied to a particular robbery at a particular place and time.

unknown subject was "possibly using a cellular device both before and after the robbery."[7] (ROA.573-574) The affidavit established that this was a premeditated crime involving multiple offenders and that the subjects likely used cell phones to communicate during the robbery. (ROA.573-574) It established a connection between smartphones and Google location information. (ROA.573-574) It explained that nearly every Android phone has an associated Google account, and that Google collects and retains location data from such devices when the account owner enables Google location services. (ROA.573-574) It also explained that Google can collect location information from non-Android smartphones if the devices are registered to a Google account and the user has location services enabled. (ROA.573-574) From this information, there was a substantial basis for the magistrate judge to find probable cause to believe that Google possessed evidence related to the robbery.[8]

In the Matter of the Search of Information that is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62 (D.D.C. 2021) (hereinafter referred

[7] Appellants allege that the affiant put this statement in his affidavit only because the affiant believed that a geofence warrant required a showing that one of the suspects was using a cellular phone. While the agent may have thought that was a requirement, there is no evidence that the statement was included simply to check a probable cause box. Rather, the statement was included because it was an accurate depiction of the evidence seen on the security camera video.

[8] Appellants make reference in their brief to the warrant requiring a search of cell phones, asserting that the government did not present sufficient probable cause to search a phone.To be clear, the warrant did not seek a search of anyone's phone. As discussed herein, a geofence warrant requires Google to search its electronic files (its "Sensorvault") for location history pertaining to users of Google apps and services. The information sought is not seeking information stored on phones (the information requested in a traditional cell phone search warrant), but rather simply which phones were using Google apps within the "box" at the time of the robbery.

to as *Google*) provides a particularly instructive opinion on geofence warrants. In that case, the magistrate judge issued a memorandum opinion explaining, in great detail, his reasoning for issuing a geofence warrant. The opinion contains a good summary of the technological aspects behind a geofence warrant, as well as a strong legal analysis of issues such as probable cause and particularity.

As set forth in the opinion, probable cause is a "practical, nontechnical conception" drawn from "common-sense conclusions about human behavior." *Google*, 579 F. Supp. 3d at 74 (citing *Illinois v. Gates*, 462 U.S. 213, 231 (1983)). It "deals with probabilities and depends on the totality of the circumstances," *Id*. at 75 (citing *Maryland v. Pringle*, 540 U.S. 366, 371 (2003)), and is "a fluid concept ... not readily, or even usefully, reduced to a neat set of legal rules." *Id*. (citing *Gates*, 462 U.S. at 232). Thus, the test for probable cause is not reducible to "precise definition or quantification." *Id*. (citing *Pringle*, 540 U.S. at 371).

The magistrate judge explained that for search warrants, probable cause requires (i) a "fair probability" that a crime has been committed and (ii) "a fair probability that contraband or evidence of [that] crime will be found in a particular place." *Google*, 579 F. Supp. 3d at 75 (citing *Gates*, 462 U.S. at 238). In other words, the inquiry is whether the application provides "a 'substantial basis' for concluding that 'a search would uncover evidence of wrongdoing'" by "demonstrat[ing] cause to believe that 'evidence is likely to be found at the place to be searched'" and "'a

nexus ... between the item to be seized and criminal behavior.'" *Id*. (citing *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017)).

In analyzing probable cause, the magistrate judge in *Google V* found there was a fair probability that the search of Google's servers would uncover useful evidence pertaining to the identities of the suspects:

> First, there is more than a "fair probability" that the suspects were within the geofence during the time windows the government established. The requested geofence encompasses the [Redacted] center and its parking lot. The CCTV footage obtained by the government shows the suspects inside the [Redacted] center.
>
> Second, the government has evidence that the suspects were actually using cell phones during the time windows set in the warrant. The CCTV footage apparently shows the suspects utilizing their devices while inside the [Redacted] center.
>
> Third, the affidavit's failure to specifically allege that the suspects, while on their phones, were using applications or other features that would communicate location data to Google, is also not fatal to the warrant application. The probability that the phones were communicating location information to Google is, at the very least, "fair," and that is all that is required.
>
> Fourth, there is also a "fair probability" that Google is in possession of identifying information for the users of phones found within the geofence.

Google, 579 F. Supp. 3d at 77-79. Accordingly, the magistrate judge determined that probable cause existed for the issuance of the warrant. Of particular interest was the magistrate judge's determination that the government need not show that any of the suspects were actually using phones within the parameters of the geofence. As stated

by the court:

> In the Court's view, however, it is not necessary that the government actually know that suspects are using their phones within the geofence. *See Google III*, 497 F. Supp. 3d at 355 (granting geofence warrant despite there being "no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense"). The core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business. *See id*. at 356 ("Unlike virtually any other item, it is rare to search an individual in the modern age during the commission of a crime and not find a cell phone on the person."); *see also United States v. James*, 3 F.4th 1102, 1105 (8th Cir. 2021) ("Even if nobody knew for sure whether the [suspect] actually possessed a cell phone, the judges were not required to check their common sense at the door and ignore the fact that most people 'compulsively carry cell phones with them all the time.'" (quoting *Carpenter*, 138 S. Ct. at 2218)).

Google, 579 F. Supp. 3d at 78.

Similar to *Google*, there was more than a fair probability that the suspects were within the geofence during the time period referenced in the warrant, as shown on the video footage from the camera across the street. While not necessary, the government had evidence that the suspects were using cell phones during the robbery. This belief was later corroborated by the appellants' phone records. The probability that the suspects' cell phones were communicating location information to Google was at least fair. There was also a fair probability that Google was in possession of identifying information for the users of the phones found in the geofence. Probable cause was satisfied.

Another instructive case on probable cause is *United States v. James*, 2019

WL 325231 (D. Minn. 2019), wherein the government used tower dump warrants to solve a series of robberies. The defendant argued there was no probable cause because it was "unknown whether a phone was used by the suspect before or after the robbery." *Id.* at *3. Nevertheless, the district court found probable cause existed based on the affiant's representations about the "ubiquitous nature" of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* Here, where McThunel used his phone just before the robbery, the basis for the magistrate's finding of probable cause was even stronger.

Messerschmidt v. Millender, 565 U.S. 535 (2012), demonstrates that the Supreme Court does not narrowly construe what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit on qualified immunity. *See Id.* The Court provided multiple reasons why it was not unreasonable to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend, including that it could "help to establish motive," it could be "helpful in impeaching [the shooter]," it could be helpful in "rebutting various defenses," and it could "demonstrat[e] [the shooter's] connection to other

evidence." *Id.* at 551-52.

Similarly, the issuing magistrate here had multiple reasons to believe that location information for those present at the robbery would constitute evidence. Investigators could use the location information to reconstruct what took place at the crime scene, to identify the robber and any accomplices, to identify potential witnesses, to obtain further evidence, to corroborate and explain other evidence, and to rebut potential defenses raised by the assailant, including an attempt to blame someone else for his crime. Thus, probable cause existed because the information sought by the warrant was evidence appropriately seized pursuant to a search warrant. The issuing magistrate had a substantial basis for finding probable cause that Google possessed location information regarding the scene of the robbery, and therefore the District Court properly denied appellants' Motion to Suppress.[9]

b. The Geofence Warrant Specified its Objects with Particularity

Under the Fourth Amendment, a valid warrant must particularly describe the place to be searched, and the persons or things to be seized. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The particularity requirement constrains a warrant so that it is no broader than the probable cause on which it is based. *Williams v. Kunze*, 806

[9] In arguing lack of probable cause, appellants also assert that the warrant was overbroad, relying on *Ybarra v. Illinois*. *Ybarra* is not applicable, as it addressed a physical search of a person, rather than simply obtaining information about a person, as we have in the present matter. *Ybarra*, 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.")

F.2d 594, 598-599 (5th Cir. 1986). It protects against exploratory rummaging in a person's belongings by requiring a particular description of the things to be seized. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). Moreover, the test for particularity "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)).

Further caselaw pertaining to the issue of particularity is set forth in detail in *Google*. As stated by the magistrate judge, the manifest purpose of the particularity requirement was to prevent general searches. *Google*, 579 F. Supp. 3d at 75 (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). Therefore, "[s]earch warrants must be specific." *Id*. (citing *United States v. Manafort*, 313 F. Supp. 3d 213, 231 (D.D.C. 2018)). There are two prongs of specificity: particularity and breadth. *Id*. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id*. at 75-76 (*citing Manafort,* 313 F. Supp. 3d at 231). A warrant is not constitutionally overbroad so long as the time, location, and overall scope of the search are consistent with the probable cause set forth in the warrant application. *Id*. at 76.

In regard to time, the court in *Google* stated:

> [T]he geofence only provides cell phone users' whereabouts in a single area for a handful of minutes on the days in question, not the sum-total

> of their daily movements. Thus, viewed in proper context, the government's request is limited and reasonable.

Google, 579 F. Supp. 3d at 81. As to location, the magistrate found "[T]he inquiry here is whether the 'target locations [are] drawn to capture location data from locations at or closely associated with the [crime].'" *Id*. at 82 (citing *Google III*, 497 F. Supp. 3d at 358).

In addressing whether or not the requested warrant was overbroad, the court in *Google* stated:

> The geofence may also capture the location information for persons who are not suspects, namely the other customers inside the [Redacted] center….For several reasons, the warrant's potential to collect location information from these other individuals does not render it deficient….As an initial matter, constitutionally permissible searches may infringe on the privacy interests of third persons—that is, persons who are not suspected of engaging in criminal activity. The Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches….The Fourth Amendment was not enacted to squelch reasonable investigative techniques because of the likelihood—or even certainty—that the privacy interests of third parties uninvolved in criminal activity would be implicated….Rather, the Fourth Amendment seeks to ensure that privacy interests are not infringed by law enforcement activities without a showing of probable cause and a particularized description of the place to be searched and the things to be seized.

Google, 579 F. Supp. 3d at 82-84.

Here, the geofence warrant was narrowly constrained based on location, date, and time. The warrant sought only location and identity information from Google regarding a one-hour interval for individuals present at the site of a robbery. Based

on the facts and circumstances agents knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the assailant and his co-conspirators.

It is no consequence that agents had not developed any suspects at the time they sought the warrant. As noted by the Supreme Court in *Zurcher*, a warrant may be used to investigate crime before agents identify a suspect, provided "it is satisfactorily demonstrated…that fruits, instrumentalities, or evidence of a crime is located on the premises." *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978); *see also United States v. Long*, 774 F.3d 653, 659 (10th Cir. 2014) (officers need not identify the perpetrator before searching a place where there is likely evidence of a crime).

The cell tower dump opinion *United States v. James* provides further persuasive authority that the warrant here was sufficiently particular. In *James*, the defendant argued that the tower dump warrants used to identify him as a robber were insufficiently particular because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames." *James*, 2019 WL 325231 at *3. The district court, however, found the warrants were sufficiently particular because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.* This reasoning is fully applicable here: the geofence warrant was

appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the tower location information in *James*. The parameters of the geographical box set forth in the geofence warrant is smaller than most cellular sites, and the government only obtained location information regarding three individuals,[10] rather than hundreds or thousands.

Appellants argue the warrant lacked particularity, stating the warrant left too much discretion to Google and the government to negotiate which users would have their account information searched. In actuality, the warrant specifically stated that it sought files and records maintained by Google, believed to conceal location information, subscriber information, and other evidence as set forth in the affidavit. There were very limiting constraints as to time and place for which the government was seeking location information. To further limit information obtained by the government, Google had established a three-step process to assist the government in narrowing the subscriber information provided by Google to only those accounts that appeared relevant to the investigation, information less than the maximum quantity of location and identity information that the warrant authorized. The warrant, however, established probable cause for all the evidence that law

[10] One individual did not appear to be involved, as the only time this device registered in the geofence was approximately 30 minutes after the robbery. Agents eventually determined this third individual was not relevant to the investigation.

enforcement could have obtained: identity information and two-hours of location data for all individuals present at the site of the robbery during the time of the robbery. The information specified by a warrant must be no broader than the probable cause on which it is based, *Kunze*, 806 F.2d at 598-599, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy. The assertion that the warrant lacked particularity is without merit.

ii. Investigators Relied Upon the Warrant in Good Faith

Even assuming the warrant lacked probable cause or particularity, suppression would not have been an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future violations, and only when the deterrent benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a

relatively new investigative technique, and there have been few judicial opinions (perhaps none in November 2018 when the warrant was sought[11]) analyzing them under the Fourth Amendment. In *McLamb*, the Fourth Circuit rejected suppression in a similar circumstance. The court held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel before seeking a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

United States v. McLamb, 880 F.3d 685, 691 (4th Circuit 2018). Here, Inspector Matney followed the approach endorsed by *McLamb* by consulting with the U.S. Attorney's Office about geofence warrants. He then sought and obtained a warrant from a U.S. Magistrate Judge. Inspector Matney did "precisely" what *McLamb* expects, and the good-faith exception precluded suppression.

Alternatively, the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), leads to the same result: no suppression. When police act in

[11] At the time of the hearing on the suppression motion, the government could only find six reported decisions pertaining to geofence warrants. The earliest of those decisions was from July 2020, 20 months after application for a geofence warrant in this matter.

"objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate judge, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> (1) when the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) when "the issuing magistrate wholly abandoned his judicial role…"; (3) when "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) when "a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004*) (*quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case.

One case relevant to the discussion is *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022).[12] The court in *Chatrie* provided a detailed account of the mechanisms behind a geofence warrant. *Chatrie*, 590 F. Supp. 3d at 907-916. The district judge in *Chatrie* found the warrant at issue lacked particularized probable cause. *Id*., at 929. However, the court acknowledged that the good faith exception to the exclusionary rule applied and thus denied the defendant's motion to suppress. *Id.*, at 936-941. For similar reasons, the good faith exception would likewise apply

[12] *Chatrie* is currently on appeal to the Fourth Circuit.

in the present matter.

Appellants argue that the good faith exception does not apply because (1) the warrant was based on recklessly false statements; (2) the affidavit lacked a substantial basis to determine probable cause; and (3) the warrant was facially deficient. It should be noted that the threshold for establishing an exception to the good faith rule is a high one because officers executing warrants cannot be expected to question the magistrate's probable-cause determination. *Messerschmidt*, 565 U.S. at 547. It is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting with the requirements of the Fourth Amendment. *Id*. The agent's belief that the warrant was issued based on probable cause was not unreasonable and the good faith exception thus precludes suppression.

To specifically address appellants' contentions, the second and third assertions have been discussed above in the section on probable cause. As to the allegation that the affidavit contained a misrepresentation of fact, this assertion is simply incorrect. In paragraph 16 of the affidavit, Inspector Matney avers that:

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

A review of the video shows exactly that. From approximately the 6:50 minute mark, when the assailant gets out of the white SUV, to approximately the 9:50 minute

mark, the assailant is seen walking around behind the post office with his left arm and hand up to his ear, as if he is holding a phone to his ear. (Exhibit "G-1," 6:50 - 9:50) While the camera is too far away to see the phone, you can clearly see the position of the assailant's arm and hand in the normal position of someone talking on the phone. There is no other logical explanation for the position of the assailant's arm and hand for that length of time and it is certainly reasonable to view the video and believe the assailant is talking on a cell phone. Inspector Matney's belief was correct. Phone records later confirmed that McThunel had a phone conversation with Smith that lasted nearly six minutes, beginning at 5:16 p.m., which would have been just about the time that Ayodele was dropping McThunel off behind the post office.

Following the attack on Sylvester Cobbs, the assailant is seen pacing behind the post office when he sets the registered mail sacks down and appears to briefly reach into his pocket and glance down, as if checking his phone for messages. (Exhibit "G-1," 13:34) Later, the assailant was seen squatting behind the post office, and he appeared that he may have been checking or texting on his phone. (Exhibit "G-1," 13:57 - 14:07) While not conclusive, these portions of the video are certainly sufficient to believe that the assailant was "possibly using a cellular device." The District Court agreed that the affiant had not made a knowing misrepresentation as to the assailant's possible use of a cellular device. (ROA.290-291) Accordingly,

appellants' argument that the affidavit contains a misrepresentation of fact is without merit.[13]

Appellants further assert the search warrant at issue required Google to search 592 million user accounts to determine which devices were near the Lake Cormorant Post Office at the time in question. Appellants contend the affiant acted with reckless disregard when he failed to disclose to the magistrate the true nature and scope of the geofence search. However, appellants have no standing to complain that the geofence warrant infringed upon the rights of others. *United States v. Wright*, 2023 WL 5804161, *10 (S.D. Ga. Sept. 7, 2023).

Furthermore, appellants' assertion regarding the scope of the search is incorrect. The warrant directed Google to search its own files for location information stored and maintained by Google – account information provided to it by users of Google apps and services. Appellants' own expert, Spencer McInvaille admitted that Google searched its "Sensorvault" (not 592 million users' phones) to

[13] The government would note that there is no need to produce evidence of cell phone usage to establish probable cause for a geofence warrant. See *Google*, 579 F. Supp. 3d 62, 78 (D.D.C. 2021) ("core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business"); *Matter of Search Warrant Application for Geofence Location Data Stored as Google Concerning Arson Investigation*, 497 F. Supp. 3d 345, 355 (E.D. Ill. 2020) (granting geofence warrant despite there being "no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense"); *United States v. James*, 3 F.4th 1102, 1105 (8th Cir. 2021) ("Even if nobody knew for sure whether the [suspect] actually possessed a cell phone, the judges were not required to check their common sense at the door and ignore the fact that most people 'compulsively carry cell phones with them all the time.'" (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018))).

obtain the data required by the warrant. (ROA.614-615) In complying with the warrant, Google reviews the location history of its account holders. (ROA.630-631) As stated by McInvaille, account holders allow Google to collect and store their location history. (ROA.631) The location history is stored with Google, in Google's "file cabinet" so to speak, which is a separate storage maintained by Google known as a "Sensorvault." (ROA.632) McInvaille agreed that the "Sensorvault" is a kind of electronic file cabinet maintained at Google's headquarters. (ROA.632-633) When Google gets a geofence warrant, it looks in its "Sensorvault," its electronic storage, to pull the requested information. (ROA.634) Furthermore, in conducting the search, Google is not looking to see where each and every account holder was located, but rather simply which accounts were located within the geofence at the time in question. No one's whereabouts are specifically known or disclosed, except for those within the geofence.[14]

Accordingly, the implication that Google searched 592 million phones to comply with the warrant is inaccurate. Google searched its own electronic file cabinet for information voluntarily provided to Google by its users. Google's computer system ran a set of GPS coordinates through its files to see which devices were within those coordinates on the subject date and time. Only those devices

[14] For a detailed explanation of how Google collects and stores location information, as well as a thorough analysis of geofence search warrant issues, *see United States v. Rhine*, 652 F. Supp. 3d 38, 67-68 (D.D.C. 2023).

(three) that appeared within the geofence were disclosed and subsequently identified. No law enforcement officer had any information as to where any other device was located, besides the three devices found in the geofence, and while Google maintains that information in its file, no one at Google reviewed the location of any other devices. This idea that Google somehow violated the privacy of 592 million people by looking to see where they were at the time of the robbery is incorrect. Google literally scanned its records to see only those devices in the geofence. Thus, there was no misrepresentation by omission in the affidavit.

iii. Additional Assertions of the Appellants

In addition to the arguments previously addressed, appellants, referencing Part II of Attachment A to the affidavit, state that the government failed to undertake "further legal process" as required in paragraph 2, Part II. (ROA.114) Appellants believe that "further legal process" meant the government had to return to the magistrate seeking another warrant for each phase of the three-step process. To the contrary, Part II set out the entire three-step process authorized by the magistrate when he issued the warrant. Step One required Google to search its files and provide a list of accounts found within the geographical "box" during the designated time. These accounts were given an anonymous numerical identifier. Numbered paragraph 2, which set forth Step One of the process, did state that additional information regarding the identified devices would come through "further legal process," but that

process was defined in numbered paragraphs 3 (Step Two) and 4 (Step Three). Step Two, set forth in paragraph 3, explained that for those accounts deemed relevant, Google shall provide additional location history outside of the predefined area to determine path of travel, which can, in some circumstances, assist the government in narrowing down the accounts for which it needs identifying subscriber information. This additional location history was limited to 60 minutes either side of the timestamps associated with the account in the initial dataset. Step Three, set forth in numbered paragraph 4, explained that Google would provide subscriber information for those accounts that the government identified as relevant.

The government followed the three-step process laid out in the affidavit and approved by the magistrate. There is no merit to the argument that failure to seek additional warrants at each step of the process violated appellants' Fourth Amendment rights. It was Google that established the extra steps the government must take in seeking geofence information, steps that arguably are not required by law.

Appellants further assert that cell phones and the data contained in them are granted heightened protections by the Fourth Amendment. However, appellants had no reasonable expectation of privacy in two[15] hours of Google location information.

[15] Step One of the warrant limited the data requested to a one-hour time frame. Step Two allowed the government to seek expanded data on relevant devices to sixty minutes either side of the first and last timestamp in the initial dataset for each device determined to be relevant to the

Appellants argue that they had a reasonable expectation of privacy in their location under *Carpenter*, but *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter*, 138 S. Ct. at 2217 n.3. Here, the government's acquisition of two hours of appellants' location information is governed by the long-standing principle that a person has no reasonable expectation of privacy in information disclosed to a third party and then conveyed by the third party to the government.[16]

Furthermore, while the Supreme Court determined that individuals have a "reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 S. Ct. at 2217 and n.3, the Supreme Court emphasized that its decision was "a narrow one." *Carpenter*, 138 S. Ct. at 2220. It explicitly declined to determine whether there is a "limited period" for which the government can acquire cell phone location information without implicating the Fourth Amendment. *Id.* at 2217 n.3. It also explicitly refused to

investigation. For one relevant device the first and last timestamps were eight minutes apart. For the other relevant device the first and last timestamps were three minutes apart. Thus, the total time period for which data was obtained for each of the two relevant devices was just slightly more than two hours.

[16] Google also disclosed to the government appellants' basic subscriber information, including email address, Google Account ID, and Google services used. In *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010), the Fourth Circuit held that a subscriber has no reasonable expectation of privacy in such information, which Google keeps for its business purpose.

decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant because tower dump information is similar to the information disclosed pursuant to the geofence warrant. A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." *Id.* Here, the geofence warrant sought information on all devices within a particular area during a particular interval.

Rather than providing an encyclopedic chronicle of the appellants' lives, the information disclosed by Google provided a summary of their location for a brief period of time immediately before, during, and after the robbery and assault of a postal employee.[17] This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

Additionally, appellants have no reasonable expectation of privacy in location information they disclosed to Google. Because *Carpenter* does not create a reasonable expectation of privacy in two hours of location information, Google's disclosure of that information to the government is subject to the principle that an individual retains no reasonable expectation of privacy in information revealed to a

[17] In their brief, appellants argue the search warrant granted the government unbridled discretion "to search deeply private data of an unlimited number of people." To the contrary, the warrant only asked Google to search its "Sensorvault" and determine which devices were in the proximity of the Lake Cormorant Post Office during the robbery. There is nothing deeply private about that.

third party and then disclosed by the third party to the government. For decades, the Supreme Court has repeatedly invoked this third-party doctrine in cases ranging from private communications to business records, and this principle applies here to appellants' location information.

In *Hoffa v. United States*, 385 U.S. 293 (1966), the Court applied the third-party doctrine to incriminating statements made in the presence of an informant. The Court held that the Fourth Amendment did not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. A decade later the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records in *United States v. Miller*, 425 U.S. 435 (1976). The Court held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party).

The Supreme Court also relied on this principle in *Smith v. Maryland*, 442 U.S. 735 (1979), when it held that a telephone user had no reasonable expectation of privacy in dialed telephone number information. The Court stated "we doubt that

people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. The Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation marks omitted). The Court explained that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44.

Appellants therefore had no reasonable expectation of privacy in Google's records of their location because they voluntarily conveyed their location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, appellants had previously taken an affirmative step to disclose their location information to Google. Moreover, they agreed that Google would have access to their location information for purposes ranging from providing them with targeted advertising or assistance with driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). These facts demonstrate that appellants voluntarily disclosed their location information to Google and the

government did not infringe their reasonable expectation of privacy when it obtained from Google information about their device's location during a two-hour interval.

Finally, the fact that appellants voluntarily disclosed their location information to Google is confirmed by the reasoning of *Carpenter*. *Carpenter* concluded that cell-site information was not voluntarily disclosed to the phone company for two reasons, neither applicable here. First, the Court held that carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. In contrast, although Google services are frequently helpful and convenient, most may be used without turning on Google location services and using Google services with location enabled is not essential to participation in modern society. Google location services are no more indispensable than having a bank account or making a phone call, and bank records and dialed telephone number information remain unprotected by the Fourth Amendment under *Miller* and *Smith*. Second, *Carpenter* held that cell-site information is collected "without any affirmative act on the part of the user beyond powering up" and that "there is no way to avoid leaving behind a trail of location data." *Id.* In contrast, in order for Google to have their location information, appellants had to affirmatively opt in, and they also retained the ability to delete their information. Finally, a cell phone user's disclosure of location information to the phone company is merely incidental to receiving communication service from the company, but a device owner's disclosure

of location information to Google is the central prerequisite to obtaining Google location services. Apellants thus voluntarily disclosed their location information to Google, and Google's disclosure of that information to the government did not infringe upon their reasonable expectation of privacy.

II. The District Court Did Not Abuse its Discretion nor Err, Manifestly or Otherwise, in Allowing the Expert Testimony of Christopher Moody.

A. Standard of Review

This Court "reviews a district court's decision to admit expert testimony under an abuse-of-discretion standard." *United States v. Hicks*, 389 F.3d 514, 525 (5th Cir. 2004). If this Court finds an abuse of discretion in the district court's admitting of evidence, it then considers any error under the harmless error doctrine. *Hicks*, 389 F.3d at 524. The district court's ruling will only be overturned if it was "manifestly erroneous." *United States v. Kuhrt*, 788 F.3d 403, 418 (5th Cir. 2015).

B. Analysis

Federal Rule of Evidence 702 governs the admissibility of expert witness testimony. "A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case."

FED. R. EVID. 702. The Rule has recently been amended to clarify the standard as by a preponderance of the evidence. *See* FED. R. EVID. 702 (effective Dec. 1, 2023). The "touchstone of the rule is whether the testimony will assist the jury." *United States v. Offill*, 666 F.3d 168, 175 (4th Cir. 2011).

For an expert to be "qualified" under Rule 702, "it is not necessary that the witness be recognized as a leading authority in the field in question or even a member of a recognized professional community." *United States v. Sutton*, 642 F. Supp. 3d. 57, 65 (D.D.C. 2022) (quoting 29, CHARLES ALAN WRIGHT & ARTHER R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 6264.1 (2d ed. 2022)). There is "no requirement that an expert possess formal education, and an expert may be qualified on the basis of his or her practical experience." *Khairkhwa v. Obama*, 793 F. Supp. 2d 1, 11 (D.D.C. May 27, 2011). The "degree of 'knowledge, skill, experience, training, or education' required to qualify an expert witness 'is only that necessary to insure that the witness testimony "assist" the trier of fact.'" *Id.* (quoting *Mannino v. Int'l Mfg. Co.*, 650 F.2d 846, 851 (6th Cir. 1981)).

The Supreme Court provided trial courts with guidance on the admission of expert testomony at trial in *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993), which established a two-prong test for the admissibility of scientific evidence.

The first prong rejected the previously widely-used "general acceptance" test enunciated in *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923) in favor of a more flexible standard that reviews the scientific validity and reliability of the evidence. The second prong, sometimes referred to as the "relevancy" requirement, simply reiterated that scientific testimony or evidence must assist the trier of fact to be admissible. *Daubert* and its principles apply to both scientific and non-scientific expert testimony. *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 147 (1999).

The trial court's task is to ensure the proposed expert testimony "both rests on a reliable foundation and is relevant to the task at hand." *Daubert*, 509 U.S. at 597. The Supreme Court in *Daubert* listed four non-exclusive factors that are helpful to determine the reliability of scientific or technical testimony: (1) whether the scientific theory or technique can be (and has been) tested; (2) whether the theory or technique has been subjected to peer review and publication; (3) whether a particular technique has a known potential rate of error; and (4) whether the theory or technique is generally accepted in the relevant scientific community. *Daubert*, 509 U.S. at 593-95. The Court noted that these factors do not constitute a "definitive checklist or test," and that "[m]any factors will bear on the inquiry" that involves "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 592-93.

It is well established that experts may base their opinions on experience—and that expert testimony can cover areas of technical and other knowledge rather than just science. *Kumho Tire Co.*, 526 U.S. at 148-49. The Fifth Circuit has held that "the *Daubert* factors are meant to be helpful and not definitive," and the Supreme Court has recognized that specific factors listed in *Daubert* "do not 'necessarily apply in every instance in which the reliability of scientific testimony is challenged.'" *United States v. Schaffer*, 439 F. App'x 344, 346 (5th Cir. 2011), (citing *Kumho Tire Co.*, 526 U.S. at 151).

On March 10, 2022, the Government designated Christopher Moody as an expert and provided notice to appellants that Moody would be used to show "the location of defendants and their cellular phones before, during and after the time of the subject robbery." (ROA.404) His curriculum vitae was also provided at that time. (ROA.405-406) On February 3, 2023, the Government provided a supplemental expert disclosure in compliance with revised Rule 16 of the Federal Rules of Criminal Procedure which stated in detail Moody's anticipated testimony. (ROA.407-410) Appellants failed to file a pretrial *Daubert* motion to exclude Moody, instead waiting until Moody was tendered at trial to raise the objection. (ROA.1273-1275)

As described above, Moody has extensive training and experience in the relevant field due to his trainings and certifications over a period of years.

(ROA.1266). Moody testified that he had been working with geolocation technology for many years and has received multiple certifications. (ROA.1266) He also testified that he completes recertifications regularly. Moody has been accepted as an expert in two other cases in the United States District Court for the Western District of Tennessee. (ROA.1267)

Accordingly, there is no question as to his qualifications nor do the appellants question any specific notation in Moody's reports. There is no suggestion by appellants that Moody plotted any location information incorrectly or interpreted any data differently from how appellants think it should have been interpreted. Appellants never objected to the authenticity of the cellphone or Google geolocation records, nor did they call an expert to question the data's reliability. Indeed, their own expert at the suppression hearing stated that the Google location records were reliable. (ROA.857)

A. Historical Cell Location Data Is Scientifically Valid, Probative, Reliable, and Admissible in this Case

The evidence that the Government offered in this case—historical Google location and cell site analysis—is scientifically valid, probative, and reliable for the purposes for which it was offered in this case. The United States submits that the district court correctly exercised its broad discretion in allowing expert testimony concerning historical cell site and Google location information because the technology and scientific principles used by cellphones to communicate with one another and that Google uses to locate its users are valid, reliable, and probative. In

addition, the evidence was relevant and assisted the trier of fact in deciding the facts at issue in this case. Indeed, appellants do not cite, and the government is not aware of, a case in which the type of testimony being offered in this case has been rejected.

B. Numerous Courts Have Affirmed the Reliability of Historic Location Analysis for Establishing the General Location of a Cell Phone

To be sure, testimony about cell phone technology and the ability to determine the general area where calls are placed and received has been admitted in courts throughout the country as a matter of course for more than a decade. *United States v. Jones*, 918 F. Supp. 2d 1, 5 (D.D.C. 2013) (collecting cases in the context of historical cell site analysis); *see generally Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2017) ("cell phone location information is detailed, encyclopedic, and effortlessly compiled").

Appellants attempt to mask the real evidence presented by Moody, who took undisputedly authenticated historical geolocation records and placed them into two software programs which created maps and animations. As the district court even noted, Moody was highly skilled to take these rather simple yet numerous records and put them into a readable form for the jury. (ROA.423-424)

As noted above, Moody has testified as an expert regarding historical cell site analysis on two other occasions. The science behind how cell phones work has been accepted in the scientific and legal community. Appellants have not cited to any cases

in which a court ruled this type of evidence untrustworthy or "junk science," or in which a court has excluded a qualified expert from providing testimony on this topic for the purpose of establishing the relevant general location of a cellular phone.

As shown in the cases discussed below, experts across the country have testified in other trials for the purpose of showing the general location of cell phone use through historical cell-site records and the coverage area of cell towers and have recently allowed testimony of Google geolocation evidence. Appellants' claim that Moody's testimony is unreliable, and he is not qualified, is based on neither fact nor law.

i. Cell Site Location Information

In *Schaffer*, this Court found no abuse of discretion in the district court's conclusion that an FBI agent's cell site analysis met the standard under *Daubert*, specifically noting that this type of testimony is "neither untested nor unestablished." 439 F. App'x at 347. In *United States v. Weathers*, 169 F.3d 336 (6th Cir. 1999), the appellate court did not even question the appearance of an expert witness on this topic. *Id.* at 339 (discussing expert testimony on cell sites). In *United States v. Feliciano*, 300 F. App'x 795 (11th Cir. 2008) (unpublished), the court allowed a police officer to testify as a lay witness where "he simply reviewed the cellular telephone records and a summary of those calls, which identified cellular towers for each call, and based on his personal knowledge concerning the locations of certain cellular towers," the witness gave a conclusion in that case suggesting that the cell

phone was not near a particular location. *Id.* at 801. The testimony here was relevant and reliable and founded in established methodology.

Moody has received FBI Cellular Analysis Survey Team (CAST) training, and persons similarly trained have testified as experts in numerous trials around the country for the purpose of showing the general location of someone using their phone through historical cell site records and the coverage area of the cell towers handling those calls. *See*, *e.g.*, *United States v. Pembrook*, 876 F.3d 812, 824-26 (6th Cir. 2017), *vacated on other grounds by Sessions v. Dimaya*, 138 S. Ct. 1204 (2018) (holding expert testimony related to using cell site data to locate defendants was sufficiently reliable and admissible at trial); *United States v. Lewisbey*, 843 F.3d 653, 659 (7th Cir. 2016) ("Using call records and cell towers to determine general location of a phone at specific times is a well-accepted, reliable methodology."); *United States v. Johnson,* 2015 WL 5012949, at *6 (N.D. Cal. Aug. 24, 2015) ("Historical cell site evidence has consistently been found admissible by federal courts."); *Jones,* 918 F. Supp. 2d at 5 ("The use of cell phone records to locate a phone has been widely accepted in both federal and state courts across the country."); *United States v. Davis*, 2013 WL 2156659, at *4 (S.D. Fla. May 17, 2013) (noting FBI agent's testimony that "as a result of the success . . . FBI agents experienced using call-detail records in investigations, the FBI formulated a nationwide Cellular Analysis Survey Team . . . whose sole job it is to analyze cellular

telephone records for use in investigation"); *United States v. Machado-Erazo*, 950 F. Supp. 2d 49, 57 (D.D.C. June 17, 2013) (finding FBI CAST agent's testimony admissible under *Daubert* as it was based on scientific knowledge that was relevant to the issues at trial). The case law makes clear the wide acceptance of testimony such as the government offered here.

ii. Google Location Data

Moody testified as to his extensive experience, training and certifications as well as to the processes he implemented to place the Google GPS coordinates into a software program. He also discussed the margin of error/radii of the Google location data.

As explained by Moody, geolocation data is used by Google to locate their users. This data is nothing more than historical GPS location data which has long been used in criminal cases. *See United States v. Mathews*, 928 F.3d 968, 980 (10th Cir. 2019) (affirming the denial of a pretrial *Daubert* hearing on the admission of expert who made maps of historical GPS data derived from ankle monitor data). As discussed below, Google data has been used in court and been held reliable.

In *State v. Pierce*, the Superior Court of Delaware determined that expert opinion based on Google location data was reliable and would assist the factfinder. *See State v. Pierce*, 222 A.3d 582, 590 (Del. Super. Ct. 2019) ("Accurate geolocation of a mobile device is an important part of Google's business plan for the Android

operating system." "Merchants use this location provided by Google to promote products, often targeting advertisements to specific geographical locations."). Other courts have also allowed evidence/testimony of Google location data. *See United States v. Crawford*, 2021 WL 2367592 (W.D.N.Y. Jan. 14, 2021) (report and recommendation adopted, 2021 WL 1730875, at *3 (W.D.N.Y. May 3, 2021)) ("Although the exact methodologies or principles used by Google to obtain this geolocation data are not yet disclosed, this Court is not inclined to find the scientific or technical validity of geolocation gained from Wi-Fi or satellite data to be so lacking in reliability that it should fail to pass the gatekeeping function of the Court under *Daubert.*"); *Pierce,* 222 A. 3d at 588, n. 27 (collecting cases).

Appellants' efforts to discredit Moody's methodology by pointing to the limits of the research he undertook generally go to the weight rather than the admissibility of his testimony. *Huss v. Gayden*, 571 F.3d 442, 452 (5th Cir. 2009); *United States v. Morgan*, 45 F.4th 192, 201 (D.C. Cir. 2022). "As a general rule, questions relating to the bases and sources of an expert's opinion affect the weight to be assigned that opinion rather than its admissibility and should be left for the [trier of fact's] consideration." *Viterbo v. Dow Chem. Co.*, 826 F.2d 420, 422 (5th Cir. 1987); *see also Daubert*, 509 U.S. at 596 ("Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence."); *United States v.*

Gladden, 11-CR-119, 2013 WL 1916125, at *8 (W.D.N.Y. May 8, 2013) (denying motion for a *Daubert* hearing because the challenges made to expert conclusions went to the weight of the evidence, not to its admissibility).

Notably, appellants' argument is contrary to opinions of their own expert witness who testified in the suppression hearing. That expert, Spencer McInvaille, was tendered as an expert in digital forensics and geolocation analysis with no objection from the Government.

McInvaille admitted that the Google data proved that two devices were on scene around the post office on the date and time in question:

Mr. Mims:	For those accounts. Okay. So you don't disagree that Smith and McThunel were present at the Lake Cormorant post office at 5:30 p.m. that evening, do you?
Mr. McInvaille:	I can't say them physically, but an account that you have associated with them, yes.
Mr. Mims:	Okay. Their devices were present, weren't they?
Mr. McInvaille:	The devices with those accounts, yes.

(ROA.857)

In sum, the court was correct in accepting Christopher Moody as an expert witness in the area of cell site and Google geolocation data and location analysis, a field in which Moody was well qualified. Furthermore, this data is reliable and well accepted within the appropriate fields of science and technology.

The district court did not abuse its discretion nor manifestly err in allowing Moody to take cell sites, phone towers, and GPS points and load them into maps and animations. Moody was well qualified, and the maps and animations assisted the trier of fact who found the appellants guilty.

CONCLUSION

For the above-stated reasons, the judgment of the district court should be affirmed in all respects.

Respectfully submitted, this the 20th day of December, 2023.

CLAY JOYNER
United States Attorney
MS Bar No. 10316

By: */s/ Robert J. Mims*
ROBERT J. MIMS,
MS Bar No. 9913
Assistant United States Attorney

CLYDE MCGEE IV
MS Bar No. 102229
Assistant United States Attorney
Northern District of Mississippi
900 Jefferson Avenue
Oxford, Mississippi 38655
Telephone: (662) 234-3351
Criminal Division Fax: (662) 234-0657

CERTIFICATE OF SERVICE

I, Robert J. Mims, Assistant United States Attorney for the Northern District of Mississippi, hereby certify that I have this day filed this Brief of Appellee with the Court's CM/ECF filing system which caused an email to be sent with an electronic link to a true copy of said brief to the following:

Goodloe T. Lewis, MSB# 9889
Attorney of Record for Jamarr Smith
Defendant/Appellant
Email: glewis@hickmanlaw.com

Paul Chiniche, MSB #101582
Attorney of Record for Gilbert McThunel, II
Defendant/Appellant
Email: pc@chinichelawfirm.com

William F. Travis, MSB #8267
Attorney of Record for Thomas Ayodele
Defendant/Appellant
Email: bill@southavenlaw.com

This the 20th day of December, 2023.

/s/Robert J. Mims
ROBERT J. MIMS
Assistant United States Attorney
MS Bar # 9913

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).

EXCLUSIVE OF THE EXEMPTED PORTIONS IN 5th Cir. R. 32.2.7(b)(3), THE BRIEF CONTAINS (select one):

A. 12,991 words, OR
B. _____ lines of text in monospaced typeface.

THE BRIEF HAS BEEN PREPARED (select one):

A. in proportionately spaced typeface using:

Software Name and Version: Microsoft Word 2016

in (Typeface Name and Font Size): Times New Roman 14cpi

B. in monospaced (non-proportionally spaced) typeface using:

Typeface name and number of characters per inch:

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/Robert J. Mims
ROBERT J. MIMS
Assistant United States Attorney

/s/*Clyde McGee IV*
CLYDE McGEE IV, MSB No. 102229
Assistant United States Attorney
Attorney for Plaintiff-Appellee