**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF OKLAHOMA**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>***Plaintiff*,**<br><br>**v.**<br><br>**SILVIA VERONICA FUENTES,**<br><br>***Defendant.*** | **Case No. CR-21-358-RAW** |

**UNITED STATES' PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING DEFENDANT'S MOTION TO SUPPRESS**

Comes now the United States of America, by and through United States Attorney Christopher J. Wilson and Assistant United States Attorney T. Cameron McEwen for the Eastern District of Oklahoma, and hereby submits its proposed Findings of Fact and Conclusions of Law Regarding Defendant's Motion to Suppress. The United States respectfully requests this Court deny the defendant's Opposed Motion to Suppress Evidence Obtained by *Google "Geofence" Search Warrant* and Brief in Support (Doc. 39).

## I. PROCEDURAL HISTORY

On November 10, 2021, the defendant was charged in a single-count Indictment by the Federal Grand Jury with Failure to Stop for an Accident Involving Death in Indian Country, in violation of 18 U.S.C. § 13, 1151, and 1152 and 47 O.S. § 10-102.1. *See* Doc. 13.

On December 14, 2021, the defendant was arraigned on the Indictment and discovery was ordered disclosed pursuant to Local Criminal Rule 16(A). *See* Doc. 20. The United States produced discovery materials to defense counsel on December 17, 2021, May 16, 2022, October 13, 2022, December 5, 2022, December 7, 2022, January 18, 2023, May 24, 2023, May 30, 2023, September 11, 2023, and September 22, 2023. This discovery included all requested documents

and records obtained from Google pursuant to the April 7, 2021 and April 28, 2021 search warrants. *See* Government's Suppression Hearing Exhibits 2, 4, and 9.

On November 23, 2022, the defendant filed a Motion for Discovery Regarding Government's Use of Google's Sensorvault Data (Doc. 38) and an Opposed Motion to Suppress Evidence Obtained by *Google Geofence Search Warrant* and Brief in Support (Doc. 39). On November 30, 2022, the United States filed a response to both the defendant's Motion for Discovery Regarding Government's Use of Google's Sensorvault Data and her Opposed Motion to Suppress Evidence Obtained by *Google Geofence Search Warrant* and Brief in Support. *See* Docs 43 and 44. On December 5, 2022, the defendant's oral motion to withdraw her Motion for Discovery Regarding Government's Use of Google's Sensorvault Data was granted by the Court. *See* Docs 49, 51, and 52. On August 22, 2023, the Court scheduled an evidentiary hearing on the defendant's Opposed Motion to Suppress Evidence Obtained by *Google Geofence Search Warrant* and Brief in Support for September 25-26, 2023. *See* Doc. 109.

On September 25-26, 2023, a suppression hearing was held before United States Magistrate Judge Jason A. Robertson on the defendant's Opposed Motion to Suppress Evidence Obtained by *Google Geofence Search Warrant* and Brief in Support. *See* Docs. 120 and 122. On September 26, 2023, the parties were ordered to submit their proposed findings of fact and conclusions of law to the Court no later than December 8, 2023, and submit their responses to the other parties' findings of fact and conclusions of law to the Court no later than December 18, 2023. *See* Doc. 123.

## II. FINDINGS OF FACT

The United States proposed Findings of Fact are as follows:

1. On March 18, 2021, at 21:54 hours, a fatal traffic collision occurred at the intersection of U.S. Highway 62 and South 460 Road in Cherokee County, Oklahoma. *See* Government's Suppression Hearing Exhibit 8 at ¶21. This location is within the Eastern District of Oklahoma and within the definition of "Indian Country," as it occurred within the boundaries of the Cherokee Nation Indian Reservation. *Id*.
2. Oklahoma Highway Patrol ("OHP") troopers were dispatched to the scene. *See* Government's Suppression Hearing Exhibit 8 at ¶22. Based on OHP's collection of evidence at the scene, including debris from a vehicle, and speaking to witnesses, investigators determined that a female, J.D., was travelling southbound on South 460 Rd. on her bicycle and was attempting to cross U.S. 62, when she was struck by an unknown vehicle travelling westbound on U.S. 62. *Id*.; *see also* Suppression Hearing Transcript at pgs. 112-116, 23-25, 1-25, 1-25, 1-25, and 1-10. J.D. was assisted by another individual not involved in the collision until she was transported by air ambulance to St. John Hospital in Tulsa, Oklahoma. *See* Government's Suppression Hearing Exhibit 8 at ¶22. J.D. later died from her injuries from the collision. *Id*. J.D. was a member of the Cherokee Nation. *Id*.
3. The collision occurred on a rural, four-lane highway separated by an unimproved median. *See* Government's Suppression Hearing Exhibit 8 at ¶23. There were no traffic control devices. *Id*. There were a small number of commercial businesses and residences located near the intersection. *Id*. OHP was able to retrieve surveillance video from several nearby businesses. *Id*.; *see also* Suppression Hearing Transcript at pgs. 113-116, lines 17-25, 1-25, 1-25, and 1-10. A review of the videos shows that the collision occurred at 21:54 hours, and that shortly after the collision, the suspect vehicle pulled over to the shoulder of the

highway a short distance from the collision. *Id*. The suspect vehicle stopped for approximately 10 seconds before resuming westbound travelling on U.S. 62 and leaving the scene. *Id*. In the one-minute timespan after the collision, the videos show six other vehicles travelling through the collision area. *Id*. Five of the six vehicles are travelling eastbound. *Id*.

4. In March of 2021, OHP Trooper and FBI Task Force Officer Dustin Thornton ("TFO Thornton") applied for a Google geofence search warrant for the area surrounding the collision scene with United States Magistrate Judge Steven P. Shreder of the United States District Court for the Eastern District of Oklahoma. *See* Government's Suppression Hearing Exhibit 6; Suppression Hearing Transcript at pgs. 118-119, lines 5-25 and 1-8. In Attachment A of the March 2021 application, the requested time period was from 21:49 – 21:59 hours, a total of 10 minutes or 5 minutes before and after the time of the collision at 21:54. *See* Government's Suppression Hearing Exhibit 6 at Attachment A; Suppression Hearing Transcript at pgs. 121-122, lines 17-25 and 1-5. Magistrate Judge Shreder rejected the March 2021 application because the time period was too long and requested it be reduced. *See* Suppression Hearing Transcript at pg. 122, lines 6-15.
5. In March of 2021, TFO Thornton was an FBI TFO and OHP investigator. *See* Suppression Hearing Transcript at pg. 112, lines 13-22.
6. Currently, TFO Thornton is an FBI TFO and a supervisor of OHP's traffic homicide unit. *See* Suppression Hearing Transcript at pgs. 111-112 and 136-139, lines 17-25, 1-12, 17-25, 1-25, 1-25, and 1-17.
7. On April 1, 2021, TFO Thornton applied for a second Google geofence search warrant. *See* Government's Suppression Hearing Exhibit 1; Suppression Hearing Transcript at pg.

122, lines 16-21. In the April 1, 2021 application, TFO Thornton reduced the time period to a total of 4 minutes or two minutes on each side of the time of the collision at 21:54. *See* Government's Suppression Hearing Exhibit 1 at Attachment A; Suppression Hearing Transcript at pgs. 122-123, lines 22-25 and 1-4. There were no other changes made between the March 2021 application and the April 1, 2021 application. *See* Government's Suppression Hearing Exhibits 1 and 6. On April 1, 2021, Magistrate Judge Shreder approved the second geofence search warrant application and signed the search warrant. *See* Government's Suppression Hearing Exhibits 1 and 2.

8. At some point after Magistrate Judge Shreder signed the April 1, 2021 Google geofence search warrant, Assistant United States Attorney ("AUSA") James Montoya asked TFO Thornton to withdraw it. *See* Suppression Hearing Transcript at pgs. 123-125, lines 13-25, 1-25, and 1-16. TFO Thornton does not recall why AUSA Montoya asked him to withdraw the April 1, 2021 search warrant. *Id*. TFO Thornton requested a withdrawal of the April 1, 2021 search warrant through the Law Enforcement Relation Services ("LERS") system. *Id*.; *see also* Government's Suppression Hearing Exhibit 7.

9. On April 7, 2021, TFO Thornton applied for a third Google geofence search warrant. *See* Government's Suppression Hearing Exhibit 8; Suppression Hearing Transcript at pg. 127, lines 4-15. In the April 7, 2021 application, TFO Thornton's affidavit established probable cause by describing the facts of the collision and evidence collected around the scene of the crime. *See* Government's Suppression Hearing Exhibit 8 at ¶¶21-23. The affidavit also explained why there was reason to believe that Google would have evidence pertaining to the collision. *Id*. at ¶¶7-26. Among these facts, the affidavit disclosed:

    (a) Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android.

Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device;

(b) Google offers numerous apps and online-based services, including messaging and calling (e.g., Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (e.g., Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed into their Google accounts;

(c) Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices;

(d) Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time;"

(e) [T]he location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a 'maps display radius,' for each latitude and longitude point;

(f) Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location- based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google

account or by enabling auto-deletion of their Location History records older than a set number of months;

(g) [A] vast majority of motorist not only own but use their smartphones while driving; and

(h) [A] significant number of collisions occur as a result of distracted driving from a variety of sources, including cellphone use[,]" and "persons involved in a collision often use their cellphone immediately or shortly after a collision if not to call emergency services, then to call family members or friends.

*Id*. Magistrate Judge Shreder found probable cause and approved the April 7, 2021 search warrant. *See* Government's Suppression Hearing Exhibits 8 and 9.

10. As for the Google geofence in question in this case, the parameters of the geofence specified a targeted geographical area, identified as an approximate 1000' by 170' area around specific latitude and longitude points surrounding the area of the collision. *See* Government's Suppression Hearing Exhibits 5 and 8 at Attachments A and B; Suppression Hearing Transcript at pgs. 119-121 and 128, lines 5-25, 1-20, 1-16, and 1-5. In the geofence, there were no public buildings or structures. *Id*. The geofence only incorporated the roadway. *Id*. The purpose of the geofence search warrant was to locate the suspect driving the vehicle and any witnesses that may have seen the collision. *Id*. The geofence search warrant requested disclosure of location information for a period of two minutes before and two minutes after the collision from accounts associated with devices within this target area at some point during the four-minute interval that included the collision. *Id.*

11. The Google geofence search warrant also requested disclosure of specified customer identity information associated with these accounts through a three-step process that enabled law enforcement to "narrow down" the information disclosed by Google and thus

obtain less than the maximum amount of information covered by the search warrant. *See* Government's Suppression Hearing Exhibit 8. In Attachment B, the geofence warrant directed that in the first step, Google was to disclose information "specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available," for "each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (i.e., "maps display radius") would permit the device to be located within the Initial Search Parameters." *Id*. at Attachment B. In the second step, law enforcement was to "review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information." *Id*. Then, "[t]he Government may, at its discretion, identify a subset of the devices." *Id*. In the third step, "Google shall disclose to the Government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the Government inquires." *Id*. This is the same three-step process outlined by Sarah Rodriguez, a Team Lead for Investigations Support at Google, in her affidavit. *See* Government's Suppression Hearing Exhibit 20 at pg. 15-17, ¶¶5-12. The purpose of this three-step process is "[t]o ensure privacy protections for Google users and to protect against overbroad disclosures based on non-contextualized LH information[.]" *Id*. at ¶5. Also, "Google instituted [this] policy [to object] to any warrant that failed to include deidentification and narrowing measures." *Id*.

12. TFO Thornton followed this three-step process when he executed the geofence warrant. In step one, Google produced geolocation data in an anonymized format, which revealed three devices inside the "geofence" boundary. *See* Government's Suppression Hearing Exhibits

10, 11, 12, 14, and 18; Suppression Hearing Transcript at pgs. 128-129, lines 6-25 and 1-18. The information produced from Google was anonymized because law enforcement had no way of identifying the individual(s) associated with the Device IDs without requesting additional data from Google. *Id*. One of these devices crossed through the geofence from 21:54:18 to 21:54:35 with three location datapoints within the geofence. *Id*. The timing and location of the datapoints of this device is consistent with the device travelling westbound on U.S. 62 at the exact moment of the collision and is consistent with the behavior of the suspect vehicle on video. *Id*. In step two, TFO Thornton identified the accounts of interest, which was all three accounts, especially the account traveling westbound that started with the numbers 276 ("Suspect Account"). *See* Government's Suppression Hearing Exhibits 10 through 17; Suppression Hearing Transcript at pgs. 128-134, lines 19-25, 1-25, 1-25, 1-25, 1-25, 1-25, and 1-17. Based on his review, TFO Thornton elected to request the basic subscriber information for all three accounts because each account was linked to an individual that reasonably could be a suspect or witness in the investigation. *Id*. In step three, TFO Thornton requested and obtained the basic subscriber information for all three of the accounts from Google, including the Suspect Account, which belonged to the defendant. *See* Government's Suppression Hearing Exhibits 11 through 17. Law enforcement would not have been able to get this information any other way than by asking Google for it. *Id*. This information revealed that the Google account associated with the device traveling westbound at the time of the collision is account XXXXXXXX6595. *See* Government's Suppression Hearing Exhibit 15. The name associated with the account is "sXXXXX fXXXXXX" with an email of "XXXXXXXXXXX@gmail.com." *Id*. The account was created on March, 1, 2011, and

uses a number of Google services and applications, including Web & App Activity, Gmail, Google Hangouts, iGoogle, Profiles, YouTube, Google Voice, Google Photos, Google Drive, Android, Google Calendar, Google Chrome Sync, Google Play Music, Google Docs, Google Play, Google Takeout, Location History, Google Cloud Print, Blogger, Google My Maps, Is In Family, Google Payments, Google Keep, G1 Phone Backup, Play Loyalty, Device Centric Auth, Android Device Console, Has Google One Membership Information. *Id*. Two cellphone numbers associated with the account are (XXX) XXX-1695 and (XXX) XXX-2760. *Id*. The account was still active, with the most recent login (at the time the data was compiled in response to the search warrant) being April 11, 2021. *Id*.

13. The only changes between the April 1, 2021 affidavit and application for a search warrant and the April 7, 2021 affidavit and application for a search warrant is the language removed from paragraph 26 of TFO Thornton's April 1, 2021 affidavit that states, "Additionally, so at to minimize data collection of devices not belonging to the unknown driver, the Government is requesting that Google exclude any devices within the Target Location for longer than three minutes;" and the "Time Restriction" section in Attachment A of the April 1, 2021 application that contains similar language. *See* Government's Suppression Hearing Exhibit 1 at ¶26 and Attachment A and Exhibit 8 at ¶26 and Attachment A; Suppression Hearing Transcript at pgs. 125-127, lines 17-25, 1-25, and 1-3. TFO Thornton does not recall why this language was removed. *Id*. However, Google likely objected to the "time restriction" language in the April 1, 2021 Google geofence search warrant, requested its removal, and this is why it was removed from the April 7, 2021 affidavit and

application. *Id*.; *see also* Suppression Hearing Transcript at pgs. 185-186 and 236-239, lines 6-25, 1-21, 21-25, 1-25, 1-25, and 1-10.

14. At no point did Google object to the April 7, 2021 Google geofence search warrant and provided everything requested in the search warrant. *See* Suppression Hearing Transcript at pg. 161, lines 2-15.

15. On April 28, 2021, TFO Thornton applied for and obtained a search warrant signed by United States Magistrate Judge Kimberly E. West of the Eastern District of Oklahoma ordering Google to disclose additional location history data, before and after the collision, as well as any photos, messages, emails, queries, and other data held by Google pertaining to account XXXXXXXX6595. *See* Government's Suppression Hearing Exhibits 3, 4, 18, and 19; Suppression Hearing Transcript at pgs. 134-135, lines 18-25 and 1-14. In this search warrant, TFO Thornton requested records from Google for the time period of March 18, 2021 at 10:00am (CST) until March 25, 2021 at 10:00pm (CST). *See* Government's Suppression Hearing Exhibit 3 at Attachment B.

16. The defendant's cellular phone at the time of the collision on March 18. 2021, can be identified by the following:

    a. Both the phone number linked to the subscribing account information from the defendant's T-Mobile records and the "Recovery SMS" phone number included in the defendant's basic subscriber information is XXX-XXX-1695. *See* Government's Suppression Hearing Exhibits 15 and 22; Suppression Hearing Transcript at pgs. 196-199, lines 3-25, 1-25, 1-25, and 1-10.

    b. According to the defendant's T-Mobile records, the Phone Model was a "MOT G STYLUS 128G BLU TMUS KIT" and the "Device Number" for her phone and this phone model was 355539112046881. *See* Government's Suppression Hearing Exhibit 22; Suppression Hearing Transcript at pgs. 196-199, lines 3-25, 1-25, 1-25, and 1-10. This phone was not released until April 2020. *See* Government's Suppression Hearing Exhibit 23; Suppression Hearing Transcript at pgs. 196-199, lines 3-25, 1-25, 1-25, and 1-10.

17. According to Marlo McGriff, a Location History Product Manager at Google in March of 2020, "the user must opt into [Location History] in her account settings and enable 'Location Reporting'—a subsetting within [Location History]—for each particular device on which she wants to use [Location History]. And to actually record and save [Location History] data, the user must then sign into her Google account on her device and travel with that device. A single Google account can be associated with multiple devices, and the 'Location Reporting' feature within [Location History] allows users to select the specific devices on which they wish to enable [Location History]. In sum, [Location History] functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it. When a user takes the above-mentioned steps, the resulting data is communicated to Google for processing and storage. Google stores this data in a database internally referred to as 'Sensorvault.' Only [Location History] information is stored in Sensorvault." *See* Government's Suppression Hearing Exhibit 20 at pg. 5, ¶¶9-11; *see also* Suppression Hearing Transcript at pgs. 187-192, lines 8-25, 1-25, 1-25, 1-25, 1-25, and 1-19.

18. According to Marlo McGriff in July of 2020, if the defendant had her Location History turned on, she would have received a monthly "Timeline updates" email from Google summarizing her monthly Location History activity. *See* Government's Suppression Hearing Exhibit 24 at pgs. 8-9, ¶19 and footnote 4; *see also* Suppression Hearing Transcript at pgs. 192-194, lines 20-25, 1-25, and 1-13. On April 9, 2021, the defendant received a

monthly "Timeline updates" email from Google summarizing her March 2021 Location History activity. *See* Government's Suppression Hearing Exhibits 25 and 26.

19. As the owner of the Motorola cellular phone identified above, which used a number of Google services and applications, the defendant affirmatively opted-in to Google's use and storage of her location information. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122) ("You can also turn on Location History if you want to create a private map of where you go with your signed-in devices."). She also had the ability to delete her location history. *Id*. Additionally, she agreed to disclose her location information to Google for multiple purposes, including for Google to provide "personalized" services to her (including "content and ads" or "driving directions") and for Google to develop new services. *Id*. This opt-in process existed in April of 2020 and March of 2021. *See* Suppression Hearing Transcript at pgs. 194-196, lines 15-25, 1-25 and 1-2.

20. FBI Special Agent Jeremy D'Errico is a member of two specialty teams with the FBI. He is member of the FBI's Cellular Analysis Survey Team ("CAST") and its Child Abduction Rapid Deployment Team. *See* Suppression Hearing Transcript at pgs. 162-166, lines 16-25, 1-25, 1-25, 1-25, and 1-5; *see also* Government's Suppression Hearing Exhibit 21. CAST is a team that "specializes in conducting mobile device location, whether its through cell site location or call detail records or advanced timing events records or other information, such as records from Google Facebook or other providers that have location information." *Id*. Special Agent D'Errico has received over 300 hours of training in these areas, including advanced, certified training. *Id*. He also has specialized training in Google location history and has presented and instructed in this area. *Id*. He has presented on

Google location history 10-15 times to hundreds of local, state, and federal law enforcement officers, as it is part of the curriculum for the FBI's basic historical cell site class. *Id*. He has also briefed his CAST team on Google location history and has presented once or twice on the subject at the FBI's annual conference. *Id*. Other training and experience he has received on Google location history includes attending webinars, reading about Google's patented technology in this area, reading Google's privacy policy, reading court filings related to this issue, testifying in court on the issue and experimenting or testing data related to Google geofence data to understand the intricacies of it. *Id*. He has been involved in over 100 cases involving Google location history and Google geofence warrants as a subject matter expert and has testified approximately 15-20 times as an expert on Google location history. *Id*. at pgs. 167-169, lines 12-25, 1-25, and 1. Special Agent D'Errico also has a bachelor's degree in computer science from James Madison University and a master's degree in security informatics from John Hopkins University. *Id*. at pg. 167, lines 4-11; *see also* Government's Suppression Hearing Exhibit 21.

21. At the suppression hearing in this matter, Special Agent D'Errico concluded the following:

    a. The Google geofence in this matter was very tightly narrowed and tailored to where the criminal activity occurred. *See* Suppression Hearing Transcript at pgs. 171-172, lines 23-25 and 1-9.

    b. A three-step process was used in this matter, which is in conjunction with the three-step process outlined by Ms. Rodriguez from Google. *See* Suppression Hearing Transcript at pgs. 172-173, lines 17-25 and 1-6.

    c. The second step does not require the government to narrow its request or ask for contextual data. *See* Suppression Hearing Transcript at pg. 173, lines 7-9.

    d. A "unique device ID" is not unique across all of Google; it is only unique within an individual's account; and it is anonymized, which means law enforcement cannot identify who the device belongs to from the device ID number itself and can only identify who the device belongs to through requesting the information from Google. *See* Suppression Hearing Transcript at pg. 173-184, lines 16-25, 1-25, 1-

25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, and 1-5. In fact, Mrs. Rodriguez affidavit supports the fact that the device number is anonymized when she states, "[t]his deidentified 'production version' of the data includes a device number, the latitude/longitude coordinates and timestamp of the stored LH information, the map's display radius, and the source of the stored LH information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower)." *Id*. at pgs. 182-184, lines 25, 1-25, and 1-5; *see also* Government's Suppression Hearing Exhibit 20 at pg. 16, ¶8.

e. At the time of this Google geofence warrant, Google provided the anonymized data via a device ID or a Reverse Location Obfuscation ID ("RLOI"). *See* Suppression Hearing Transcript at pg. 184-185, lines 6-25 and 1-5. Both mechanisms are anonymized. *Id*.

f. The defendant had an Android phone at the time of the collision that was purchased no earlier than April 1, 2020. *See* Government's Suppression Hearing Exhibits 15, 22, and 23; Suppression Hearing Transcript at pgs. 196-199, lines 3-25, 1-25, 1-25, and 1-10. Because the defendant's phone was not released until April of 2020, the "phone had to go through a consent flow in order to enable Location Reporting on that device for Google to collect Location History information[,]" and she would have had to opt-in and enable the Location Reporting at a minimum. *Id*.; see also Government's Suppression Hearing Exhibit 20 at pg. 5, ¶¶9-11; Suppression Hearing Transcript at pgs. 235-236, lines 3-25 and 1-20.

g. There is no evidence that a false positive occurred in this matter. *See* Suppression Hearing Transcript at pg. 244, lines 5-10.

22. In October of 2018, Google had 592 million accounts in their Sensorvault database. *See* Suppression Hearing Transcript at pgs. 213-215, lines 12-25, 1-25, and 1-21; *see also* Defendant's Suppression Hearing Exhibit A1-6 at pg. 24, ¶3. This number may or may not have been different in March of 2021. *Id*. At that time, approximately one-third of Google users had Location History enabled on their accounts. *See* Defendant's Suppression Hearing Exhibit A1-6 at pg. 24, ¶3. Before Google provides "Device Ids" or "RLOI" information to law enforcement in response to a Google geofence search warrant, it searches all its accounts for the requested information. *See* Suppression Hearing Transcript at pgs. 213-215, lines 12-25, 1-25, and 1-21. This process is similar to the search process for an account number with a credit card company. *Id*. Google does not provide

data and information related to all 592 million accounts to the government in response to a Google geofence warrant and the government has no control or access to all those accounts. *Id*. at pgs. 243-244, lines 10-25 and 1-4.

23. Google's accuracy goal for a device being located within a display radius is 68%. *See* Suppression Hearing Transcript at pg. 61, lines 18-24. This is not a statistic, but a goal. *Id*. This goal is based on a combination of GPS, Wi-Fi, and cellular sources. *Id*. at pg. 79, lines 12-21. If the accuracy goal was based solely on a GPS source, it is possible that the accuracy goal may be higher. *Id*. The location source used in the defendant's case was GPS. *See* Government's Suppression Hearing Exhibit 11.

24. At the time this geofence warrant was issued by Magistrate Judge Shreder in 2021, geofence warrants were a novelty and a new area for law enforcement. *See* Suppression Hearing Transcript at pg. 151, lines 13-16. This was TFO Thornton's first Google geofence warrant. *Id*. at pg. 116, lines 11-23. However, prior to working on this search warrant, he did have significant experience writing and working on other types of search warrants. *Id*. at pgs. 139-140, lines 20-25 and 1-6. Prior to this geofence warrant and because of the novelty of it, TFO Thornton's training and experience identified in paragraphs 7 through 20 of his April 7, 2021 affidavit was limited and stemmed from his conversations with other law enforcement officers, including experienced investigators who had previously applied for Google geofence warrants, along with his own personal experience dealing with "Bluetooth" devices. *Id*. at pgs. 143-148, 155-157, 159, and 159-161, lines 23-25, 1-25, 1-25, 1-25, 1-25, 1, 15-25, 1-25, 1-2, 3-5, 16-25, and 1. One such officer he consulted with was from Springfield, Arkansas. *Id*. Prior to this warrant, TFO Thornton had no formal training on Google geofence warrants and was not an expert on geofence warrants. *Id*. As

confirmed by FBI Special Agent D'Errico, all substantive information contained in paragraphs 7 through 20 is true and correct. *Id*. at pgs. 158-159 and 239, lines 22-25, 1-2, and 11-21. Although TFO Thornton did not read the studies in paragraphs 24 and 25 of his April 7, 2021 affidavit, he does have law enforcement experience related to the information in the paragraphs and per FBI Special Agent D'Errico the information in the paragraphs related to the studies is correct. *Id*. at 148-150 and 239-240, lines 22-25, 1-25, 1-19, 22-25, and 1-8. Also, based on TFO Thornton's experience, the number of individuals driving a vehicle with a cell phone is likely greater than 88 out of 100. *Id*. Subsequent to this geofence warrant, TFO Thornton has applied for 10-15 other Google geofence warrants, all of which have been approved by a magistrate judge or the court. *Id*. at pgs. 116-117, lines 24-25 and 1-22.

25. AUSA Montoya is the AUSA with whom TFO Thornton worked with and collaborated with throughout the entire search warrant process. *See* Suppression Hearing Transcript at pgs. 123-125, 127-128, and 141-150, lines 13-25, 1-25, 1-16, 15-25, 1-5, 22-25, 1, 23-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, and 1-19. With the assistance of TFO Thornton, AUSA Montoya physically drafted the search warrant affidavit. *Id*. TFO Thornton typically consults with a prosecutor during the drafting of a search warrant to ensure it is "lawful" before it is presented to a judge. *Id*.

## III. CONCLUSIONS OF LAW

This issue is a matter of first impression for the Eastern District of Oklahoma and the Tenth Circuit has not addressed the issue. The Google geofence search warrant authorized location information associated with electronic devices that were within a geographical area approximately 1000' by 170', surrounding the scene of a fatal traffic collision between a vehicle and an individual

on a bicycle. The geofence warrant also authorized location information for these devices for a period two minutes before and two minutes after the collision. This Court should deny the defendant's motion to suppress for three separate and independent reasons.

First, the defendant lacked any protected Fourth Amendment privacy interest in the four minutes of location information that Google disclosed about her devices. Obtaining short-term location information is not a Fourth Amendment search under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc). In addition, even if this was a search under the Fourth Amendment, the defendant disclosed her location to Google to obtain location-based services, and the United States therefore did not violate the defendant's Fourth Amendment rights when it obtained that information from Google.

Second, the geofence search warrant complied with the Fourth Amendment because it was supported by probable cause and sufficiently particular. Regarding probable cause, the affidavit established that an individual on a bicycle was hit by a vehicle, the vehicle stopped for a moment and then fled the scene, and there was a fair probability that Google would store evidence of the crime. As to particularity, the warrant was appropriately tailored temporally and geographically to collect evidence related to the crime: it was limited to four minutes of location information for devices that were within a geographical area approximately 1000' by 170', surrounding the scene of a fatal traffic collision between a vehicle and an individual on a bicycle. The parameters of the geofence covered the location of the collision and public roadway area around it, but not any residences or buildings.

Third, suppression of evidence in this case is not appropriate because investigators reasonably relied in good faith on the geofence warrant. Suppression is inappropriate under *Leon*:

the warrant was not facially deficient or so lacking in probable cause that an investigator could not rely on it. Moreover, when TFO Thornton obtained the Google geofence search warrant in April of 2021, a Google geofence search warrant was a new investigative technique and there were no judicial opinions analyzing these types of search warrants. It was therefore reasonable for an investigator to rely on the Google geofence search warrant after consulting with counsel about the search warrant, consulting with other investigators about this type of search warrant, and then obtaining the search warrant from a magistrate judge.

**A. The defendant had no protected Fourth Amendment interests in any information disclosed pursuant to the Google geofence search warrant.**

The geofence search warrant information can be divided into three categories: four minutes of the defendant's location information, the defendant's subscriber identity information, and information pertaining to other Google customers. The defendant has not claimed that she had a protected Fourth Amendment interest in the latter two categories, and any such argument would be foreclosed by controlling precedent. *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (holding that Fourth Amendment rights "may not be vicariously asserted").

Nor does the defendant have any protected Fourth Amendment interests in the four minutes of information Google disclosed about her location. The Supreme Court has explained that the existence of protected Fourth Amendment interests in location information held by a third party lies "at the intersection of two lines of cases" – cases addressing "a person's expectation of privacy in his physical location and movements" and cases addressing "what a person keeps to himself and what he shares with others." *Carpenter*, 128 S. Ct. at 2214-16. Here, as discussed below, each of these two lines of cases provides independent reasons to conclude that Google's disclosure of four minutes of the defendant's location information did not infringe on her Fourth Amendment rights. The defendant bears the burden of establishing that she has a protected privacy interest in the

information she seeks to suppress, *see United States v. Daniels*, 41 F.4th 412, 415 (4th Cir. 2022), and she has not met that burden here.

***1. The defendant lacked protected Fourth Amendment interests in four minutes of information regarding her location.***

In *Carpenter v. United States*, 138 S. Ct. 2206, 2217 & n.3 (2018), 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 [a phone company's cell-site location information] constitutes a Fourth Amendment search." The Court emphasized that its decision was "a narrow one," and 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, or whether a cell tower dump constituted a search. *Id*. at 2217 n.3, 2220. These limitations are relevant here 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.* In short, *Carpenter* recognized a privacy interest only in certain long-term, comprehensive location information. Here, the geofence warrant sought information on all devices that were within a particular area during a particular interval.

Although *Carpenter* declined to resolve whether obtaining less than seven days of cell phone location information constitutes a search, *Carpenter's* reasoning demonstrates that obtaining four minutes of location information does not. The Court framed the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court cited its previous holding from *United States v. Knotts*, 460 U.S. 276, 282 (1983), that a person "on public thoroughfares has no reasonable expectation of

privacy in his movements from one place to another," *id*. at 2215, but it cautioned that *Knotts* had reserved whether this principle applied to "more sweeping modes of surveillance." *Id*. *Carpenter* emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id*. at 2216–17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time." *Id*. at 2220. Rather, the Court explained, the case concerned "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id*. at 2220. By this standard, the government did not conduct a search here when it obtained four minutes of the defendant's location information pursuant to the Google geofence search warrant.

*Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc) (hereinafter "*Leaders*"), confirmed the distinction between long-term and short-term location tracking. In *Leaders*, the Court held that a Baltimore aerial surveillance program, under which the city collected and retained for at least 45 days a "record of where everyone came and went within the city during daylight hours," was a search under *Carpenter*. *Id*. at 341, 346. *Leaders* held that "*Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns." *Id*. at 341. Under *Carpenter*, "[t]he latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant." *Id*. The 45-day surveillance period was not short-term because it exceeded "ordinary police capabilities": "[p]eople understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time." *Id*. at 345.

Here, the United States obtained only four minutes of the defendant's location information. This acquisition is consistent with ordinary police capabilities identified by *Leaders* – security cameras and being tailed. The search warrant's step 1 information is similar to security camera footage in that it captured the defendant's presence and movement in close proximity to the collision scene. Thus, under *Leaders*, the United States did not infringe the defendant's Fourth Amendment interests. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google showed her device's location for four total minutes.

Importantly, in assessing whether the government has conducted a search under *Carpenter* and *Leaders*, a court assesses the quantity of information accessed by the government, not the quantity of information possessed by the provider. This Court confirmed this analysis in *Leaders* when it found that "Carpenter was clear on that issue: a search took place 'when the Government accessed CSLI from the wireless carriers.'" *Leaders*, 2 F.4th at 344 (quoting *Carpenter*, 138 S. Ct. at 2219). Under *Carpenter* and *Leaders*, Google's retention of information about the defendant does not transform the government's acquisition of a small portion of that information into a search.

In addition, in numerous cases involving other sophisticated new technologies, lower courts held that *Carpenter* protects only comprehensive, long-term location information. For example, the Seventh Circuit held that real-time tracking of a specified cell phone over a period of approximately six hours was not a search. *See United States v. Hammond,* 996 F.3d 374, 387-92 (7th Cir. 2021). The Seventh Circuit previously determined that a cell tower dump was not a search, and two other district courts reached the same result. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))"

(emphasis in original)); *United States v. Walker*, 2020 WL 4065980 at *8 (W.D.N.C. July 20, 2020) (concluding that the "privacy concerns underpinning the court's holding in *Carpenter* do not come into play" for a cell tower dump, which is limited to "particular *place* at *a limited time*") (emphasis in original)); *United State v. Rhodes*, 2021 WL 1541050 at *2 (N.D. Ga. Apr. 20, 2021) (stating that *Carpenter* "centrally relied on the strong Fourth Amendment privacy interests implicated when law enforcement monitors or obtain voluminous, detailed cell phone information of a person's physical presence compiled over a lengthy period that effectively delineates the contours of the individual's life and communications"). These cases all support the conclusion that the United States did not infringe on the defendant's Fourth Amendment interests when it obtained four minutes of her location information from Google.

Similarly, courts have rejected a broad interpretation of *Carpenter* in cases involving automatic license plate reader databases, which record the time and place a license plate is observed. Obtaining a large amount of location information about an individual from such a database could potentially implicate *Carpenter*'s concerns regarding comprehensive location information. But investigators do not conduct a search when they obtain only a small quantity of location information from such a database. *See Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) ("[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case."); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under *Carpenter*

because "the information in the database did not reveal 'the whole of [Yang's] physical movements.'").

Four Minutes of location data is only 1/2520th of the period that *Carpenter* held constituted a search, and it does not provide the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court. *Carpenter*, 138 S. Ct. at 2217. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google provided a summary of her location for a short time period. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

The defendant's additional *Carpenter*-related arguments do not establish that the United States infringed her reasonable expectation of privacy. The Supreme Court in *Carpenter* stated that cell-site information "is rapidly approaching GPS-level precision," and *Carpenter*'s holding "t[ook] account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218-19. Thus, because the Supreme Court grounded *Carpenter*'s holding in an assumption that cell-site information would approach the precision of GPS, any distinction in precision between them cannot create enhanced Fourth Amendment protections for GPS information.

Geofence information is indistinguishable from a wide variety of other business records, or even from witness testimony. For example, credit card records, landline telephone records, employee time sheets, and IP address records may enable law enforcement to retrospectively locate individuals at particular points in time. However, like the geofence information, none of these records provide a comprehensive inventory of the whole of a person's movements, and the United States does not infringe the privacy interest protected by *Carpenter* when it obtains them.

*See, e.g.*, *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019) (unpublished) (holding that defendant had no reasonable expectation of privacy in IP address information, even after *Carpenter*).

***2. The defendant lacked protected Fourth Amendment interests in location information she disclosed to Google to obtain location-based services.***

There is a second, independent reason why the defendant had no protected Fourth Amendment interests in the location information Google disclosed to the United States – the defendant voluntarily disclosed information about the location of her phone to Google to obtain location-based services. Thus, Google's disclosure of that information to the government is governed by the long-standing principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *United States v. Miller*, 425 U.S. 435, 443 (1976).

In cases ranging from private conversations to business records, the Supreme Court has repeatedly held that the Fourth Amendment does not protect information voluntarily revealed to a third party and then conveyed by the third party to the government. For example, 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). Furthermore, it applies to information disclosed to an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36 (1973).

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. First, the Court stated that "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. In addition, 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. And in this case, this principle applies to the location information the defendant disclosed to Google to obtain location-based services.

In *Carpenter*, the Supreme Court held that the third-party doctrine did not apply to a phone company's cell phone location information, but the Court did not reject the third-party doctrine or "disturb the application of *Smith* and *Miller*." *Carpenter*, 138 S. Ct. at 2220. Instead, *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company for three reasons: first, the phone company collects cell-site information "without any affirmative act on the part of the user beyond powering up," second, "there is no way to avoid leaving behind a trail of location data," and third, carrying a cell phone "is indispensable to participation in modern

society." *Id*. at 2220. These three factors are not present for Google's Location History service. First, Location History is off by default and a user must opt into it. In fact, Google could not obtain and store the defendant's device location without her undertaking multiple affirmative acts, including signing into Google on her phone, enabling the phone's device location setting, enabling Location Reporting, and opting into Location History. Second, the defendant also had discretion to delete any or all of her Location History. Finally, none of the services associated with Google's storage of Location History are indispensable to participation in modern society. In fact, according to October 2018 data, approximately two-thirds of Google's users rejected those services. Furthermore, *Carpenter's* holding was based on facts specific to the cell phone provider context that Carpenter had not voluntarily disclosed his cell phone location information to the phone company, but it did not otherwise reverse or limit the third-party doctrine. *See Carpenter*, 138 S. Ct. at 2220. Thus, if this Court determines that the defendant voluntarily disclosed her location to Google, this Court must conclude that the defendant had no reasonable expectation of privacy in the location information the United States obtained from Google, as "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44.

The defendant's voluntary disclosure of her phone's location to Google is evident from the nature of the relationship between Google and its users – users must provide their devices' location to Google to obtain location-based services. Courts often infer that an individual disclosed information to a third-party based on the nature of the relationship between the individual and the third party. For example, in *Miller*, the Supreme Court did not consider Miller's explicit agreements with his bank. Instead, the Court determined that Miller disclosed financial information to the bank by "examin[ing] the nature of the particular documents sought" and

concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442. Similarly, in *Smith v. Maryland*, the Court held that "[a]ll 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." *Smith*, 442 U.S. at 742. The Ninth Circuit recently applied this analysis to disclosure of location information in *Sanchez v. Los Angeles Dep't of Transportation*, 39 F.4th 548 (9th Cir. 2022), in which the court rejected a Fourth Amendment challenge to a Los Angeles regulation mandating that e-scooter companies disclose to its transportation department real-time location data for every scooter. The court explained that when one "rents an e-scooter, he plainly understands that the e-scooter company must collect location data for the scooter through its smartphone applications. Thus, the voluntary exposure rationale fits far better here than in *Carpenter*." *Id*. at 559. Furthermore, the Supreme Court has held that if one discloses information to a third party, the third party's storage decisions lack constitutional significance. *See Smith*, 442 U.S. at 745 (stating that a phone company's choice to store dialed telephone number information did not "make any constitutional difference" because the defendant "voluntarily conveyed to it information that it had facilities for recording and that it was free to record").

The same reasoning applies here. Google customers disclose their devices' locations to Google to obtain services that depend on Google knowing their specific location, such as mapping, traffic updates, help finding their phones, and help with their commutes. Google also uses location information to target advertisements to users via radius targeting, store visit conversions, and inferences drawn from Location History. These services demonstrate that Google is not merely providing a storage service for users to store their own location information. Based on a user's location, Google provides services that are helpful to the user, to other users, to advertisers, and to

Google itself. In sum, a user of Google's location services does not keep his or her location private; instead, the user shares location information with Google to obtain location-based services. Thus, the user's Fourth Amendment interests are not infringed when Google discloses his or her location information to the government.

Additionally, the defendant had no reasonable expectation of privacy in Google's records of her location because she voluntarily conveyed her location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, the defendant had previously taken an affirmative step to disclose her location information to Google. Specifically, the defendant could not have successfully opted in without Google presenting the supported consent flow language to her by making her opt-in and enable Location History and/or Location Reporting. Moreover, she agreed that Google would have access to her location information for purposes ranging from providing her 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 the defendant voluntarily disclosed her location information to Google, and the United States did not infringe on her reasonable expectation of privacy when it obtained from Google information her device's location(s) during a four-minute interval.

The fact that the defendant voluntarily disclosed her location information to Google is also 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 her location information, the defendant had to affirmatively opt in, and she also retained the ability to delete her 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. The defendant thus voluntarily disclosed her location information to Google, and Google's disclosure of that information to the United States did not infringe upon her reasonable expectation of privacy.

Google's Privacy Policy further supports the fact that the defendant voluntarily disclosed her phone's location information to Google. Courts rely on privacy policies in evaluating whether a customer discloses information to a service provider. *See, e.g., Sanchez*, 39 F.4th at 559 (stating that e-scooter user "must agree to the operator's privacy policies," which allow collection and storage of location data).

Finally, the defendant claims that obtaining her information from Google constitutes a search under "a property-based theory of the Fourth Amendment" is rooted in Justice Gorsuch's solo dissent in *Carpenter*, where he discussed a transformation of the Fourth Amendment that would jettison not only *Smith* and *Miller*, but also the reasonable expectation of privacy test of *Katz v. United States*, 389 U.S. 347 (1967). *See Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J.,

dissenting). The defendant's argument is based on Google's statement in its Amicus Brief in *Chatrie* that "'Location History' is not a business record, but a journal of a user's location and travels that is created, edited and stored by and for the benefit of Google users who have opted into the service[,]" thus allegedly making Google a "mere bailee" of the defendant's data. See Defendant's Suppression Hearing Exhibit A1-6 at pg. 687. This argument is flawed. First, there is no "property rights" exception to the third-party doctrine. *See* Couch v. United States, 409 U.S. 322, 328-29 (1973) (an individual cannot exercise a property right privilege when a summons or order is directed at a third-party and privilege does not exist). Second, Google is not just a "mere bailee" that stores location information for users. At no point does the user have sole discretion on how their Location History is used. With limitations, Google can also actively use the user's location information, such as providing services to its users, advertisers, and other users. Ultimately, Justice Gorsuch concluded that *Carpenter* forfeited this argument because he did not raise it. *See id.* at 2272. Regardless, a solo dissent is not the law, and *Smith*, *Miller*, and *Katz* remain binding on this Court.

Under existing law, Google's disclosure of location information to the United States did not infringe upon any reasonable expectation of privacy nor did the government conduct a search under the Fourth Amendment when it obtained this location information from Google.

**B. The geofence warrant complied with the Fourth Amendment.**

This Court should deny the defendant's suppression motion on the basis that the warrant complied with the Fourth Amendment. A warrant satisfies the Fourth Amendment if it is: (1) supported by probable cause; (2) sufficiently particular; and (3) issued by a neutral and disinterested magistrate judge. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). Here, the

affidavit established a fair probability that Google would have evidence of the crime, and the warrant described that evidence with mathematical precision.

***1. 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." *United States v. Reed*, 195 Fed.Appx. 815, 821 (10th Cir. 2006) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (unpublished opinion); *see also United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019). It is "not a high bar." *Bosyk*, 933 F.3d at 325 (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). In addition, this Court does not conduct de novo review concerning the existence of probable cause: a "judge's 'decision to issue a warrant is entitled to great deference,' and we 'need only ask whether, under the totality of the circumstances presented in the affidavit, the … judge had a 'substantial basis' for determining that probable cause existed.'" *Perrine*, 518 F.3d at 1201 (quoting *United States v. Artez*, 389 F.3d 1106, 1111 (10 Cir. 2004); *see also United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39) ("the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.").

Here, the affidavit in support of the warrant provided an ample basis for the issuing magistrate judge's finding of probable cause. In particular, the affidavit established that:

(a) an unknown subject was involved in a fatal traffic collision with an individual on a bicycle;

(b) the unknown subject driving the vehicle that was involved in the collision stopped the vehicle seconds after the collision and then subsequently fled the crime scene;

(c) Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device;

(d) Google offers numerous apps and online-based services, including messaging and calling (e.g., Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (e.g., Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed into their Google accounts;

(e) Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices;

(f) Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time;"

(g) The location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a 'maps display radius,' for each latitude and longitude point;

(h) Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location- based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google

account or by enabling auto-deletion of their Location History records older than a set number of months;

(i) A vast majority of motorist not only own but use their smartphones while driving; and

(j) A significant number of collisions occur as a result of distracted driving from a variety of sources, including cellphone use[,]" and "persons involved in a collision often use their cellphone immediately or shortly after a collision if not to call emergency services, then to call family members or friends. This information gave the magistrate a substantial basis to conclude that there was a fair probability that Google possessed evidence related to the robbery. Indeed, although the district court found that the warrant lacked probable cause as to other users within the geofence, it did conclude that "a fair probability may have existed that the Geofence Warrant would generate the suspect's location information."

*See* Government's Suppression Hearing Exhibit 8 at ¶¶11-25.

Moreover, the Supreme Court broadly construes what may constitute evidence for purposes of a search warrant. In *Messerschmidt v. Millender*, 565 U.S. 535, 539 (2012), police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. The Court provided multiple reasons why "all gang-related materials" could be seized as evidence in connection with someone shooting at his ex-girlfriend, including that the materials could "help to establish motive," could be "helpful in impeaching [the shooter]," could be helpful in "rebutting various defenses," and could "demonstrat[e] [the shooter's] connection to other evidence." *Id*. at 551-52.

Similarly, the issuing magistrate judge here had multiple reasons to believe that location information for those present at the crime scene would constitute evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the collision. They could use it to identify the unknown suspect driving the vehicle. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate

and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the unknown subject driving the vehicle, including an attempt by the individual to blame someone else for his or her crime. Thus, probable cause existed because the information sought by the warrant was in fact evidence appropriately seized pursuant to a search warrant.

The Supreme Court's decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), sets forth the probable cause analysis applicable here. In *Zurcher*, the Supreme Court approved a search warrant that authorized the search of a newspaper's office to seize photographs of a crime scene at which unidentified individuals had assaulted police officers. *See id*. at 551, 553-560. That warrant was analogous to the one here – it authorized seizure, from a third party not suspected of crime, of crime-scene evidence to identify perpetrators and others present at the scene of a crime. The Court held that "[t]he critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Id*. at 556. A search warrant "may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id*. at 559.

The defendant argues that the search warrant in this case fails to establish particularized probable cause specific to her, but her analysis is inconsistent with the *Zurcher* standard. In *Zurcher*, the Supreme Court held "[i]n situations where the State does not seek to seize 'persons' but only those 'things' which there is probable cause to believe are located on the place to be searched, there is no apparent basis in the language of the Amendment for also imposing the requirements for a valid arrest—probable cause to believe that the third party is implicated in the crime." *Id*. at 554.

Furthermore, the Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). The defendant therefore lacks standing to challenge the United States' acquisition of others' location information. *See, e.g., United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting a defendant's argument that investigator's use of a cell-site simulator violated the privacy rights of third parties, because the defendant was "not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated"). Additionally, these other individuals also voluntarily disclosed their location information to Google. Therefore, Google's disclosure of other individuals' location information pursuant to the geofence warrant did not infringe their Fourth Amendment rights either.

The defendant also relies on *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), in which the Supreme Court held that the probable cause that supported a warrant to search a tavern and its bartender for drugs did not extend to a search of tavern patrons. But *Ybarra* and its progeny explicitly address limitations on physical searches of persons pursuant to warrants, not the standard for searching property (such as the information here) for evidence. As *Ybarra* stated, "Where the standard is probable cause, a search or seizure *of a person* must be supported by probable cause particularized with respect to that person." *Ybarra*, 444 U.S. at 91 (emphasis added). The geofence warrant authorized obtaining evidence from Google about a crime scene; it did not authorize the arrest, search, or seizure of any person.

*Ybarra* is thus an exception to the general rule for search warrants, which is that "a lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search." *United States v. Ross*, 456 U.S. 798, 820-21 (1982). *Ybarra* and its

progeny do not apply here because no persons were arrested, searched, or seized pursuant to the Google geofence search warrant. Here, the search warrant affidavit established a fair probability that Google had evidence of the collision in its records which it accessed and used to provide services to its users and advertisers, and that probable cause supported issuance of the search warrant.

*Illinois v. Lidster*, 540 U.S. 419 (2004), further demonstrates that the Fourth Amendment permits investigators to collect identity information of those present at crime scenes. In *Lidster*, the Court held that police did not violate the Fourth Amendment when they set up a roadblock to briefly seize all motorists at the scene of a hit-and-run a week after the crime, for the primary purpose of finding witnesses. *See id*. at 423, 428. The Court found that the roadblock was "appropriately tailored ... to fit important criminal investigatory needs" and that the stops "interfered only minimally with liberty of the sort the Fourth Amendment seeks to protect." *Id*. at 427. It would be very strange for the Fourth Amendment to allow physical stops, without individualized suspicion, of all persons at a crime scene a week after the crime, but not allow issuance of a search warrant to obtain direct crime-scene evidence, without the physical seizure of any person, merely because the crime scene information revealed the presence of persons other than the perpetrators.

Although at this time no federal appellate court has issued an opinion as to Google geofence search warrants, the Eighth Circuit in *United States v. James*, 3 F.4th 1102 (8th Cir. 2021), held that a series of cell tower dump search warrants used to solve a series of robberies complied with the Fourth Amendment. Cell tower dump search warrants are similar to Google geofence search warrants, insofar as they require a phone company to provide the government with information about all cellular devices that used cell towers in the vicinity of a crime, but their geographic

coverage is typically much larger than Google geofence search warrants.[1] In *James*, the Eighth Circuit concluded that probable cause supported the cell tower dump search warrants because "there was 'a fair probability' that the cellular-tower records would identify the robber." *Id*. James's probable cause analysis supports the issuance of the Google geofence search warrant in this case.

Finally, all that is required for probable cause is a fair probability that evidence will be found in the place to be searched. *See Gates*, 462 U.S. at 238. In addition, a magistrate judge may "draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant." *Id*. at 240. Here, the magistrate judge's finding of probable cause was based on a combination of specific facts (there was a collision between a vehicle and individual on a bicycle; the driver of the vehicle stopped within seconds of the collision; and the driver subsequently fled the crime scene after the stopping) and reasonable inferences (that there was a fair probability that Google stored location evidence pertaining to this crime). Search warrants commonly rely on a combination of specific facts and reasonable inferences, and the defendant cites no contrary case law. For example, in *United States v. Jones*, 942 F.3d 634, 639-40 (4th Cir. 2019), the court held that a magistrate judge had made a reasonable inference that evidence of a defendant's threats would be found at his home. Here, the magistrate judge similarly made a reasonable inference that Google stored evidence of the crime.

***2. The geofence warrant was sufficiently particular.***

First, the geofence warrant did not remotely resemble a general warrant. A general warrant "specified only an offense—typically seditious libel—and left to the discretion of the

[1] For example, the cell-sites in *Carpenter* placed the defendant in sectors "ranging from one-eighth to four square miles." *Carpenter*, 138 S. Ct. at 2218. The geofence here covered a geographical area approximately 1000' by 170'.

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 Google geofence search warrant in this case authorized the United States to obtain from Google limited and specified information directly tied to a particular criminal offense at a particular place and time. As set forth below, because the search warrant was supported by probable cause and specified its object with particularity, the defendant's argument that the warrant was a general warrant is without merit.

More broadly, the facts of this case illustrate why a warrant that requires disclosure of information about devices in a particular place at a particular time is not a general warrant. When TFO Thornton sought the Google geofence search warrant, he was investigating a serious crime, and he had reason to believe that the perpetrator knowingly fled the scene after hitting someone on a bicycle. The search warrant allowed him to solve the crime and protect the public by examining a remarkably limited and focused set of records from Google – location information over a four-minute interval of the defendant and two other individuals. This investigative technique involved no unreasonable search or seizure and should be encouraged, not condemned.

Second, under the Fourth Amendment, a valid warrant "must particularly describe the things to be seized, as well as the place to be searched." *Dalia v. U.S.*, 441 U.S. 238, 239 (1979); *see also Mink v. Knox*, 613 F.3d 995, 1003 (10 Cir. 2010); *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017). The "particularity requirement ensures that a search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause." *U.S. v. Pulliam*, 748 F.3d 967 (10th Cir. 2014) (quoting *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985). The particularity requirement also constrains a warrant so that it is "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d

463, 473 (4th Cir. 2006). Furthermore, "[t]he particularity requirement 'ensures that the search will be carefully tailored to its justifications and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.'" *United States v. Otero*, 563 F.3d 1127, 1131-32 (10 Cir. 2009) (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). In essence, it protects against "exploratory rummaging in a person's belongings." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *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)). Here, the Google geofence search warrant satisfied these requirements.

Here, the geofence warrant specified with precision the items to be seized – four minutes of location information associated with electronic devices that were, during the two minutes on either side of the fatal traffic collision, within a geographical area approximately 1000' by 170' surrounding the location of the collision. In addition, the warrant was sufficiently particular because it was appropriately constrained based on location, dates, and times. The geofence boundary was based on specific features of the site of the collision and appropriately tailored towards its investigatory purposes, which was to obtain evidence to help identify the driver of a vehicle who struck an individual on a bicycle. In addition, the duration of the geofence enabled investigators to distinguish between the suspect, victim, and other witnesses.

The Eight Circuit's decision in *James* further confirms that the warrant here was not overly broad and sufficiently particular. Although tower dump search warrants typically cover broader areas than geofence warrants, the court held that the tower dump search warrants were appropriately "constrained—both geographically and temporally—to the robberies under

investigation." *James*, 3 F.4th at 1106. In particular, because the tower dumps "covered only the cellular towers near each robbery" for a "narrow and precise" 90-minute period, "the warrants were 'sufficiently definite' to eliminate any confusion about what the investigators could search." *Id*. This reasoning is fully applicable here – the geofence warrant was appropriately constrained in space and time to obtain evidence of the traffic collision. Indeed, the location information obtained from Google was more narrowly constrained than the location information in *James*. The target geographical area of 1000' by 170' identified in the geofence warrant is smaller than most cellular sites, and the United States only obtained location information regarding three individuals, rather than hundreds or thousands.

The defendant also challenges the geofence warrant because it included a "two-step" process for executing the warrant that leaves discretion of whose data to search and seize to law enforcement. The geofence warrant, however, established probable cause for all the evidence that law enforcement could have obtained – identity information and four minutes of location data for all individuals present at or near the scene of the traffic collision. The information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, 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.

Although TFO Thornton had discretion to narrow the information obtained from Google in the three-step process, the Fourth Amendment does not require this narrowing because the Google geofence search warrant was supported by probable cause to seize four minutes of location and basic identity information for anyone at the site of the collision during the four-minute interval. As one magistrate judge explained in issuing a Google geofence search warrant, "the government

has established probable cause to seize all location and subscriber data within the geofence locations identified. Whether it chooses to obtain all that information, or partial information, is of no matter to the Court's consideration of the constitutionality of the warrant under the Fourth Amendment." *In re Search Warrant Application*, 497 F. Supp. 3d 345, 362 (N.D. Ill. 2020).

Even if there was a particularity problem with the three-step process for the Google geofence search warrant because of the "narrowing" discretion it gave to the government, the appropriate remedy would at most be to sever the paragraphs of the search warrant allowing this "narrowing" discretion and the information received in that step. "Under the severance doctrine, the constitutionally infirm portion of a warrant—usually for lack of particularity or probable cause—is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted." *Cobb*, 970 F.3d at 330 (internal quotation marks omitted).

Here, step 2 of the Google geofence search warrant contained narrowing, discretionary language. However, TFO Thornton did not utilize this "narrowing" function of the search warrant because he reasonably believed the location information he received from Google pursuant to step 1 of the search warrant belonged to the unknown suspect driving the vehicle westbound that was involved in the collision or potential witnesses to the crime. There was no need to narrow the devices. Thus, any subsequent evidence against the defendant obtained as a result of the location and identity information obtained pursuant to the search warrant's three-step process in this case would not be the fruit of the poisonous tree.

Similarly, the most-heavily litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that

component did not violate the Fourth Amendment. Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that "in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016). It is important to note that eleven Courts of Appeals have considered various challenges to the *Playpen* warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) ("[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called 'NIT warrant.' Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed."); *see also United States v. Wagner*, 951 F. 3d 1232 (10th Cir. 2020); *United States v. Cookson*, 922 F.3d 1079 (10th Cir. 2019); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017).

Some defendants argued that the discretion given the FBI in executing the *Playpen* warrant violated the Fourth Amendment's particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that "the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site." *See also Anzalone*, 208 F. Supp. 3d at 368 ("Every court to consider this question has found the NIT search warrant sufficiently particular."). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is

immaterial, as the geofence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the scene of the traffic collision.

Additionally, the defendant complains that the Google geofence search warrant required Google to filter its entire Sensorvault database to find location information responsive to the search warrant, but this argument is without merit. This database contains all the Location History for Google's account holders. In October of 2018, the number of accounts in the Sensorvault database was 592 million. The current number is unknown. In the context of Google geofence search warrants, "the relevant question is not how Google runs searches on its data, but what the warrant authorizes the Government to search and seize." *United States v. Rhine*, 2023 WL 372044, at *28 (D.D.C. Jan 24, 2023) (upholding geofence warrant). Otherwise, "no doubt many search warrants and most third-party subpoenas for protected records would be unconstitutionally overbroad because they necessarily would require the third party to search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server." *Id*. Filtering a large database to find a narrow set of information is not new – for example, in response to a subpoena, a phone company may review every call made by all its customers in order to find calls made to a specified phone number. *See Ameritech Corp. v. McCann*, 403 F.3d 908, 910 (7th Cir. 2005).

The nature and uses of Google's Sensorvault database confirm that, if necessary, it is appropriate for a search warrant to seek a narrow subset of information from within that database. Google accesses this information freely to provide users and advertisers with location-based services. Google geofence search warrants are similar to radius targeting advertising and measurement of store visit conversions, as they involve determinations of whether users' devices are in specific locations at specific times. The Fourth Amendment does not prohibit Google, in

response to a search warrant, from filtering information in a manner similar to the way it uses the same information for its own business purposes.

Furthermore, at no point did the government ask for the location and identity information for all account holders in Google's Sensorvault database. Nor did the government ask Google to filter through all its account holders in the database. Google's filtering of a large set of data to comply with the Google geofence search warrant is a result of Google's internal data storage practices, not an overbroad warrant. The constitutionality of a search warrant does not depend on a service provider's internal data-storage practices, which are invisible to customers and the government alike. For example, in *Smith v. Maryland*, the Supreme Court held that a phone company's internal practices regarding storage of dialed number information did not "make any constitutional difference." *Smith*, 442 U.S. at 745. Here, the appropriate measure for the breadth of the Google geofence search warrant is the records sought by the search warrant, not the size or organization of Google's Sensorvault database.

Lastly, the defendant cannot demand any exacting scrutiny of the Google geofence search warrant merely because she was involved in a collision with an individual on a bicycle that resulted in that individual's death, because Fourth Amendment rights may not be vicariously asserted. *See Rakas*, 439 U.S. at 133-34. In any event, the geofence warrant satisfied the Fourth Amendment under the standards of *Zurcher* because it was issued based on probable cause and specified its objects with particularity.

**C. The good-faith doctrine precludes suppression.**

Even if the defendant could identify a Fourth Amendment flaw in the search warrant, and even if the defendant could establish a protected Fourth Amendment interest in the information disclosed by Google, suppression would not be an appropriate remedy. Suppression is a remedy

of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence 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.

***1. TFO Thornton reasonably relied on the geofence warrant.***

Suppression is inappropriate under the good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984). When officers act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate, "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 "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; (2) 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"; (3) when "the issuing magistrate wholly abandoned his judicial role"; and (4) 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." *Leon*, 468 U.S. at 923; *United States v. Perez*, 393 F.3d 457, 461 (4th Cir. 2004). These circumstances are not present in this case.

a. The search warrant was not so lacking in probable cause as to render reliance on it unreasonable.

The defendant argues that the Google geofence search warrant was devoid of probable cause, but the affidavit demonstrates otherwise. As an initial matter, "the threshold for establishing this exception is a high one" because "[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority." *United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt*, 565 U.S. at 547). As explained above, the warrant was supported by probable cause because the affidavit established that the suspect driver hit an individual on a bicycle, the suspect driver stopped within seconds after the collision, and then subsequently fled the crime scene, and it explained why there was a fair probability that Google would store cell phone users' location information. In addition, given the layout of the crime scene, the radius of the geofence was reasonably tailored to specifically collect evidence of the crime. That is sufficient to show that TFO Thornton's reliance on the warrant was reasonable.

The defendant's numerous additional objections to the probable cause that supported the Google geofence search warrant lack merit. First, the defendant references *Ybarra* and related cases, but the probable cause standards of *Ybarra* do not apply to a Google geofence search warrant because this type of warrant does not involve an arrest, search, or seizure of a person. However, even if this Court ultimately decides that *Ybarra* govern Google geofence search warrants, TFO Thornton could reasonably have relied on the search warrant, given the probable cause standard of *Zurcher* and the lack of case law applying *Ybarra* to Google geofence search warrants.

Second, although the defendant analogizes Google to a multi-unit building, this analogy is confusing and misleading. The search warrant appropriately required Google to disclose particular information specific to a certain time and place. Moreover, given the lack of contrary precedent,

it was not unreasonable for TFO Thornton to rely on the warrant based on the actual information sought by the warrant, rather than on Google's internal filtering processes.

Third, the defendant challenges the inferences that supported the Google geofence search warrant, but her challenge is meritless because a magistrate judge may "draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant." *Gates*, 462 U.S. at 240. Here, TFO Thornton included in the search warrant a combination of specific facts (including the suspect driver's vehicle hitting the victim, stopping seconds after the collision, and then subsequently fleeing the crime scene) and reasonable inferences regarding why Google would store evidence of the phone's location and why the driver of the suspect vehicle likely had a cell phone with him or her at the time of the collision. Although the defendant argues that TFO Thornton's lack of training and experience with these types of search warrants and the fact he did not read a couple of surveys somehow prohibited Magistrate Judge Shreder from drawing reasonable inferences from this information, she provides no evidence to show that the facts within the search warrant that led to these reasonable inferences were not substantively true and correct. In fact, FBI Special Agent D'Errico, an expert on Google geofences, confirmed that each of these facts related to Google and the surveys identified in the search warrant were true and correct. Therefore, Magistrate Judge Shreder and TFO Thornton's reliance on the search warrant was reasonable.

b. <u>The warrant was not facially deficient.</u>

The Google geofence search warrant was not facially deficient that TFO Thornton could not reasonably rely on it. It was specifically tailored in both time and space. The search warrant was limited to disclosure of location information over a four-minute interval, as well as accompanying identity information, for devices present within a small, defined radius of the site

of the collision that did not include any residences or buildings. Those limitations are more than sufficient for an officer to reasonably rely on the facial validity of the warrant.

c. The magistrate judge did not abandon his judicial role.

Magistrate Judge Shreder did not abandon his judicial role in analyzing and approving the Google geofence search warrant in this case. In fact, the evidence shows that he did quite the opposite. Magistrate Judge Shreder asked TFO Thornton to reduce the time interval from 10 minutes, or five minutes on each side of the collision time, because he thought it was too large a period of time. Once it was reduced to four minutes, or two minutes on each side of the collision time, Magistrate Judge Shreder approved the search warrant. He then proceeded to consider the search warrant a third time when the "time restriction" language was removed from the affidavit and Attachment B. Magistrate Judge Shreder was actively performing his judicial role throughout the search warrant application process.

d. The magistrate judge was not misled by information in the search warrant.

The defendant argues that TFO Thornton recklessly and intentionally misled Magistrate Judge Shreder in his affidavit by not being truthful about his training and experience related to Google, he intentionally omitted necessary facts related to Google that he should have included in the affidavit, and he misrepresented his knowledge about the surveys identified in the affidavit. Essentially, the defendant is asserting a *Franks* violation against TFO Thornton, despite the fact she did not allege a *Franks* violation in her motion to suppress.

Although the defendant did not allege a *Franks* violation in her motion to suppress or establish facts necessary to be entitled to a *Franks* hearing, the United States will address the defendant's *Franks* allegations made during the Motion to Suppress hearing. Under *Franks v. Delaware*, 438 U.S. 15 (1978), "Fourth Amendment violation occurs if '(1) an officer's affidavit

supporting a search warrant application contains a reckless misstatement or omission that (2) is material because, but for it, the warrant could not have been lawfully issued.'" *United States v. Moses*, 965 F.3d 1106, 1110 (10th Cir. 2020) (citations omitted).

TFO Thornton did not mislead Magistrate Judge Shreder. At the suppression hearing, TFO Thornton testified that his training and experience related to paragraphs 7 through 20 of the affidavit about Google was limited to talking to other investigators that had done Google geofence search warrants and his personal knowledge in dealing with bluetooth. Furthermore, he testified that in preparing the search warrant application, he worked directly with AUSA Montoya, who physically drafted the affidavit. FBI Special Agent D'Errico, an expert on Google geofences, testified that each of these facts related to Google identified in the search warrant were true and correct.

Due to the novelty of these types of warrants at the time, TFO Thornton's training and experience would be expected to be limited or minimal. TFO Thornton took affirmative steps in consulting with AUSA Montoya who drafted the affidavit in order to prepare a search warrant application that established probable cause. Thornton's affidavit was not knowingly false nor did Thornton display a reckless disregard for the truth. Any alleged misstatements made by TFO Thorton pertaining to his training and experience are immaterial to the substance of the affidavit and do not affect the probable cause determination made by Magistrate Judge Shreder.

Other federal courts have addressed this argument in the context of motions to suppress Google geofence search warrants. In those cases, the courts have not found bad-faith when an affiant is accused of misstating his training and experience in the search warrant affidavit. *See United States v. Smith*, 2023 WL 1930747 at *12 (N.D. Miss. February 10, 2023) (motion to suppress denied even though affiant officers lacked prior training and experience related to Google

geofence search warrants); *United States v. Carpenter*, 2023 WL 3352249 (M.D. Florida February 28, 2023) report and recommendation adopted by the District Court, 2023 WL 2910832 (M.D. Florida April 12, 2023) (motion to suppress denied even though affiant officer lacked training related to Google geofence search warrants; the affiant officer did not mislead the magistrate judge even though the affidavit included language such as "based on my training and experience, I know" before each Google-related fact in his affidavit).

Second, as for the Google omissions, the defendant faults TFO Thornton for not informing the magistrate judge about Google's internal data filtering process and the number accounts Google internally searches, Google's 68% accuracy goal, the fact that false positives and false negatives in location information is possible, and there are no specific Google location statistics for the area around the geofence in this case. However, these facts lack Fourth Amendment significance, and it is impossible for Google's internal filtering process to produce Google location statistics for any specific area. To the extent that the defendant is arguing that the affidavit should have addressed potential inaccuracies (false positives and false negatives) in Google's location information, the fact that there is imprecision in cell phone location measurements is common knowledge, and it could reasonably be expected that Magistrate Judge Shreder would be aware of that fact at the time he approved the search warrant. Nor would potential inaccuracies in location data affect the existence of probable cause because potential inaccuracies would ultimately go to the weight of location information at trial, not its admissibility. Therefore, TFO Thornton did not intentionally or recklessly omit material information from the affidavit by not including these facts and did not commit a *Franks* violation.

Lastly, as to TFO Thornton's knowledge of the surveys referenced in paragraphs 24 and 25 of his affidavit, he admitted to not reading them. However, this does not mean that he

intentionally or recklessly omitted material information from the affidavit when attesting to the truthfulness of these paragraphs. Once again, the material information as to these paragraphs is correct. This was confirmed by FBI Special Agent D'Errico, who has read and reviewed the surveys. Furthermore, because of TFO Thornton's extensive experience as a OHP Trooper, he knows the content in those paragraphs to be true even without reading the surveys. He testified that he believes that the number of those who drive a vehicle with a cell phone is higher than 88 out of 100 based on his experience as a state trooper. Therefore, TFO Thornton did not intentionally mislead or recklessly omit material information from the affidavit when didn't read the surveys identified in paragraphs 24 and 25.

Furthermore, even if the alleged *Franks* violation was not waived, nothing in the record establishes that TFO Thornton committed a *Franks* violation.

***2. The geofence warrant was not a general warrant.***

The Google geofence search warrant was not a general warrant, as it was supported by probable cause and specified its object with particularity. In addition, the defendant errs by attempting to invent a new rule to avoid *Leon's* good-faith analysis. The defendant asserts that the good-faith doctrine should not apply where a court deems a warrant to be a "general warrant." But the good-faith exception depends on whether the officer reasonably relied on a warrant, not on how the reviewing court labels it. The defendant cites *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992), in which the court suppressed evidence from a warrant it called a general warrant. But *George* explicitly suppressed evidence based on *Leon's* framework. The court found the warrant "so facially deficient" that officers could not reasonably rely on it. *Id*. at 77. Where the fruits of a warrant are not suppressible under *Leon*, it would be inconsistent with *Leon* to suppress evidence on the basis that the court describes the warrant as a "general warrant."

***3. TFO Thornton reasonably relied on a search warrant and consulted with counsel before using a new investigative technique.***

When TFO Thornton sought the Google geofence search warrant in this case in March of 2021, this type of warrant was a new and novel investigative technique, and there were no judicial opinions analyzing them under the Fourth Amendment. The defendant even conceded during the suppression hearing that this type of warrant was novel at the time it was sought in this case. In *United States v. McLamb*, the Fourth Circuit rejected suppression in these types of circumstances. 880 F.3d 685 (4th Cir. 2018). 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 and then sought 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.

*Id*. at 691. Here, TFO Thornton followed the approach endorsed by *McLamb*. Because of the novelty of the search warrant, he consulted with an AUSA about the search warrant prior to obtaining it and conferred with the AUSA throughout the entire search warrant process to ensure its accuracy and legality. TFO Thornton also sought and obtained a Google geofence search warrant from a United States magistrate judge. Thus, TFO Thornton did "precisely" what *McLamb* expects, and the good-faith exception precludes suppression here. In sum, he behaved reasonably for an investigator seeking to employ a new investigative technique.

The defendant objects to the search warrant because TFO Thornton received no formal training on Google geofence search warrants prior to seeking this search warrant, but there is no indication in *McLamb* that the agents in that case had received training on darknet child

pornography warrants prior to seeking the warrants. Indeed, such trainings may not exist when a new investigative technique first arises. *McLamb* calls for consultation with prosecutors and then seeking a warrant, not meeting a bureaucratic training requirement. Consulting directly is an effective form of training, even if it is not officially categorized as such. TFO Thornton did what *McLamb* calls for, and the good-faith exception therefore applies.

As cited above, in *United States v. Smith*, the court found that the good faith exception applied even though neither investigator who testified at the suppression hearing had any prior personal experience with Google geofence search warrants at the time they applied for the search warrant. *United States v. Smith*, 2023 WL 1930747 at *12 (N.D. Miss. February 10, 2023). Similarly, in *United States v. Carpenter*, the court denied a motion to suppress a Google geofence search warrant even though the affiant officer testified that he did not have training on the Google-related facts in his affidavit and that he relied more on his experience. *United States v. Carpenter*, 2023 WL 3352249 (M.D. Florida February 28, 2023) report and recommendation adopted by the District Court, 2023 WL 2910832 (M.D. Florida April 12, 2023).

Recent judicial opinions provide further evidence that TFO Thornton's reliance on the warrant was reasonable. Numerous judges have issued or upheld geofence warrants, and if they have all been mistaken, it was reasonable for TFO Thornton to be mistaken as well. *See United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017) (stating that if eight federal judges were mistaken in upholding a particular warrant, investigators "could reasonably have made the same mistake"). United States magistrate judges have issued opinions explaining why they issued Google geofence search warrants. *See, e.g., In re Search Warrant Application*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Search of Information*, 579 F. Supp. 3d 62 (D.D.C. Dec. 30, 2021).

Furthermore, district courts have denied Google geofence suppression motions and held that the Google geofence search warrants complied were constitutional and/or the good faith exception applied. *See Rhine*, 2023 WL 372044, at *32-33 (held the geofence warrant to be constitutionally valid and the good faith exception applied); *United States v. Smith*, 2023 WL 1930747 at *6-12 (N.D. Miss. February 10, 2023) (recognizing that because of the "novelty of the warrants of this nature and for reasons set forth more fully hereinafter, the Court need not definitively resolve" the reasonable expectation of privacy issue; held "the geofence warrant contained sufficient probable cause[;]" "agree[s] with the Government's overall position that the warrant was particular in identifying the places to be searched and things to be seized[;]" "the Court makes no determination as to whether geofence warrants are per se constitutional but, instead, finds that a case-by-case determination is appropriate in determining the appropriate geographic parameters[;]" "reject[ed] the Defendants' argument that the warrant was so overbroad as to render it unconstitutional. But the Court does find that 'further legal process' required law enforcement to obtain an additional warrant before requesting Steps Two and Steps Three data[;]" the court "does not find that suppression in this case would further the rationale underlying the good faith exception"); *United States v. Chatrie*, 590 F.Supp.3d 901 (E.D. Virginia, Richmond Division 2022) (held that the geofence warrant violated the Fourth Amendment, but denied the motion to suppress under the good faith exception); *United States v. Anthony*, No. 1:21-CR-128, ECF No. 125 at 31 (W.D. Mich. Mar. 1, 2022) (orally denying motion to suppress ten geofence warrants and stating "the warrants challenged here with respect to the geofences at issue do satisfy traditional probable cause and particularity standards," except for one state warrant that was "a little sparse on some of the information regarding social media," but still sufficient for *Leon*'s good faith exception); *United States v. Carpenter*, 2023 WL 3352249 (M.D. Florida, February 28, 2023)

report and recommendation adopted by the District Court, 2023 WL 2910832 (M.D. Florida, April 12, 2023). In fact, at this time, the United States is not aware of any district court throughout the country who has denied a Google geofence search warrant. And the Eighth Circuit approved cell tower dump warrants based on reasoning that supports a Google geofence search. *James*, 3 F.4th at 1105-06. If all of these courts have erred, TFO Thornton could reasonably have made the same mistake and reasonably relied on the magistrate judge's decision to issue the warrant.

## IV. CONCLUSION

Based on the foregoing, the United States respectfully requests that this Court deny the defendant's Opposed Motion to Suppress Evidence Obtained by *Google "Geofence" Search Warrant* and Brief in Support (Doc. 39).

Respectfully submitted,

CHRISTOPHER J. WILSON
United States Attorney

s/ T. Cameron McEwen
T. CAMERON MCEWEN
AL Bar #7161R67M
Assistant United States Attorney
520 Denison Avenue
Muskogee, Oklahoma 74401
(918) 684-5100
Cameron.McEwen@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on December 8, 2023, I electronically transmitted the attached document to the Clerk of Court using the ECF System for filing. Based on the records currently on file, the Clerk of Court will transmit a Notice of Electronic Filing to the following ECF registrants:

Juan L. Guerra, Jr., Attorney for the Defendant
Sidney Warren Thaxter, Attorney for the Defendant
Michael W. Price, Attorney for the Defendant

s/ T. Cameron McEwen
T. CAMERON MCEWEN
Office of the United States Attorney