**UNITED STATES DISTRICT
COURT EASTERN DISTRICT
OF OKLAHOMA MUSKOGEE
DIVISION**

UNITED STATES OF AMERICA	§	
	§	
	§	
VS.	§	**CRIMINAL CASE 6:21-cr-358-RAW**
	§	
	§	
SILVIA VERONICA FUENTES	§	

DEFENDANT SILVIA VERONICA FUENTES' POST HEARING FINDING OF FACT AND MEMORANDUM OF LAW IN SUPPORT OF DEFENSE MOTION TO SUPPRESS EVIDENCE

Defense files the following post-hearing proposed finding of facts and memorandum of law in support of the November 18, 2022, motion to suppress.

PROCEDURAL HISTORY

A motion to suppress was filed by the defense on November 18, 2022. The prosecution filed a response in opposition on November 30, 2022. A hearing on the motion was held on September 25-26, 2023. At the close of that hearing the honorable Magistrate Judge Jason Robertson granted leave for counsel to file a proposed finding of fact and conclusions of law in support of the proposed order.

PROPOSED FINDING OF FACTS

1. Google Location History

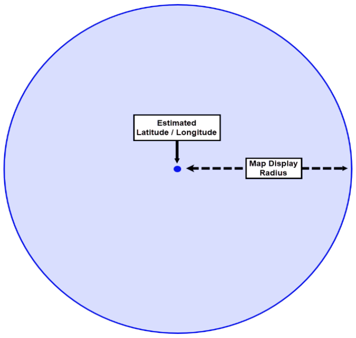
Location History is a Google feature that logs device location data, showing where a user has been with a specific device. *See* Ex. A(6) at 5. If a user has Google Location History enabled, then Google estimates the user's device location using GPS data, the signal strength of nearby Wi-Fi networks, Bluetooth beacons, and cell phone towers. Ex. (A)(2) at 4; *see also* Tr. 37:17-23. Approximately one-third of all active Google users have Location History enabled on their accounts, which, according to Google, was approximately 592 million accounts as of 2018. Ex. (A)(2) at 4; Ex. A(5) at 205.

Location History is not an "app"; it is a setting on the Google account associated with a device, and it is currently an "opt-in" feature. Once enabled, it records that device's location as often as five or six times per minute, regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. Tr. 39:8-40:1; Ex. A(5) at 436–37, 513. This data is considerably more precise than Cell Site Location Information (hereinafter "CSLI") as it can locate someone inside a home or on a streetcorner as opposed to a neighborhood or town. Tr. 38:12-42:22.

Google saves Location History data in each user's "Timeline," Ex. A(6) at 6, which Google describes as a "digital journal" of a user's locations and travels. *Id.* at 16. Google considers this information to be communications "content" for purposes of the Stored Communications Act, 18 U.S.C. § 2703, requiring the government to obtain a warrant to access it. *See id.* Google does not consider it a business record. *Id.*; *see also* Tr. 43:25-44:25. Google uses Location History data to target advertising based on a user's location, although it obscures individual device information, preventing businesses from being able to track individuals. *See id.* at 43:3-24; *see also* Ex. A(5) at 197.

Despite the precise nature of the data neither the Timeline feature nor the advertising relies on a high degree of accuracy. Rather, Location History is merely Google's estimation of where a device is. Ex. A(5) at 212. It is not hard data but is instead Google's best guess at device location based on available information. *See* Ex. A(6) at 10–11 n.7 ("In that respect, LH differs from CSLI [Cell Site Location Information], which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points …"). As Google puts it, Location History is a "probabilistic estimate," and each data point has its own "margin of error." *Id.* Thus, when Google reports a set of estimated latitude/longitude coordinates in Location History, it also reports a "confidence interval," and "Map Display Radius." Ex. A(5) at 212, 530–31.

A Display Radius represents the geographical area Google believes the device is located. On a map, Google shows the coordinates as a small, solid "blue dot." And it shows the Display Radius as a larger "light blue circle" around the dot. *See* Ex. A Figure 3.



Importantly, Google is equally confident that a device could be anywhere within the Display Radius, i.e., the shaded circle. Ex A(5) at 214. The estimated coordinates are simply the center point of that circle. Tr. 58:21-59:12. It is equally likely that the device is at the center point as anywhere else in the shaded circle, even at the edge. *Id.* The Map Display Radius is not fixed; it expands and contracts in accordance with Google's confidence in each location estimation.

Furthermore, despite the precision of Location History data, Google has significant accuracy problems. Google states their *goal* is to correctly place a device within the display radius 68% of the time. Tr. 61:18-24; *see also* Ex. A at 6; Ex. A(2) at 8-9. So, their accuracy rate could in fact be lower.[1] However, assuming that they obtained their 68% accuracy goal, devices would still fall outside that display radius 32% of the time. Or in other words, the odds are almost 1-in-3 that the user's actual location lies beyond the shaded circle. Indeed, Google users may be familiar with this phenomenon, as "in the common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake." *In re Search Warrant Application for Geofence Location Data Stored at Google*, No. 20 M 525, 2020 WL 6343084 at *9 (N.D. Ill. Oct. 29, 2020).

A confidence interval of 68% is the industry standard, and as Google explains it is "an Estimated Latitude/ Longitude approximation sufficient for its intended product uses," namely Timeline and advertising. *See* Ex. A(5) at 581. Because it was not intended to solve crimes, Google warns that its use in geofence warrants risks generating "false positives." Ex. A(6) at 20 n.12. According to Google, "the margin of error associated with LH data means that the government's effort to use this information for purposes for which the LH service was not designed creates a likelihood that the LH data will produce false positives-that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." *Id.*

[1] While Jeremy D'Errico claimed to have anecdotal evidence Location History is more accurate than their stated goal this was not a formal or systematic review and thus he provided no statistical data to support the claim. Tr. 216:18-218:14. Nor had he read any peer reviewed published studies on the subject. *Id.* In fact, published studies indicate the "hit rate" for Wi-Fi can be as low as 7% and as low as 52% for GPS. *See* Andrea Macarulla Rodriguez, Christian Tiberius, Roel van Bree & Zeno Geradts (2018) *Google timeline accuracy assessment and error prediction*, Forensic Sciences Research, 3:3, 240-255, DOI: 10.1080/20961790.2018.1509187.

Google is clear that it does not ever share Location History data with advertisers or other third parties. Tr. 43: 16-24; Ex. A(5) at 198; 367-69. This is done for privacy purposes, so that advertisers do not get to see which devices were in the area. *Id.* at 197, 199. Likewise, advertisers cannot go back to Google and ask for more information about where certain devices were before or after they saw an ad or visited a store. *Id.* at 199. In fact, advertisers cannot get any identifiable information about individual Google users. *Id.* at 199.

Although, currently, Google Location History is a feature that the user must actively turn on or opt-into, that was not always the case. Tr. 45:9-47:4. Google uses a system called "consent flows" which ostensibly notify the user that they are turning on Location History and what potential data is collected as a result. *Id.* at 47:5-48:11. Spencer McInvaille testified the earliest "consent flow" he had ever seen in a case was from either 2015-2016. *Id.* at 48:2-5. This was not controverted by the Government's expert. While the "consent flows" have become more explicit over time, even when Google converted to an opt-in model the "consent flow" notices to customers as to what they were doing could be unclear and confusing. *Id.* at 47:5-48:18.

While it is sometimes possible to deduce how Location History was turned on with an account using a record called an "account change history," the records in this case were insufficient to show how Ms. Fuentes Location History was activated. *Id.* at 48:19-49:5. Furthermore, her account was created in 2011 and Location History was activated in 2013, prior to the earliest "consent flows" seen by any experts in this case. *See id.* at 48:2-5; *see also* 49:6-50:10. Therefore, it is impossible to tell what kind of notification she might have received about the data being collected by Google. While the government's witness speculated that Ms. Fuentes must have had to opt-in because she activated a phone in 2020, there was nothing in the "account change history" to support this theory nor did they provide a consent flow for that period showing what notifications she would have received during that potential opt-in process. *See id.* at 194:15-199:5. Furthermore, while Agent D'Errico testified that Ms. Fuentes should have been receiving emails regarding her Location History data, he provided no evidence that she actually received them or, more importantly, that she read them. *Id.* at 192:20-13. The only actual evidence introduced by the government was an email sent to her account on April 9, 2021—after the search warrant in this case was executed. Ex. 25.

2. Google Geofence Warrants

Generally, geofence warrants follow a three-step process designed by Google and the Computer Crime and Intellectual Property Section (hereinafter "CCIPS), a division of the Department of Justice (hereinafter "DOJ"). Tr. 51:21-54:11; *see also* Ex. A(5) at 456:16-458:2; Ex. A(3) at ¶ 3-12.

In step one of this process the government "generally obtains a search warrant compelling Google to disclose a deidentified list of all Google user accounts for which there is saved LH information in a defined geographic area during a defined timeframe." Ex. A(3) at ¶ 6. To comply with this step Google must conduct a search across the Location History of all of its approximately 592 million users with Location History activated. Ex. A(3) at ¶ 7; Tr. 54:12-56:13. This broad search occurs regardless of whether or not those users were actually within the area described within the geofence. *Id.* In other words, unlike a tower dump where the search is only across the subset of users who access a tower or set of towers, this occurs across all Google customers with Location History enabled. *Id.* at 56:14-57:4; *see also* Ex. A(6) at 14.

In the DOJ's step two, the government examines the Location History data seized during step one and identifies additional devices for which they would like to obtain "contextualization" data. Ex. A at 5; *see also* Ex. A(6) at 13. This contextualization process involves obtaining additional "anonymized" location information "showing where certain users moved during an extended period of time 30 minutes before and 30 minutes after the original timeframe. This additional contextual LH information can assist law enforcement in eliminating devices that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation." *Id.* at 13-14. This step was ostensibly created to protect the privacy of users. *Id.* at 12.

In step three of the DOJ's process the government compels "Google to provide account-identifying information for the anonymized device numbers that it determines are relevant to the investigation." *Id.* at 14.

3. The Investigation of Trooper Thornton

On March 18, 2021, Trooper Thornton was at home, off duty, when the was notified for a fatal collision that involved a pedestrian and a vehicle. Tr. 112:23-113:9. He went to the scene and located one witness on scene and three surveillance videos. *Id.* at 113:8-25. One of those videos showed the impact and showed a car briefly pulling over onto the shoulder before leaving the scene. *Id.* at 114:4-11. However, the video was not clear enough to identify the vehicle. At that point Trooper Thornton began to "explore the geofence technology through Google." *Id.* at 116:13-17.

4. The Warrants

On March 18, 2021, Trooper Thornton applied for the first geofence warrant. Ex. 6. This application was rejected by the magistrate because they believed the timeframe covered was too long. *Id.* at 122:6-15. On April 1, 2021, a second warrant application was submitted. Ex. 1. No new information was presented, but the terms of the warrant differed as to how step one was to be conducted, changing the timeframe from 21:49-21:59 hours to 21:52-21:56 hours. *Compare* Ex. 6 Attachment A at (2), *with* Ex. 2, Attachment A at (2). That second warrant was withdrawn by Trooper Thornton at the request of the AUSA. Tr. 123:13-23. Trooper Thornton did not remember why he was asked to withdraw the warrant. Tr. 125:13-16. However, the subsequent warrant omitted the following language:

> "Time Restriction: Devices that reported their location more than once within the Target Location on the date and during the time period above and where no more than three minutes elapsed between the time that the first time the device reported its location and the last time that the device reported its location." *Compare* Ex. 2 Attachment A at (2), *with* Ex. 8, Attachment A at (2).

As a result of this omission the government's witness speculated that it was withdrawn because Google "pushes back" on those types of warrants. Tr. 185:15-186:7. However, he admitted that Google had the technical means of complying with the April 1st warrant and that they could have been compelled to comply with the April 1st warrant by the government through further legal process. *Id.* at 230:17-232:16.

On April 7, 2021, Trooper Thornton submitted a third warrant application (hereinafter "the Warrant Application"). *Id.* at 127:4-11. Again, the magistrate granted the application and issued the warrant (hereinafter "the Warrant"). *Id.* at127:10-14.

5. The Warrant Application

In the Warrant Application Trooper Thornton implied that he had extensive training and experience with Google Location History and Google data. *See* Ex. C ¶ 7-20. However, on the stand he admitted this was in fact his first geofence warrant and his "training and experience" included merely speaking to other officers about geofence warrants. Tr. 116:21-23 & 144:2-

148:1. He didn't know the level of training and experience of those officers, except to say that one of them, from Springdale, Arkansas, he was specifically "referred to by local people here." *Id.* at 146:17-23. Further, he could not remember how many times he actually spoke with that individual. *Id.* at 146:25-147:3. Nor did he know if that person was an expert in the area. *Id.* at 156:6-13. During his testimony it became apparent that officer Thornton did not draft the Warrant and that he never verified much of the information in it. *See id.* at 147:14-19; 148:22-148:9; 149:18-150:3. Instead, he relied on the AUSA to provide accurate information in the application, even though he had never worked with the AUSA and had no understanding of the AUSA's level of experience with Google Location History or geofence warrants. *Id.* at 150:4-151:6.

Trooper Thornton admitted that at the time he applied for the geofence warrant he had no idea who Ms. Fuentes was. *Id.* at 153:14-154:24. She was not a suspect, nor did he have probable cause to search her or her account. *Id.* at 154:12-24. Nor did his affidavit provide any evidence the person driving the vehicle was using Google or had Google Location History Enabled. *See* Ex. C. Because he lacked any evidence showing that the suspect was using Google and had Google Location History enabled, Trooper Thornton in his affidavit stated that "[i]n 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 use their smartphones in 88 out of every 100 trips." Ex. C ¶ 24; *see also* Tr. 64:6-10. Defense expert Spencer McInvaille explained, those statistics are meaningless because they do not answer the question of whether or not a specific person had a Google account or Google Location History enabled. *Id.* at 64:6-65:24. Nor do they establish a statistical likelihood that a person had a Google account or Google Location History enabled. *Id.* Additionally, Trooper Thornton had not actually read those studies despite swearing to their contents. *Id.* at 148:22-148:9; 149:18-150:3.

The Warrant Application omitted several important facts about how Google Location History functions and how Google geofence warrants work. First, it failed to explain that the first step of a geofence warrant requires Google to conduct a search across the Location History of all of its approximately 592 million users with Location History activated. Ex. A(3) at ¶ 7; Tr. 54:12-56:13; 223:4-17. Therefore, the issuing magistrate was not made aware that regardless of the physical or temporal dimensions of the Warrant the search at step one would be a search of all Google users with Location History enabled. *Id.* at 73:18-74:19.

Second, the Warrant Application never discussed Google's acceptable error rate in their estimations of device location. Again, Google states their goal is to correctly place a device within the display radius 68% of the time. *Id.* at 61:18-24; *see also* Ex. A at 6; Ex. A(2).

Third, the Warrant Application referred to a "maps display radius" as a margin of error. However, this description was incomplete, as it implied Google believes the device is at the actual center point or latitude/longitude provided but that there is some chance it falls within the margin of error outside that center point. However, the reality is that center point is merely that-a center point. Tr. at 58:21-59:12. The device is equally likely to be anywhere within the display radius. Ex A(5) at 214.

6. The Warrant

The Warrant in this case diverged from the three-step process developed by the DOJ and Google. Specifically, it removed the middle step of obtaining "contextual" data. Ex. A at 5; *see also* Ex. A(6) at 13.

Additionally, despite stating in the affidavit that the government would command Google to turn over Reverse Location Obfuscation Identifiers (hereinafter "RLOI") the Warrant requested the "unique device ID." *Compare* Ex. C ¶ 27(a) *with* Ex. B Attachment B ¶ I(1). While Spencer McInvaille and Jeremy D'Errico disagreed on the level of anonymity provided by unique device IDs, there was no dispute that a unique device ID is not the same thing as a RLOI. *Compare* Tr. 95:9-96:13 *with* Tr. 174:12-25.[2] The former is permanent and unique ID within an account, the latter is generated in direct response to a warrant and has no permanent significance in the Google infrastructure. *Id.* at 66:26-67: 24.

Finally, and perhaps most importantly, the Warrant provided officer Thornton complete discretion as to which of the accounts seized at step one, he could de-anonymize or demand full account information from at step two. Ex. B Attachment B ¶ I(2); Tr. 223:17-25.

7. The Results of the Warrant

In response to the Warrant Google provided six datapoints which included three unique device IDs. Ex. 11. Three of those datapoints were connected to Ms. Fuentes account. Two were connected to another account ending in 008. *Id.* And one was connected to an account ending in 161. *Id.* Once officer Thornton obtained this step one data, he immediately requested personal identifying information for each account including things like names, email addresses, registration IP addresses, credit card numbers, physical billing addresses, and phone numbers. *See* Ex. F; Ex. 15, 16, & 17; Tr. 70:1-12.

Once Trooper Thornton obtained all this information on the account holders, he eliminated account ending in 008 because he discovered that individual had stayed on scene until police arrived. *Id.* at 71:24-72:2. Had they used the process designed by DOJ and Google, this

[2] The substance of the dispute hinged around whether a unique device ID was truly anonymous. However, both sides agreed that the unique device ID is unique within an account. *Compare* Tr. 97:23-98:6 *with* Tr. 175:21-5.

device would have been eliminated without revealing all the personal information for account 008, because the fact that the device remained on scene would have been evident in the Location History data. *Id.* at 72:3-17. It is unclear how or why police eliminated account ending in 161. However, Trooper Thornton used Ms. Fuentes name to track her to a home where a white vehicle was seen parked in front of the house. *See* Ex. 3 at ¶ 23-30. Based on the Location History data and fact that they discovered fragments of a white vehicle[3] on scene police obtained a warrant for all of Ms. Fuentes Google account data on April 28, 2021. *Id.*

As a result of that April 28, 2021, warrant police obtained further location information, photographs, google searches, phone numbers and other data they deemed to be either incriminating or used to obtain further warrants and information. This information and the subsequently obtained information are the basis of the prosecution against Ms. Fuentes. Therefore, all the evidence obtained in this matter against Ms. Fuentes flowed directly from the Warrant.

MEMORANDUM OF LAW

Here the government, without identifying Ms. Fuentes, and without any probable cause to believe the person who struck Jacklyn Dobson was a Google user or had Google Location History enabled, obtained a search warrant to search Ms. Fuentes' Location History, along with the Location History of approximately 592 million other users. After that initial search the government seized data from three devices despite having no particularized probable cause that any of those devices belonged to the individual who struck Ms. Dobson. From there, the Warrant

[3] Although Trooper Thornton initially believed the vehicle to be white because of fragments he found on scene, he later found chips of black paint on the decedents clothing and stated in subsequent warrants he believed the vehicle was black.

granted police complete discretion as to which accounts, they could seize further data from and deanonymize. To obtain this vast general warrant, the government deceived the magistrate as to their experience with geofence warrants, omitted important facts about Google Location History, concealed what the search entailed, and ignored the three-step process developed by the Department of Justice for geofence warrants. Therefore, suppression of the Google data and all the fruits therefrom is required.

I. MS. FUENTES HAD A REASONABLE EXPECATION TO PRIVACY IN HER LOCATION HISTORY DATA.

Ms. Fuentes had a reasonable expectation of privacy in her Location History data following the Supreme Court's landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012), because, like CSLI and GPS data, Location History reveals the "privacies of life." *Carpenter*, 138 S. Ct. at 2214. Although this case involves a shorter duration of data, the precision and always-on nature of Location History makes it even more invasive, requiring less to achieve the same effect. Indeed, just a small amount of Location History can identify individuals inside of their homes and other private spaces. And as a result, a geofence warrant almost always involves intrusion into these constitutionally protected areas, infringing on fundamental privacy interests recognized by the Court in *United States v. Karo*, 468 U.S. 705, 715-18 (1984), and *United States v. Kyllo*. 533 U.S. 27, 37 (2001). Furthermore, the only courts to directly consider this question have found a reasonable expectation of privacy in Location History Data. *See Comm. v Fleischmann*, No 2072CR00046 at *8-10 (Superior Court MA August 31, 2021); *Arizona. v. Baitan*, CR20204747-001(Superior Court AZ March, 23, 2022). Others, like the court in *Chatrie*, declined to reach the issue, but strongly suggested there was a reasonable expectation of privacy and that the third-party doctrine does not apply. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 908 (E.D. Va. 2022); *see also Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) ("Fuentes Opinion"). ("[T]here is much to suggest that Carpenter's holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration."); *Matter of Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *5 n7 (N.D. Ill. July 8, 2020) ("Weisman Opinion"). On the other hand, no court has ruled that Google customers lack a reasonable expectation to privacy in their Location History data.

A. Location History Is At Least As Precise as CSLI, Often Has GPS-Quality Precision, and Is Highly Intrusive

Location History data, even small quantities, can reveal the "privacies of life" because of its greater precision and frequency of collection. It is at least as precise as CSLI, but it can also be as precise as GPS. *See* Ex. A(6) at 10. That is because Google uses multiple data sources to estimate a user's location, including CSLI and GPS, as well as Wi-Fi and Bluetooth, which vary in their accuracy and precision. *Id.*; *see also* Ex. A at 3-4. In this case, all the estimated Location History points with known data sources derive from GPS signals, which Google states are "capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." Ex. A(2) at ¶ 12. Furthermore, Location History logs a device's location as often as several times a minute—regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. Tr. 41:14-23.

By contrast, the precision of CSLI "depends on the geographic area covered by the cell site." *Carpenter,* 138 S. Ct. at 2211. This may be sufficient to place a person "within a wedge-shaped sector ranging from one-eighth to four square miles," for example. *Id.* at 2218. As a result, a single CSLI data point could be used to determine which neighborhood or zip code someone was in, but it would not be accurate enough to identify the block and building. Moreover, even though cell phones 'ping' nearby cell sites several times a minute, service providers only log when the phone makes a connection, by placing a phone call or receiving a text message, for example. *Id.* at 2211. These differences between Location History and CSLI are significant because they affect how much data is needed to infer where someone was and what they were doing. While *Carpenter* anticipated that the precision of CSLI would improve, *id.* at 2218-19, the Court also faced technology that required stitching together some minimum amount of CSLI to reveal the "privacies of life." The Court settled on seven days, but this was not a magic number; it was simply the timespan for the shortest court order in the record. *See id.* at 2266-67 (Gorsuch, J., dissenting). In fact, that order only produced two days of CSLI. *Id.* at 2212. The Court in *Carpenter* explicitly declined to say "whether there is any sufficiently limited period of time for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 2217 n.3. But short-term searches may still be capable of revealing the "privacies of life," *id.* at 2214, which was the main concern in both *Carpenter* and *Jones*.

Although *Jones* and *Carpenter* involved so-called "long-term" searches, what motivated the Court in each case was the risk of exposing information "the indisputably private nature of which takes little imagination to conjure: the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (internal quotation omitted); *accord Carpenter*, 138 S. Ct. at 2215. Thus, "[i]n cases involving even short-term monitoring, some unique attributes of

GPS surveillance . . . will require particular attention." *Jones*, 565 U.S. at 415. The same is true for the data here, given that "[a] cell phone faithfully follows its owner beyond public throughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.

Before *Jones* and *Carpenter*, the Court was concerned with short-term location tracking, especially when it reveals information about a private interior space. In *Karo*, using an electronic beeper to track an object inside a private residence was a search. 468 U.S. at 716. In *Kyllo*, using a thermal imaging device to peer through the walls of a private residence was a search despite taking "only a few minutes" and not showing people or activity inside. 533 U.S. at 30, 37. Location History's greater precision and frequency of collection means that less time is needed to reveal the "privacies of life." It might take days of CSLI to piece together a mosaic with enough detail to be so revealing, but it takes just a little Location History to achieve the same end. Although Google initially "anonymized" this data, Trooper Thornton could have obtained the subscriber information at any time using a subpoena. *See Fuentes Opinion*, 481 F. Supp. 3d at 749. Others who have considered geofence warrants have also recognized the private nature of Location History data. *See Id.* at 737 ("[T]here is much to suggest that Carpenter's holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration."); *Weisman Opinion*, 2020 WL 5491763, at *5 n7 ("The government's inclusion of a large apartment complex in one of its geofences raises additional concerns … that it may obtain location information as to an individual who may be in the privacy of their own residence").

The *en banc* Fourth Circuit also recently confronted a similar retrospective location tracking scheme, and held that citizens whose locations were recorded had a reasonable expectation of privacy. *Leaders of a Beautiful Struggle v. Baltimore Police Dept.* involved a police-contracted surveillance program in which planes flew over Baltimore continuously, capturing high-resolution photographs that depicted over 32 square miles for 12 hours a day. 2 F.4th 330, 334 (4th Cir. 2021). The images were kept for 45 days. *Id.* During that time, when a crime occurred, police could review photographs from the area, and then, just as with a geofence warrant, track individuals and compile reports with images. *Id.* These "tracks" were "often shorter snippets of several hours or less." *Id.* at 342.

The Fourth Circuit held that "Carpenter applies squarely to this case" because the data allowed police to "travel back in time" to observe a target's movements, as if they had "attached an ankle monitor" to every person in the city. *Id.* at 341. This "'retrospective quality of the data' enables police to 'retrace a person's whereabouts,' granting access to otherwise 'unknowable' information." *Id.* at 342. Google location history is far more intrusive than the pixilated surveillance photos in *Leaders*. In fact, Location History data is even more intrusive than aerial surveillance photos, because it records movements inside as well as outside, including in private homes. And Location History data can stretch back months or years, for as long as the service has been enabled. Thus, under *Leaders*, as well as *Carpenter*, *Jones*, *Karo*, and *Kyllo*, Ms. Fuentes had a reasonable expectation of privacy in her data.

B. The Third-Party Doctrine Does Not Apply

The so-called "third-party doctrine" does not foreclose finding an expectation of privacy in Location History data. The Supreme Court has never sanctioned a warrantless search of an individual's cell phone location data, let alone the search of millions at once. *See Carpenter*, 138 S. Ct. at 2219 (noting that the Court has "shown special solicitude for location information in the third-party context"). Indeed, the *Carpenter* Court declined to extend the third-party doctrine to similar data and instructed lower courts not to "mechanically" apply old rules to new technologies. *Id.*

To begin with, Likewise, Location History is not a "business record," as in *Smith v. Maryland*, 442 U.S. 735 (1979). Google affirmatively states that it is the property of the account holder and not a business record. Ex. A(6) at 6-9. Nor is Location History an "invited informant" as in *Hoffa v. United States*, 385 U.S. 293, 302 (1966), or a "negotiable instrument," as in *United States v. Miller*, 425 U.S. 435, 438 (1976). All of these "third-party doctrine" cases involved situations where individuals were actively aware that they were interacting with another person or business. Here, by contrast, it is unclear whether Ms. Fuentes actively turned on Location History or, if she did, what notice she was given in the "consent flow" that accompanied that act. Instead, it is likely she did not know Location History was enabled, let alone how much data was being collected or how to manage it. There was no monthly bill to remind her, unlike the digits dialed in *Smith*. And there was no deposit slip or receipt from the bank. Rather, Location History data is most like the CSLI at issue in *Carpenter*, in which the Supreme Court found the third-party doctrine inapplicable.

Finally, Google's Privacy Policy, Terms of Service, and Consent Flows have little if any bearing on an individual's Fourth Amendment expectations of privacy. *See United States v. Irving*, 347 F. Supp. 3d 615, 621 (D. Kan. 2018) (rejecting government's argument that defendant had no expectation of privacy in his Facebook account information even though Facebook informed users that it collects user information). That is because Fourth Amendment rights do not rest on the terms of a contract. *See United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018) (recognizing that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement). As the Court said in *Smith*, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." 442 U.S. at 745. Otherwise, by "choosing" to live in the digital age and to participate in the digital world, an individual would be forfeiting any right to privacy in their effects. Such a state of affairs cannot stand when "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

As in *Carpenter*, the question is not whether there was an agreement between an individual and a service provider. The question is whether, in a "meaningful sense," users "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements" to the government. *Carpenter*, 138 S. Ct. at 2220. And in the case of Location History, Google's pop-ups and terms of service do not suffice to extinguish users' privacy interest in their account data.

II. MS. FUENTES HAD A PROPERTY INTEREST IN HER LOCAITON HISTORY DATA

Ms. Fuentes also had a property interest in her Location History data, the digital equivalent of her private "papers and effects." U.S. Const. Amend. IV. Google states 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..." Ex. A(1) at 6. Thus, Google was a mere bailee of Ms. Fuentes data, and the government converted her property interest in her data through its search and seizure. Supreme Court jurisprudence has long adhered to—and continues to validate—a property-based understanding of the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2213-14 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *Jones*, 565 U.S. at 406- 07 ("For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."); *id.* at 414 ("Katz's reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.") (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 40 ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass"). Most recently, in his dissenting opinion in *Carpenter*, Justice Gorsuch opined that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* Justice Gorsuch drew a strong analogy between cell phone location data and mailed letters, which have had an established Fourth Amendment property interest for over a century, whether or not they are held by the post office. *Id.* at 2269. Just as Gmail messages belong to their senders and recipients (and not to Google), so too does Location History data belong to the users who generate them. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010); *see also* Michael J. O'Connor, Digital Bailments, 22 U. Pa. J. Const. L. 1271, 1309 (2020) ("Founding sentiment, courts, and scholars all agree: Yes, digital documents are indeed the same papers, even if they use new and unfamiliar ink.").

Ms. Fuentes location information belongs to Ms. Fuentes. Google may be responsible for collecting and maintaining it, but Google also understands that it is private user data. Ex. A(1) at 6. For example, Google allows their users to delete data or pause the collection of data. See Ex. A(6) at 6. They view it as a "history or journal that users can choose to create, edit, and store to record their movements and travels." *Id.*

These are not "business records." Businesses do not let customers export or delete the company's records at will. Ms. Fuentes merely entrusted her information to Google. The data is heritable, alienable, and exclusive—classic attributes of property. In short, it is Ms. Fuentes (and millions of other citizens') "papers" under the Fourth Amendment, held in trust by Google. As Justice Gorsuch explained in *Carpenter*, "[e]ntrusting your stuff to others is a bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). Here, Google is the bailee, and it owes a duty to the bailor, Ms. Fuentes to keep her data safe. While Google reserves the right to use the data for advertising or development purposes, it also promises not to disclose it to companies, organizations, or individuals outside of Google, subject to a short list of explicit exceptions. In other words, Ms. Fuentes retains the right to exclude others from her location data, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Laws of England *2 (1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things … in total exclusion of the right of any other."); *Loretto v. Teleprompter Manhattan CATV Corp.,* 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most treasured strands" of the property rights bundle); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). The government converted this interest and thus committed a search and seizure under the Fourth Amendment, frustrating Ms. Fuentes right to exclusivity and control over her Location History data.

III. THE WARRANT APPLICATION FAILED TO ESTABLISH PROBABLE CAUSE THAT RELEVANT LOCATION HISTORY EXISTED

The affidavit filed in support of the search warrant failed to establish probable cause that relevant Location History existed. Probable cause is defined as "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause requires a logical connection, or evidentiary "nexus" between the crime for which probable cause exists and the evidence to be seized, which the government did not demonstrate. *See United States v. Rowland,* 145 F.3d 1194, 1204 (10th Cir. 1998) (no probable cause to demonstrate that video tapes the defendant picked up from a P.O. box and brought to work would be found in his home); *United States v. Lyles*, 910 F.3d 787, 795 (4th Cir. 2018); *see also* LaFave, 2 Search and Seizure (6th Ed.), § 3.7(d). This means a nexus between the alleged crime and any phone that is the subject of a warrant. In *Lyles*, for example, the government obtained a warrant to search a house for items including cell phones. 910 F.3d at 790-91. But the Fourth Circuit held the warrant invalid because "the warrant application lacked any nexus between cell phones and marijuana possession. There is insufficient reason to believe that any cell phone in the home, no matter who owns it, will reveal evidence pertinent to marijuana possession simply because three marijuana stems were found in a nearby trash bag. At some point an inference becomes, in Fourth Amendment terms, an improbable leap." *Id.* at 795.

As in *Lyles*, the Warrant Application here provided no case-specific facts that the driver of the car that struck Ms. Dobson was a Google user, or had Location History enabled at the time in question. The affidavit did not provide any factual information demonstrating that the driver used or possessed a cell phone or acted in concert with anyone else. *See* Ex. C. Instead, the application offers only generalizations that "drivers used smartphones in 88 out of 100 trips…"

and that a "significant number of collisions occur as a result of distracted driving from a variety of sources including cellphone use" Ex. C at ¶ 24-25.

Broad conjecture does not amount to probable cause. Probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *United States v. Curry*, No. 3:17-CR-130, 2018 WL 1384298, at *11 (E.D. Va. Mar. 19, 2018) ("[G]eneralized suspicion and fear cannot substitute for specific and articulable facts") (citations and quotation marks omitted), aff'd, 965 F.3d 313 (4th Cir. 2020); *United States v. Glenn*, No. CR-609-027, 2009 WL 2390353, at *5 (S.D. Ga. 2009) (A "generalized belief that some of the patrons whom [police] had targeted for a systematic pat down might possibly have a weapon was insufficient to justify a cursory frisk of everyone present.") (quotation marks omitted); *Commonwealth v. Brown*, 861 N.E.2d 504, 505 (Mass. App. Ct. 2007) (finding a warrant "authorizing a search of 'any person present'…resulted in an unlawful general search"); *Carroll v. United States*, 267 U.S. 132, 153–54 (1925) (stating it would be "intolerable and unreasonable" to "subject all persons lawfully using the highways to the inconvenience and indignity" to a search just because some cars may contain contraband); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding a "warrant to search all suspected places" for stolen goods was unlawful because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested"). For this reason, the D.C. Circuit struck down a warrant authorizing the search of all cell phones in a house, finding that the affidavit "conveyed no reason to think that [the suspect], in particular, owned a cell phone" and no "reason to believe that a phone may contain evidence of a crime." *United States v. Griffith*, 867 F.3d 1265, 1272-74 (D.C. Cir. 2017).

Similarly, boilerplate assertion that drivers use smartphones "'cannot substitute for the lack of evidentiary nexus'" between the particular crime for which probable cause exists and the evidence sought. *United States v. Ramirez*, 180 F. Supp. 3d 491, 495 (W.D. Ky. 2016) (quoting *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir.1994)).

However, even if the court were to engage with the government's attempts to use generalities in place of facts, Trooper Thornton's affidavit fails because the statistics provided were merely adjacent to the point they were attempting to demonstrate. The statistics would support claims that people driving and people involved in traffic accidents are likely to have been using smartphones. However, the fact that 88% of drivers used smartphones during a given drive doesn't demonstrate how many people were Google account holders or how many of them had Location History activated. The government's attempt at establishing probable cause relies on a syllogistic fallacy that goes as follows: a) 88% drivers use smartphones, b) Google Location History is generated by smartphones, therefore c) 88% drivers have Google Location History enabled. While a smartphone is a necessary element of Google Location History data collection, it is not determinative. To finish the statistical link, the government would have to establish how many smartphone users have a Google account and how many of those people have Location History enabled. The Warrant Application didn't address either question. To put this in a more obviously flawed context, it is like saying: "70% of American homes have smart televisions. Smart televisions are required to view the Netflix show 'Real Rob.' Therefore, 70% of households watch the show 'Real Rob.'"[4] Trooper Thornton's attempt at providing a statistical

[4] Although Netflix does not disclose show ratings "Real Rob" was poorly received by critics and has a Rotten Tomatoes review of 0%. Review of Real Rob, https://www.rottentomatoes.com/tv/real_rob/s01 (last visited Dec. 6, 2023).

probability was equally flawed—though buried under seemingly impressive credentials and studies.

Therefore, the Warrant Application failed to establish probable cause through factual allegations (as required by law) or statistical probability that relevant Location History data existed.

IV. THE WARRANT LACKED PROBABLE CAUSE TO SEARCH MS. FUENTES THE 592 OTHER GOOGLE USERS OR TO SUBSEQUENTLY SIEZE DATA FROM MS. FUENTES AND TWO OTHER USERS

The Warrant here entailed two massive searches of all Google users who had Location History enabled on their devices. Step one was an epic dragnet, conducted by Google at the government's direction. The Oklahoma Highway Patrol commandeered Google to search through millions of private accounts to determine if any of them contained data of interest. The Warrant was therefore unconstitutionally overbroad, a modern-day general warrant. And as if that was not sufficient, step two, allowed for the seizure of additional location data and identifying data including the account holder's names, email addresses, registration IP addresses, credit card numbers, physical billing addresses, and phone numbers—all without judicial oversight.

A. The Search

It is axiomatic that a warrant may not authorize a search or seizure broader than the facts supporting its issuance. *See Veeder v. United States*, 252 F. 414, 418 (7th Cir. 1918). Here, however, the government did not have probable cause to order Google to search Ms. Fuentes' Location History, let alone the Location History in millions of other accounts. Indeed, it is difficult to imagine that any amount of probable cause could justify a search of over 592 million accounts. Nor did they have probable cause to seize data from the three accounts identified by Google during that search.

From the outset, the government enlisted Google to search over 592 million unknown accounts in one of the largest fishing expeditions in Fourth Amendment history. The number of individuals affected by this case dwarfs the number of people searched in almost any other reported criminal opinion.[5] The fact that Google produced records for three device IDs in response does not diminish the scope of the initial search conducted at the government's behest. On the contrary, it illustrates just how broad the search really was. Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the Warrant forced Google to act as an adjunct detective, scouring the accounts of over 592 million users to generate a lead for the government. In short, the Warrant compelled a search of the intimate, private data belonging to millions, in a digital dragnet that snared three Device IDs— the data which the police then seized—all without probable cause to search or seize data from a single account. The Warrant was a massive fishing expedition, fatally overbroad from the beginning.

B. The Seizure

In addition to being overbroad in the initial search, the Warrant lacked particularized probable cause for the subsequent seizure of data from three devices located within the vicinity of a stretch of highway 10. "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). In Illinois, Judge Fuentes denied a similar geofence

[5] The only other known search that exceeds what was occurred here is known as a "reverse-keyword warrant" which occurs across all Google users regardless of whether or not they have an account or were signed in. *See e.g. People v. Seymour*, 2023 CO 53, ¶ 1, 536 P.3d 1260 (C.O. 2023).

application in part on these grounds. *See Fuentes Opinion*, 481 F. Supp. 3d 730, 754. As here, Judge Fuentes found that government's position "resembles an argument that probable cause exists because those users were found in the place . . . [where] the offense happened," an argument the Supreme Court rejected in *Ybarra*. *Id.*

Similarly, in *Chatrie*, the court stated that "warrants, like this one, that authorize the search of every person within a particular area must establish probable cause to search every one of those persons." *Chatrie*, 590 F. Supp. 3d at 927. There, at step one, the government seized data related to 19 devices found within a 150 meter radius of a bank. *Id.* The court explained that "warrants must establish probable cause that is particularized with respect to the person to be searched or seized. This warrant did no such thing. It first sought location information for all Google account owners who entered the geofence over the span of an hour." *Id.* at 929 (citations omitted). The court found "unpersuasive the United States' inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person nearby." *Chatrie*, 590 F. Supp. 3d at 933.

Here, similarly, the Warrant sought to seize data from all Google account owners found within the surroundings of a stretch of highway 10 over a four-minute period. This resulted in the seizure of six datapoints from three individuals. Thus "the warrant lacked any semblance of such particularized probable cause to search each of its [three] targets, and the magistrate thus lacked a substantial basis to conclude that the requisite probable cause existed." *Id.* at 927.

For those reasons the search of 592 million accounts and the subsequent seizure of three accounts were overbroad.

V. THE WARRANT LACKED PARTICULARITY

The Fourth Amendment's requirement that warrants "particularly describe[e] . . . the things to be seized," U.S. Const. Amend. IV, means that the description of "what is to be taken" can leave "nothing . . . to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford v. Texas*, 379 U.S. 476 (1965). The description must be provided or confirmed by a "detached" magistrate, "instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 13-14 (1948). A magistrate issuing a warrant cannot "assign[] judicial functions to the executive branch." *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 176 (4th Cir. 2019). The Warrant here violates the particularity requirement by delegating discretion at each step to Google and the Oklahoma Highway Patrol, not a judge, to answer basic critical questions.

A. Step One Seizure

The step one seizure fails the particularity requirement because it does not specify the accounts to be searched and the data to be seized. Instead, it concocted a two-step process to mask that is actually searching 592 million accounts.

Geofence warrants differ from other types of police requests. Typical requests compel Google to disclose information for a specific user, while "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." Ex. A(6) at 11. Here, the Warrant did not identify Ms. Fuentes. Nor did it identify any of the individuals whose personal information was searched and turned over to the Oklahoma Highway Patrol. Instead, the Warrant operated in reverse: it required Google to search all accounts with Location History enabled—at least 592 million people—a portion of which was then seized.

To be sure, there are circumstances where the government need not identify the name of the individual whose information is to be searched and seized. But this is not one of them. So called "John Doe" warrants—warrants that do not expressly identify the person to be searched or arrested—require something more. To comply with the Fourth Amendment, they must provide "a particularized description of the person to be arrested . . . on the face of the 'John Doe' warrant." *United States v. Jarvis*, 560 F.2d 494, 497 (2d Cir. 1977) (citing *West v. Cabell*, 153 U.S. 78, 86 (1894)).

"All persons" warrants, which aim to search and/or seize all individuals who happen to be at a location during a search—require much more: "probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004). Here, the government has not alleged any good reason to suspect or believe that all persons present within the stretch of Route 10 was guilty of causing the death of Ms. Dobson. As in *Owens*, such "all persons" language is insufficient if it is "based on nothing more than their proximity to a place where criminal activity may or may not have occurred." *See id.* at 276-77.

Finally, anticipatory warrants, which rely on a triggering condition not yet met at the warrant's issuance, require at least more than being in the wrong place at the wrong time. *See United States v. Grubbs*, 547 U.S. 90, 96-97 (holding anticipatory warrants must satisfy two prerequisites—1) "if the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place'"; and 2) "there is probable cause to believe the triggering condition will occur"—to meet the Fourth Amendment's probable cause requirement); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that in order to access a child pornography website running FBI malware, a user had to download special software and enter a 16-character URL consisting of random letters and numbers, as well as a username and password).

The Warrant here contained no names, and it contained no particularized description of the accounts to be searched and seized. There was no basis to conclude that all three of the devices identified in step one were involved in the hit and run. There was no triggering condition to cabin officer discretion. The Warrant simply failed to adequately identify any accounts and thus lacked the particularity required by the Fourth Amendment.

B. Step Two Seizure

Step two of the Warrant explicitly gave the Oklahoma Highway Patrol discretion to determine which Google users would be subject to further searches and seizures. Specifically step two said: "The Government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The Government may, ***at its discretion***, identify a subset of the devices." Ex. B Attachment B(I)(2) (emphasis added). This means that Trooper Thornton (not a court) was responsible for identifying what was "relevant" and what else to seize. Here, Trooper Thornton determined ***all*** the data returned at step one was "relevant," and without returning to the court for additional authorization or without conducting any narrowing he unilaterally obtained names, email addresses, registration IP addresses, credit card numbers, physical billing addresses, and phone numbers on all three devices. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See Fuentes Opinion*, 481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); *Weisman Opinion*, 2020 WL 5491763, at *6 ("[T]his multi-step process simply fails to curtail or define the agents' discretion in any meaningful way.").

The Fourth Amendment does not "countenance open-ended warrants, to be completed while a search is being conducted and items seized[.]" *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979). The Warrant Clause requires the determinations of probable cause and particularity be made *ex ante* by a "neutral and detached judicial officer," and not through "the hurried judgment of a law enforcement officer engaged in the often competitive enterprise of ferreting out crime." *Id.* at 326. But step two of the Warrant explicitly empowered Trooper Thornton to determine whose data was subject to seizure and the Fourth Amendment cannot sustain such a warrant because it lacks particularity.

VI. TROOPER THORNTON DECIEVED THE ISSUING MAGISTRATE AS TO MATERIAL FACTS

Trooper Thornton was able to obtain the Warrant in part because of a series of deceptions and omissions related to probable cause and how geofence warrants work. These deceptions and omissions were material and therefore require suppression pursuant to *Franks v. Delaware*, 438 U.S. 154, 155-156 (1978).

A search warrant may be vitiated upon a showing that the facts establishing probable cause contained intentional, reckless, or grossly negligent inclusions or omissions. *Id. at* 171 (intentional or reckless disregard); *see also, Davis v. United States*, 131 S.Ct. 2419, 2426 (2011) (gross negligence); *United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015) (gross negligence exception applies even when a warrant is obtained). Where those false statements or omissions are material to the issuance of the warrant suppression is required. *Franks*, 438 U.S. at 171-172.

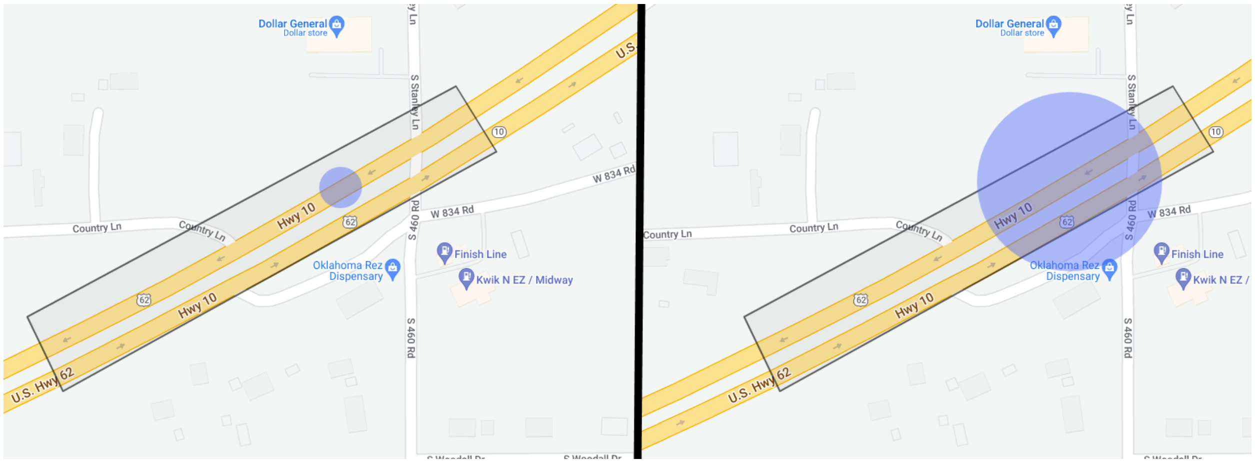
Here Trooper Thornton deceived the issuing magistrate as to how geofence warrants worked. The magistrate in this case appeared genuinely interested in reducing the number of individuals searched in this warrant. This is evidenced in their attempt to restrict the size and duration of the geofence. However, Trooper Thornton never explained that because of the way Google Location History works the magistrate was signing a warrant to search and seize data from individuals who were not actually present in the geofence at the time of the incident.

One of the purposes of the Fourth Amendment's particularity requirement is to "ensure[] that the magistrate issuing the warrant is fully apprised of the scope of the search and can thus accurately determine whether the entire search is supported by probable cause." *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986); *see also United States v. Medlin*, 842 F.2d 1194, 1195–96 (10th Cir. 1988) (search warrant for firearms used to search for stolen property); *United States v. Rettig*, 589 F.2d 418, 422-23 (9th Cir. 1979); *State v. Andrews*, 227 Md. App. 350, 413, 134 A.3d 324, 361 (2016)(holding "the government may not use a cell phone simulator without… sufficient information about the technology involved to allow a court to contour reasonable limitations on the scope and manner of the search, and that provides adequate protections in case any third-party cell phone information might be unintentionally intercepted"). In *Rettig*, the Ninth Circuit required suppression where the government withheld material information about the intended scope of the search. *Id.* "By failing to advise the judge of all the material facts, including the purpose of the search and its intended scope, the officers deprived [the court] of the opportunity to exercise meaningful supervision over their conduct and to define the proper limits of the warrant." *Id.* at 422. "A judicial officer cannot perform the function of issuing a warrant particularly describing the places to be searched and things to be seized," if "the agents withh[o]ld [material] information." *Id.* at 423. This challenge regarding the alleged scope of the search can be "distinguished from those in which the defendant seeks to attack the factual accuracy of the underlying affidavits in order to establish a warrant's improper issuance." *Rettig*, 589 F.2d at 422.

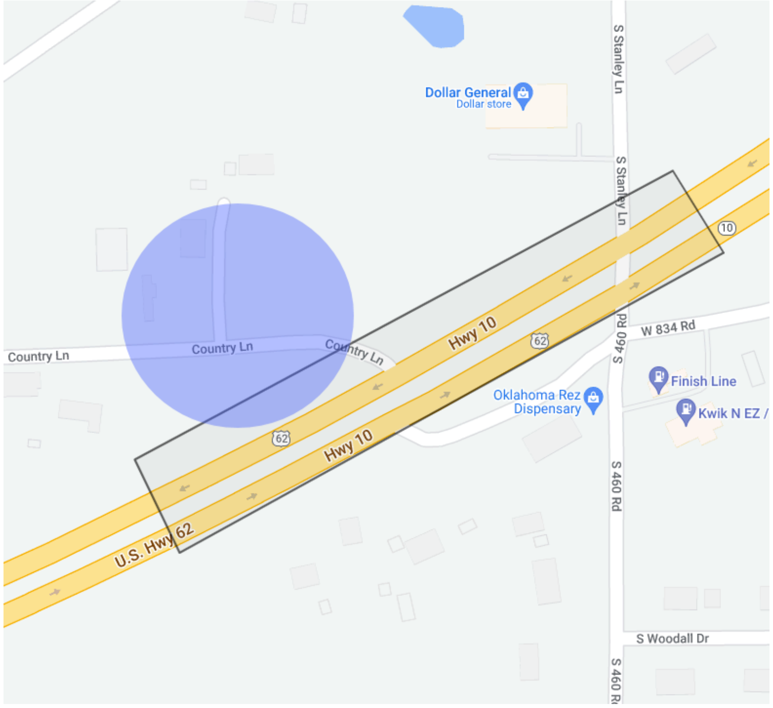
The Warrant Application here deceived the magistrate in several ways. First, the application never explained that because of the way Google indexes Location History data the search conducted at step one would entail searching approximately 592 million user accounts. Instead, the judge was left to believe that the search was just across whatever accounts were in the vicinity of the crime.

Second, the Warrant Application omitted mention of Google's acceptable error rate in their estimations of device location. Google states their goal is to correctly place a device within the display radius 68% of the time. Tr. 61:18-24; *see also* Ex. A at 6; Ex. A(2). To be clear— this is a goal and not a statistic. *Id.* So, their accuracy rate could in fact be lower. However, assuming that they met their 68% accuracy goal, devices would still fall outside that display radius 32% of the time. No explanation of these accuracy targets was contained in the affidavit and so the magistrate was left to believe the datapoints, like CSLI, represented historical fact.

Third, the Warrant Application's description of the "maps display radius" was incomplete, as it implied Google believes the device is at the actual center point or latitude/longitude provided, but that there is some chance it falls within the margin of error outside that center point. The reality is that center point is merely that- a center point. Tr. 58:21-59:12. The device is equally likely to be anywhere within the display radius. Ex A(5) at 214. This is important here because the Warrant allowed for a seizure of all device data "[f]or 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…" Ex. C Attachment B ¶ I (1). In other words, instead of authorizing a seizure of devices as shown in image 1 of figure 4,



the search authorized a search of devices as shown in image 2 of figure 4 and figure 5.



All of this means that the magistrate was under the impression that at step one they were authorizing a search for only devices within the geofence, when in reality they were authorizing a search for devices that were outside boundaries geofence. Had Trooper Thornton provided a full explanation of Google's error rates, the significance of the center point, and the relevance of each to his request, the magistrate would have denied or altered the Warrant.

Like the state judges in *Rettig* and *Andrews*, the magistrate here was left to believe the scope of the Warrant was significantly less than what it was. Instead of signing a warrant that authorized a search and seizure of only those devices within the particular geographic area depicted in the Warrant, the judge was authorizing a search of 592 million accounts and a seizure of all accounts in a much greater geographical area.

Trooper Thornton also deceived the issuing magistrate in his attempt to establish probable cause. First, he implied that he had robust training and experience with the subject matter when, in fact, this was his first geofence warrant and he had no more expertise than the average person. Tr. 116:21-23; 144:2-148:1. Furthermore, he cited misleading studies that he later admitted he never read. Tr. 148:22-148:9; 149:18-150:3. In fact, it appears the Warrant was written entirely for him and that he failed to verify multiple claims therein before submitting it to the magistrate. *See id.*

Trooper Thornton's affidavit spent 14 paragraphs in the affidavit discussing his "training and experience" with Google and "relevant technology." *See* Ex. C ¶ 7-20. However, on the stand he admitted this was in fact his first geofence warrant and his "training and experience" consisted of speaking to other officers (of unknown experience) about geofence warrants. Tr. 116:21-23 & 144:2-148:1. Furthermore, although he said talking to an expert constituted training and experience, he didn't know whether anyone he talked to could be considered an expert and none of them purported to be experts. Tr. 156:6-13.[6]

[6] While Trooper Thornton claimed much of the information in the section describing Google Location History doesn't require technical knowledge, he admitted he did not actually write any of it. Tr. 147:14-19.

In contrast to his non-existent training and experience with Google Location History, Trooper Thornton demonstrated real training and experience with regard to accident reconstruction. *See* Tr. 137:16-139:5. This included three phases of fundamental classes and further training on event data recorders, physics, video surveillance, and more. Tr. 138:13-22; *see also* Ex. E. In all this included 28 different classes trainings and certifications. *See id.* Thus, Thornton's claims that informal discussions with other officers is something the Oklahoma State Troopers consider "training and experience" is highly dubious.

This section on the Trooper Thornton's "training and experience" was drafted by AUSA Montoya and was intended to demonstrate to the judge both his credibility as an affiant and his basis for understanding Google's Location History data, how it is stored, and what it means. *Id.* Had the application correctly explained his training and experience was in fact limited to informal conversations about the technology with individuals of unknown expertise, the issuing magistrate would likely have made further inquiries about the technology as well as the statistics supposedly supporting the government's application. Or, given Trooper Thornton's lack of knowledge relating to the technology he was proposing to use, the magistrate may have simply rejected the Warrant Application altogether until it was supported by an affidavit of someone with actual knowledge of the subject matter.

Additionally, Trooper Thornton's affidavit attempted to establish probable cause that Google was in possession of relevant Location History data using statistics. In doing so, Trooper Thornton averred that he had read multiple studies that supported his conclusion that Google was in possession of Location History of the individual who struck Ms. Dobson. Ex. C at ¶ 24-25. However, he had not read those studies. Tr. 148:22-148:9; 149:18-150:3. Instead, he claimed to be relying on the fact that the person who drafted the affidavit had read them. *Id.* 150:4-151:6.

Therefore, the magistrate was left to rely on an affiant who relied on another, who, for all we know, simply copied the cite to that study from another warrant. *See id.*

These studies were inserted to bolster Trooper Thornton's expertise and provide a sense of objective truth to the likelihood that the data would exist within Google. While they do not actually establish that likelihood, *see supra* § III, they are not without effect on the magistrate and appear to be "artfully drawn" to deceive the magistrate. *See United States v. Simpson*, 813 F.2d 1462, 1471 (9th Cir 1987); *see also United States v. Aileman*, 986 F.Supp. 1228, 1240 (N.D.C.A. 1997) (Explaining in the context of wiretap affidavits "it is wholly unrealistic to expect most district judges to spend hours and hours of assertive analytical effort dissecting and probing affidavits like this. It is reasonable to expect reviewing judges to be conscientious, and to read the affidavits carefully, but the affidavits must be crafted in a way that will permit a conscientious district judge to understand all the essential elements of the investigatory situation without committing an unreasonable number of hours to the effort."); *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, 411 F. Supp. 3d 333, 336 (FISA Ct. 2019) (observing that the government has a "heightened duty of candor . . . in *ex parte* proceedings . . . such as proceedings on electronic surveillance applications") (quotation marks omitted).

Therefore, the sum total of Trooper Thornton's intentional misstatements and omissions were material to the magistrate's determination of probable cause and the issuance of the Warrant.

VII. THE GOOD FAITH DOCTRINE DOES NOT APPLY

The Fourth Amendment's most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is based on "objectively reasonable law enforcement activity." But, *Leon* "good faith" "is not boundless" and offers no qualifications in four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted as a rubber stamp for the police, id. (citing *Gates*, 462 U.S. at 288); (3) where a warrant affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid. *Id.* at 923.

The Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id.* at 917, 923. The *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was void *ab initio*. As set forth above, this geofence warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). But, even if the Court determines that *Leon* applies here, three of the firm boundaries to the good faith rule that *Leon* recognized clearly apply.

First, the good faith exception should not apply because the geofence warrant was "so lacking in indicia of probable cause" to search for Ms. Fuentes data that it was entirely unreasonable for any objective officer—i.e., one with even a rudimentary understanding of the

Fourth Amendment's requirements—to rely on. *See Leon*, 468 U.S. at 923. Police must demonstrate a fair probability that the evidence the police seek will be where they are searching. *See United States v. Gonzales,* 399 F.3d 1225, 1230 (10th Cir. 2005) (Rejecting application of the good faith doctrine where the warrant application contained "no facts explaining how the address was linked to Mr. Gonzales, the vehicle, or the suspected criminal activity, or why the officer thought the items to be seized would be located at the residence."); *United States v. Doyle*, 650 F.3d 460, 472 (4th Cir. 2011) (rejecting good-faith exception where warrant application contained "remarkably scant evidence . . . to support a belief that [the defendant] in fact possessed child pornography"); *see also United States v. Church*, 2016 WL 6123235, at *6-7 (E.D. Va. Oct. 18, 2016) (observing that good-faith exception inappropriate where no evidence to connect suspect's house to the crime under investigation); *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013). That did not happen here. Rather, the police obtained a warrant based on conjecture that Google had location data for a suspect in a fatal traffic incident—a suspect for which the police had no evidence had a cell phone, let alone one with a Google account that had Location History enabled. *See supra* § IV. Obtaining warrants based on conjecture is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

Second, the good faith exception should not apply because the geofence warrant was "facially deficient" and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. As set forth above, "it is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also Groh* *v. Ramirez,* 540 U.S. 551, 563 (2004) ("Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid."); *United States v. Leary*, 846 F.2d 592, 607- 09 (10th Cir. 1988) ("reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases); *United States v. Winn*, 79 F. Supp. 3d 904, 923-24 (S.D. Ill. 2015) (refusing to find good faith where two officers had fifteen years of experience between them and obtained a warrant that "gave them unbridled discretion to search for and seize whatever they wished"). In *Leary*, the government obtained a warrant that provided "only two limitations. First, the documents to be seized had to fall within a long list of business records typical of the documents kept by an export company. Second, those documents had to relate to "the purchase, sale and illegal exportation of materials in violation of the" federal export laws. In this context—the search of the offices of an export company—these limitations provide no limitation at all." *Leary*, 846 F.2d at 600-601. Instead, it allowed the custom agents to select what documents to search for and seize. *Id.* Here, similarly, the Warrant allowed the government to choose which accounts to seize data from at step 2. Therefore, the good faith doctrine does not apply because it was so "facially deficient in its description of the items to be seized that the executing officers could not reasonably rely on it." *Id.* at 609.

Third, the Warrant Application is riddled with false and misleading statements and is severely compromised by material omissions that would have informed the reviewing judge about the effects of authorizing such a warrant. *See supra* § VI. Here, the Warrant Application says nothing about the approximately 592 million accounts to be searched, that the effective area covered would extend well beyond the authorized geofence, that the geofence would capture devices outside of the geofence, or that the approximate device locations were only an estimated

68% accurate at best. *See id.* The Warrant Application also falsely claimed that the information returned would utilize fully anonymous GUIDs. Ex. A at 4. This level of omission and misinformation only underscores that the geofence warrant in this case was not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

Additionally, the government cannot say that Trooper Thornton acted in good faith where he ignored the three-step process designed by Google and CCIPS in 2018.[7] As explained by Mr. McInvaille, Trooper Thornton removed a step that looks at "contextual" data prior to revealing subscriber information from those accounts. Ex. A at 5. The DOJ ostensibly included this step to avoid seizing some unnecessary personal information from accounts for which the government lacked probable cause to search. However, Trooper Thornton (or the individual who drafted the Warrant) removed that step from the Warrant. In short, Trooper Thornton was neither acting in accord with legal precedent, nor internal law enforcement policy (however constitutionally unsound that policy may have been). Therefore, he cannot be said to have been acting in good faith.

The Court in *Chatrie* found that despite the fact the warrant lacked particularized probable cause, the good faith doctrine precluded suppression. *Chatrie*, 590 F.Supp.3d at 937-938. However, in *Chatrie* the detective executed the warrant on May 19, 2019, when no "court had yet ruled on the legality of such a technique." *Id.* at 938. By contrast, the Warrant in this case was submitted on April 7, 2021, after courts had started to raise serious concerns over the legality of geofence warrants. *See e.g. In re Search of Info. That Is Stored at the Premises Controlled by Google ("Kansas"),* 542 F. Supp. 3d 1153 (D. Kan. 2021) (Mitchell, Mag. J.); *Weisman Opinion,*

[7] While that three-step process is of dubious constitutional value, *see Chatrie*, 590 F.Supp.3d at 934-935, it does have some steps in place designed to reduce the number of people whose subscriber and other personal information is seized by the government.

No. 20 M 297, 2020 WL 5491763 (N.D. Ill. 2020) (Weisman, Mag. J.); *Fuentes Opinion*, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020). Furthermore, the detective in *Chatrie* had previously been granted three geofence warrants and consulted with government attorneys for the warrant in question in that case. *Chatrie*, 590 F.Supp.3d at 938. On the other hand, Trooper Thornton had never been granted a geofence warrant and apparently ceded all responsibility of drafting the affidavit to a government attorney with whom he had never worked, whose level of experience with geofence warrants he did not know, and whose work he did not check.

Therefore, the good faith doctrine from *Leon* does not apply under the facts of this case and all evidence obtained from the Warrant and the fruits thereof must be suppressed.

CONCLUSION

The Warrant in this case was completely void of probable cause, overbroad, unparticularized and almost unimaginable in scale—exactly the type of general warrant the Framers sought to prohibit through the particularity clause. Furthermore, it was obtained only through intentional, reckless, and grossly negligent omissions and deceptions. Therefore, all evidence flowing from the Warrant must be suppressed.

Respectfully Submitted,

JUAN L. GUERRA, JR. & ASSOCIATES, PLLC

/s/ Juan L. Guerra, Jr.
Juan L. Guerra, Jr.
Federal Bar No. 38079
4101 Washington Ave., 3rd Floor
Houston, Texas 77007
(713) 489-6839 - Office
(713) 571-4294 - Fax
jlg@jlglawoffice.com
Attorney for the Defendant,
Silvia Veronica Fuentes

/s/ Sidney W. Thaxter
Sidney W. Thaxter (pro hac vice)
NY Bar No. 50366009
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202)465-7654
sthaxter@nacdl.org

/s/ Michael W. Price
Michael W. Price
NY Bar No. 4771697 (pro hac vice)
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org