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

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

UNITED STATES' RESPONSE TO DEFENDANT'S FINDING OF FACT AND MEMORANDUM OF LAW IN SUPPORT OF DEFENSE MOTION TO SUPPRESS EVIDENCE

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 response to the defendant's Finding of Fact and Memorandum of Law in Support of Defense Motion to Suppress Evidence (Doc. 130) and 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).

In response to the defendant's finding of fact and memoranda of law, the United States respectfully requests that the Court incorporate and consider its findings of fact and conclusions of law previously filed in its Proposed Findings of Fact and Conclusions of Law Regarding Defendant's Motion to Suppress (Doc. 131) as well as consider the following supplemental conclusions of law:

The defendant lacked protected Fourth Amendment rights in four minutes of information regarding her location

The defendant argues that the Google geofence search warrant in this case violated her Fourth Amendment rights. In *United States v. Hammond*, 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). In *Hammond's*, the court concluded that "although *Carpenter* rejected *Knotts'* reasoning as applied to *historical* CSLI, [the court agreed] with the Sixth Circuit that given the opinion's limited holding, *Carpenter* otherwise 'left undisturbed [the Supreme Court's] holding in *Knotts*[.]'" *Id*. at 389 (quoting *United States v. Trice*, 966 F.3d 506, 518 (6th Cir. 2020)).

In *Knotts*, the Supreme Court held "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [a suspect] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property." *Knotts*, 460 U.S. at 281-282.

In coming to its conclusion, the court in *Hammond's* reviewed the following facts: "Ghiringhelli's monitoring of Hammond's location lasted only a matter of hours–from roughly 6 p.m. on October 30 until close to midnight, when officers were able to physically follow Hammond without the aid of the CSLI pings. This is very different from the 127 days of monitoring at issue in *Carpenter* and more similar to the monitoring of the discrete car trip at issue in *Knotts*. Furthermore, Ghiringhelli's real-time CSLI request only collected location data that Hammond had

already exposed to public view while he travelled on public, interstate highways and into parking lots within the public's view." *Hammond*, 996 F.3d at 389 (citations omitted).

Furthermore, "unlike in *Carpenter*, the record of Hammond's (and Knotts') movements for a matter of hours on public roads does not provide a 'window into [the] person's life, revealing ... his familial, political, professional, religious, and sexual associations' to the same, intrusive degree as the collection of historical CSLI. *Carpenter*, 138 S. Ct. at 2217 (internal quotations omitted). Law enforcement used the real-time CSLI to find Hammond's location in public, not to peer into the intricacies of his private life. The records here and in *Knotts* do not suggest that law enforcement used either the real-time CSLI or the beeper to examine the defendants' movements inside of a home or other highly protected area. And, Hammond does not argue that he was in private areas during this time period. In *Carpenter*, law enforcement's surveillance became a 'search' because the surveillance followed Carpenter long enough to follow him into, and record, his private life. But here, and in *Knotts*, law enforcement only followed Hammond on public roads, for the duration of one car trip. *See also United States v. Skinner*, 690 F.3d 772, 780–81 (6th Cir. 2012) (distinguishing "comprehensive tracking" from the collection of real-time CSLI to merely locate a drug-trafficking suspect) (superseded by statute on other grounds)." *Hammond*, 996 F.3d at 389.

Similar to *Knotts* and *Hammond*, the information sought after by TFO Thornton in this case in the Google geofence search warrant did not involve any aspect of the defendant's private life; involved only information that she already exposed in public view while traveling on a public roadway; and only included a short duration of location history captured within the parameters of a very small geofence. Therefore, the United States did not infringe on the defendant's Fourth

Amendment rights when it obtained four minutes of her location information from Google while she drove on a public roadway.

There is no reasonable expectation of privacy for the subscriber information and the Location History information the defendant voluntarily provided to Google

The defendant argues she had a reasonable expectation of privacy to her Google Location History information. In *United States v. Perrine*, the Tenth Circuit noted that "[e]very federal court to address [the Fourth Amendment challenge to the government's acquisition of a suspect's subscriber information] has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation." *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008). Thus, the court held that "Perrine has no Fourth Amendment privacy expectation in the subscriber information he gave to Yahoo! and Cox."

The Court in *Perrine* identified the following cases to support its holding:

1. *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001) (in a non-criminal context, "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person-the system operator");

2. *United States v. Hambrick*, 225 F.3d 656 (4th Cir.2000) (unpublished), affirming *United States v. Hambrick*, 55 F.Supp.2d 504, 508–09 (W.D.Va.1999) (there is no legitimate expectation of privacy in noncontent customer information provided to an internet service provider by one of its customers);

3. *United States v. D'Andrea*, 497 F.Supp.2d 117, 120 (D.Mass.2007) ("The *Smith* line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access.");

4. *Freedman v. America Online, Inc.*, 412 F.Supp.2d 174, 181 (D.Conn.2005) ("In the cases in which the issue has been considered, courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information.");

5. *United States v. Sherr*, 400 F.Supp.2d 843, 848 (D.Md.2005) ("The courts that have already addressed this issue ... uniformly have found that individuals have no Fourth Amendment privacy interest in subscriber information given to an ISP."); *United States v. Cox*, 190 F.Supp.2d 330, 332 (N.D.N.Y.2002) (same);

6. *United States v. Kennedy*, 81 F.Supp.2d 1103, 1110 (D.Kan.2000) ("Defendant's constitutional rights were not violated when [internet provider] divulged his subscriber information to the government. Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information.");

7. *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir.2008) ("e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."); and

8. *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir.2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers.... They may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient.").

Id.

Under *Perrine*, the defendant lacks a protected privacy interest in any of the subscriber identity information obtained in the third step of the warrant. Thus, if the Court holds that the location information and account identifier in Step 1 were properly acquired, the defendant would lack Fourth Amendment standing to challenge the subscriber identity information the government subsequently obtained. Therefore, not only does the defendant have no reasonable expectation of privacy or privacy interests to the subscriber identity information she voluntarily provided to Google, but she also has no reasonable expectation of privacy or privacy interests to the Location History information she voluntarily provided to Google when she opted-in and enabled Location History and Location Reporting.

The defendant's Fourth Amendment rights were not violated by use of Google's internal filtering processes

The defendant argues that Google's search of 592 million subscriber accounts in its Sensorvault database is a violation of her Fourth Amendment rights. However, Google's internal data filtering processes, which are invisible to both the government and Google's users/subscribers, lack Fourth Amendment significance. The Supreme Court in *Carpenter* focused on the government's access to information, not the phone company's internal filtering process. The Court asked "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," and it held that "when the Government accessed CSLI from the wireless carriers, it invaded *Carpenter's* reasonable expectation of privacy in the whole of his physical movements." *Carpenter*, 118 S. Ct. at 2212, 2219. This focus in *Carpenter* on information the government accesses, rather than the provider's internal filtering processes, makes sense – the government learns nothing about anyone whose information it is not provided. Therefore, the fact that Google has to search all subscriber accounts in its Sensorvault database as part of its internal filtering process, does not mean that it is a search under the Fourth Amendment or that the defendant's Fourth Amendment rights were violated when this filtering process is utilized.

The defendant did not have a property interest in her Location History information

The defendant argues that she had a property interest in her Location History information. In *Couch v. United States*, the Supreme Court concluded "that the Fifth Amendment privilege is a personal privilege: it adheres basically to the person, not to information that may incriminate him." *Couch v. United States*, 409 U.S. 322, 328 (1973). The Court continued by stating, "[t]he

Constitution explicitly prohibits compelling an accused to bear witness 'against himself': it necessarily does not proscribe incriminating statements elicited from another." *Id*. In *Couch*, the defendant gave information to his or her accountant, a third-party. *See id* at 329. "The summons and the order of the District Court enforcing it [were] directed against the accountant. He, not the taxpayer, [was] the only one compelled to do anything. And the accountant [made] no claim that he may tend to be incriminated by the production." *Id*. Although Couch was entitled to this Fifth Amendment privilege, as it pertained to her, this privilege did not apply to his accountant and the information the defendant provided him or her, unless the accountant claimed the production of this information would incriminate him or her. *Id*. at 328-336. Furthermore, because "no confidential accountant-client privilege exists under federal law[,]" the defendant did not have any reasonable expectation of privacy pursuant to the Fourth Amendment as to the information she provided her accountant. *Id* at 335-336. Therefore, in effect, *Couch* signifies that there is no "property rights" exception to the third-party doctrine, and the defendant does not have a property interest in her Location History information she provided Google.

Additionally, Google is not a bailee that just stores location information for its users/subscribers. At no point do subscribers have sole discretion on how their Location History is used. For example, Google can actively use the users/subscribers' Location History information to provide services to its users/subscribers, such as 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). Thus, the defendant does not have a property interest in her Location History information she provided Google.

A magistrate judge's finding of probable cause can be based on a combination of specific facts and reasonable inferences

The defendant argues that the Google geofence search warrant in this case provided no case-specific facts to warrant probable cause and was based on nothing more than broad conjecture and boilerplate assertions. In *Illinois v. Gates*, the Supreme Court held that all that is required for probable cause is a fair probability that evidence will be found in the place to be searched. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983). 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. Thus, a magistrate judge's finding of probable cause may be based on a combination of specific and reasonable inferences. 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 made a reasonable inference that evidence of a defendant's threats would be found at his home.

Here, the magistrate judge found probable cause based on a combination of specific facts and reasonable inferences. The specific facts include the following:

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. 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 reservation.

2. Affiant and other Troopers of the Oklahoma Highway Patrol were dispatched to the scene. Based on our observation of evidence at the scene, including debris from a vehicle, and speaking to witnesses, investigators determined that a female later identified as Jacklyn Dobson, 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. Dobson was assisted by another motorist until she was transported by air ambulance to St. John Hospital in Tulsa. She later died from her injuries. Dobson was confirmed as a member of the Cherokee Nation.

3. The location of the collision is a rural, four-lane highway separated by an unimproved median. There are no traffic control devices. There are a small number of commercial businesses and residences located near the intersection. I was able to retrieve surveillance video from several nearby businesses. 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. The suspect vehicle stopped for approximately 10 seconds before resuming westbound travel on U.S. 62 and leaving the scene. In the one-minute timespan after the collision, the videos show six other vehicles travelling through the collision area. Five of the six vehicles are travelling eastbound.

Government's Suppression Hearing Exhibit 8 at ¶¶ 21-23. In these paragraph's, Trooper Thornton provided specific facts to the magistrate judge that a collision occurred at a certain time and location; a vehicle traveling westbound caused the collision; the westbound vehicle stopped for a certain period of time after the collision; the westbound vehicle subsequently continued to travel westbound after stopping; and the suspect driver caused the death of the victim. These specific facts helped form the basis of probable cause for the search warrant.

Additionally, although there was no direct evidence in the government's possession at the time TFO Thornton applied for the search warrant that the suspect driver had a cell phone on him or her or that the suspect driver was a Google subscriber, several additional facts were presented to the magistrate judge where he could draw reasonable inferences that the suspect driver probably had a cell phone on him or her, the suspect driver was probably a Google subscriber, and Google probably stored evidence of the crime. These reasonable inferences could be drawn from the following facts:

1. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

2. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet ("wi-fi") access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

3. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by applications (apps) installed on a device as part of the apps' operation.

4. Based on my training and experience, I know 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.

5. In addition, based on my training and experience, I know that 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. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (e.g., example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed into a Google account.

6. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has

the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

7. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

8. According to my training and experience, as well as open-source materials published by Google, I know that 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.

9. Based on my training and experience, I know that 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.

10. Based on open-source materials published by Google and my training and experience, I know that 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.

11. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

12. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

13. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

14. Based on my training and experience, as well as a review of professional literature, a vast majority of motorists not only own but use their smartphones while driving. In one of the largest and most comprehensive distracted driving studies to date, involving the

collection and analysis of data from over 570-million trips driven by three million motorists over a three-month time period, drivers used their smartphones in 88 out of every 100 trips. Cameron Jahn, *Largest Distracted Driving Behavior Study*, Zendrive (Apr. 17, 2017), http://blog.zendrive.com/blog/distracted-driving/; Angie Schmitt, *Study: Drivers with Smart Phones Use Them Almost Every Time They Drive*, StreetsBlogUSA (Apr. 17, 2017), https://usa.streetsblog.org/2017/04/17/study-drivers-with-smart-phones-use-them-almost-every-time-they-drive. Despite legislative efforts and public awareness campaigns to curb cellphone use while driving, research suggests that the number of motorists who use their cellphones has been trending upward. See, e.g., Jeff Plungis, *Drivers Still Can't Keep Hands Off Phones, Study Finds*, Consumer Reports (Jan. 24, 2019), https://www.consumerreports.org/car-safety/distracted-driving-study-drivers-cant-keep-hands-off-phones (noting that in one study, the number of motorists using cellphones while driving increased 57 percent from 2014 to 2018).

15. Based on my training, experience, and a review of professional literature, a significant number of collisions occur as a result of distracted driving from a variety of sources, including cellphone use. See, e.g., Nat'l Highway Traffic Safety Admin., *Distracted Driving 2018* (2020) available at https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812926. Additionally, it has also been my experience that 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.

Government's Suppression Hearing Exhibit 8 at ¶¶ 7-20 and 24-25. Despite the defendant's best efforts to attack TFO Thornton's credibility on these facts, each of these facts is substantively true and correct. The defendant provides no evidence to the contrary. Furthermore, just because TFO Thornton did not include information about Google's internal data filtering processes and the number of accounts Google internally searches to gather the information it provides to law enforcement, Google's 68% accuracy goal, the fact that false positives and false negatives in location information is possible, and Google's statistical information specific to the location of the collision, this does not mean that the magistrate judge did not have enough information to draw reasonable inferences from the above-mentioned facts that the suspect driver probably had a cell phone on him or her at the time of the collision, the suspect driver probably was a Google

subscriber, and Google probably had in its possession evidence of the crime. Nor has the defendant provided any evidence to the Court that TFO Thornton should have known that this additional Google-related information even existed at the time he applied for the search warrant or that this information was commonly known to law enforcement at the time. In fact, it would have been impossible for TFO Thornton to have known about any Google statistical information specific to the location of the collision because it is impossible for Google to produce these types of statistics at this time. Lastly, law enforcement can establish probable cause for a search warrant in cell phone-related cases even though there is not specific factual evidence at the time of the application for the search warrant that the suspect had a cell phone on his or her possession at the time of the crime. In *United States v. James*, the Eight Circuit found probable cause in a cell tower dump case where there was no specific factual evidence the suspect had a cell phone on him when he committed the crime. *See United States v. James*, 3 F.4th 1102 (8th Cir. 2021). Therefore, the magistrate judge correctly based his finding of probable cause on a combination of specific facts and reasonable inferences.

TFO Thornton did not commit a Franks violation by omitting Google-related information in his application for a search warrant

The defendant argues that TFO Thornton committed a *Franks* violation when he omitted certain Google-related information in his application for a Google geofence search warrant in this case. However, as already conceded by the defendant, these types of warrants were a novelty and new at the time TFO Thornton applied for the search warrant. Just because TFO Thornton did not include information about Google's internal data filtering processes and the number of accounts Google internally searches, Google's 68% accuracy goal, the fact that false positives and false

negatives in location information is possible, and Google's statistical information specific to the location of the collision, does not meant that TFO Thornton intentionally or recklessly left out this information or misrepresented anything to the magistrate judge. In fact, the defendant provides no evidence that TFO Thornton should have known that this additional Google-related information even existed at the time he applied for the search warrant or that this information was commonly known to law enforcement at the time. Furthermore, it would have been impossible for TFO Thornton to have known about any Google statistical information specific to the location of the collision because it is impossible for Google to produce these types of statistics at this time. Therefore, the defendant's claims that TFO Thornton committed a *Franks* violation are unfounded and should be denied.

Wherefore, 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 18, 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