UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF OKLAHOMA

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

FINDINGS AND RECOMMENDATION

This matter comes before this Court on Defendant's Opposed Motion to Suppress Evidence Obtained by Google "Geofence" Search Warrant (Docket Entry #39). This Motion was referred to the undersigned for the entry of Findings and a Recommendation by United States District Judge Ronald A. White, who presides over this case. The parties were afforded the opportunity to submit additional briefing to incorporate the evidence presented at the evidentiary hearing. The submissions were made by both parties in a timely fashion.

Factual Allegations

On March 18, 2021 at approximately 9:54 p.m., a pedestrian/vehicle accident occurred at the intersection of U.S. Highway 62 and South 460 Road in Cherokee County, Oklahoma. This location was largely rural but was located within the Cherokee Nation Indian Reservation. The Oklahoma Highway Patrol responded to

the accident scene. Based upon their investigation, it was determined that J.D., a female, was traveling southbound on South 460 Road riding on her bicycle and was attempting to cross U.S. Highway 62 when she was struck by a vehicle traveling westbound on U.S. Highway 62. J.D. eventually died from the injuries she sustained in the collision.

While investigating the circumstances surrounding the collision, Dustin Thornton, a state trooper and supervisor with the Oklahoma Highway Patrol's traffic homicide unit and a Task Force Officer with the Federal Bureau of Investigation ("Thornton"), retrieved surveillance video from businesses that were in the vicinity of the accident. In all, Thornton was able to obtain three surveillance videos, one from a convenience store to the south of the intersection, one from a dispensary southwest of the intersection, and one from a car wash that was northeast of the intersection. The video from the car wash showed that a vehicle struck the bicycle, stopped briefly and pulled to the shoulder for approximately ten seconds, then left the scene. The video revealed six vehicles in all were in the vicinity, with five of them travelling eastbound. The video also confirmed that the collision occurred at 9:54 p.m.

Thornton could ascertain from the video that the vehicle involved in the collision was passenger vehicle, but because of the distance of the video camera

from the collision and the fact it was nighttime, further identification of the vehicle could not be determined. As a result, Thornton began exploring alternative methods of identifying the vehicle which brought him to the idea of geofence technology through Google, LLC. Thornton had never previously applied for a geofence warrant.

Facts Surrounding the Application and Issuance of the Geofence Search Warrant

In March of 2021, Thornton authored an Application for Search Warrant and presented the same to United States Magistrate Judge Steven P. Shreder.[1] This Application sought Location History data transmitted from any devices within a specified area to Google. Specifically, Thornton sought Location History data from Google for March 18, 2021 from 21:49 hours to 21:59 hours within a polygon specified in a map accompanying the Application as well as the longitude and latitude for the search area. Magistrate Judge Shreder rejected this first application, contending the time frame within which the device information would be disclosed by Google was too long.

Thornton then provided an Amended Application for Search Warrant to Magistrate Judge Shreder.[2] The Application sought Location History information

1 See, Gov't Exh. No. 6.
2 See, Gov't Exh. No. 1.

from Google for the date of March 18, 2021 from 21:52 through 21:56 and for a geographic area approximately 1000' by 170' with longitudinal and latitudinal coordinates. The Application also contained the following language in Attachment A:

> Time Restriction: Devices that reported their location more than once within the Targe 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.

Magistrate Judge Shreder signed this Search Warrant dated April 1, 2021. This Search Warrant, however, was withdrawn by Thornton at the request of the Government. He could not remember why it was withdrawn.

Thornton proceeded to submit a Second Amended Application for Search Warrant to Magistrate Judge Shreder.[3] This Application sought the same Location History data for the same date and time and geographic location. The difference in the request was found in the omission of language referenced above in Attachment A to the Application pertaining to "Time Restriction." On April 7, 2021, Magistrate Judge Shreder signed the Search Warrant.[4]

The Second Amended Application set out other attestations by Thornton in

3 See, Gov't Exh. No. 8.
4 See, Gov't Exh. No. 9.

justifying the existence of the Location History data sought from Google. Specifically, Thornton attested in paragraphs 7-20 of the Application as follows:

> 7) **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.
>
> 8) **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.
>
> 9) **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.

10) **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.

11) **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.

12) 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 in to 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.

13) **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.

14) **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.

15) **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.

16) **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.

17) **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.

18) 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.

19) **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.
>
> 20) **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.
>
> (Emphasis added by this Court).

Thornton testified at the hearing that, despite the references to "training and experience", the totality of paragraphs 7-20 in the Second Amended Application for Search Warrant were, in fact, authored by Assistant United States Attorney James Montoya.[5] The "training and experience" to which Thornton attests was explained by him to be primarily "conversations with other police officers mostly."[6] Thornton

5 Tr. p. 143, l. 16 through p. 147, l. 19.
6 Tr. p. 144, l. 3.

testified that he had no formal training as to any of the matters set out in paragraphs 7-20 of the Affidavit.[7] The information provided was "largely" based on conversations that Thornton had with other law enforcement.[8]

Paragraphs 21-29 of the Second Amended Affidavit for Search Warrant sets out the probable cause for the issuance of the geofence warrant. Thornton testified that AUSA Montoya also authored these sections.[9] Thornton first testified he reviewed the paragraphs for accuracy.[10] Paragraphs 24 and 25 in the Affidavit reference studies on the prevalence of cell phones in motor vehicles. These paragraphs specifically state as follows:

> 24) 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 ThemAlmostEveryTimeTheyDrive,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.

7 Tr. p. 147, ll. 20-23.
8 Tr. p. 147, ll. 24-25, p. 148, l. 1.
9 Tr. p. 148, ll. 15-17.
10 Tr. p. 148, l. 21.

> 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).
>
> 25) 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.

Thornton, as the affiant attesting to the accuracy of the content of the Second Amended Affidavit, however, stated that he had not reviewed the studies referenced in the Affidavit or written the paragraphs in the Affidavit.[11] In the end, Thornton testified that he did not know if the information provided in Paragraphs 24 and 25 was accurate.[12]

Thornton testified that prior to executing the Search Warrant for the Location History data, he had no idea of Defendant's identity, her e-mail address, or her Google identifier.[13]

11 Tr. p. 148, ll. 22-25, p. 149, l. 1, 7-9, 23-25.
12 Tr. p. 150, ll. 1-3.
13 Tr. p. 153, ll. 15-23, p. 154, ll. 13-16.

The Mechanics of Google's Compliance With the Search Warrant

The source of the information sought by the Search Warrant in this case is the activated Location History on a device such as a cell phone utilizing a Google created and sponsored application. As explained in the amicus curiae brief filed by Google in another proceeding, millions of users choose to create a Google account and log into them from their mobile devices or while using Google applications to take full advantage of account-specific products such as the e-mail application, Gmail and to obtain a more personalized experience on applications such as Google Maps or the Google Search Engine. Location History is an optional account-level Google service. It does not function automatically for Google users but must be consciously activated. But when users opt into Location History on their Google accounts, it allows those users to keep track of locations they have visited while in possession of their mobile devices. Google describes Location History as being where "information is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels."[14] Location History allows a Google user to "keep a virtual journal of her whereabouts over a period of time."[15] This journal is captured in the Timeline feature of the Google Maps

14 See, Def. Exh. A6 at p. 6.
15 Id.

application.[16]

In order to activate Location History on a device, the user must (1) ensure the device-location setting on her mobile device is turned on. When this is activated, the mobile device automatically detects its location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks; (2) the user must configure her mobile device to share location information with applications capable of using that information; (3) the user must opt into Location History in her account settings and enable "Location Reporting"; and (4) to actually record and save Location History data, the user must sign into her Google account on her device and travel with that device.[17] Google states that the Location History data "can be considerably more precise" that other kinds of location data, including cell site location information ("CSLI").[18] The location provided, however, is a "probabilistic estimate" of the user's location based on "multiple inputs" with each input having a margin of error so that a user's actual location will not always align with any one estimation location data point in the Location History.[19] When Google reports the estimated longitude and latitude of a user's device, it also provides a display radius where the device may be located in its estimation. According to the

16 Id.
17 Id. at p. 7-8.
18 Id. at p. 10.
19 Id. at p. 10, n.7.

evidence, Google estimates that the device should be located within the display radius provided with a goal to be 68% accurate.[20]

A three-step process designed by Google and the Computer Crime and Intellectual Property Section of the Department of Justice is employed to obtain a geofence information pursuant to a warrant from Google. In the first step, "law enforcement generally obtains a search warrant compelling Google to disclose a deidentified list of all Google user accounts for which there is saved [Location History] information in a defined geographic area during a defined timeframe." In order to accomplish this first step, Google must conduct a search across all Location History data to identify users within the relevant timeframe and run a computation against every set of stored Location History coordinates to determine which records match the geographic parameters in the warrant.[21] In 2018, it was estimated that approximately 592 million users had Location History activated on their Google account and the step one parameters requires a search of all of these accounts for time and geographic compliance.[22]

At step two of the process, the Government review the anonymized data produced at step one to identify anonymized device numbers of interest. Some of

20 See, Def. Exh. No. A at p. 7.
21 See, Def. Exh. No. A3 at p. 2, ¶ 6-7.
22 See, Def. Exh. No. A at p. 3.

the devices are eliminated because of time spent in the geographic area of interest. The Government then identifies which anonymized device numbers for which it will require Google to produce identifying user account information.[23]

At step three, the Government can compel Google to provide account-identifying information for the anonymized device numbers it determines are relevant to the investigation. This request then requires Google to provide account subscriber information on the now-identified devices. This may include the Gmail address associated with the account and the first and last name entered by the user on the account.[24]

The Search Warrant and Its Execution in This Case

The Search Warrant signed in this case directed Google to

1) query Location History data based on the Initial Search Parameters of geography and time identified in the Application and for each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (i.e., "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the Government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2) 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

23 See, Def. Exh. No. A6 at p. 14.
24 Id.

may, at its discretion, identify a subset of the devices.

3) Google shall disclose to the Government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the Government inquires.[25]

The information authorized by the Search Warrant permitted the Government to obtain non-anonymized data for the devices responsive to the search parameters since it required the production of device IDs. The original Affidavit sought for Google to produce "a (sic) anonymized identifier, known as a Reverse Location Obfuscation Identifier . . . that Google creates and assigns to device for purposes of responding to this search warrant."[26]

The Search Warrant executed in this case only required a two-step process to be followed. The process employed, however, deviated from the three-step process established between Google and the Government in that the information produced under step one was not anonymized and in a second step, the specific account information was then produced based entirely upon the Government's judgment as to which account user information was relevant to their investigation and would be produced by Google.

In this case, Google provided six data points which included three unique

25 See, Gov't Exh. No. 9.
26 See, Gov't Exh. No. 8 at p. 11.

device IDs. Three data points were connected to Defendant's account, two data points were connected with an account ending in 008, and one data point was associated with an account ending in 161.[27] After this data was produced, Thornton requested and obtained personal account identifying information on all three accounts.[28]

Thornton immediately eliminated the person associated with the account ending in 008 because the individual stayed at the scene until law enforcement arrived.[29] If the Search Warrant had followed the three-step process, this account would have likely been eliminated from the investigation without the revelation of the individual's personal information because the contextualized data would have been evaluated for the length of time the user stayed at the scene.[30]

Based upon the information obtained from Google, Thornton obtained address and other personal information pertaining to Defendant. He located her homes in Broken Arrow, Oklahoma and found that a white vehicle was parked in front of one home. Thornton had retrieved pieces of a white vehicle at the accident scene. He obtained a Search Warrant from Google of records from Defendant's Google accounts on April 28, 2021.[31]

---

27 See, Gov't Exh. No. 11.
28 See, Gov't Exh. No. 15, 16, and 17.
29 Tr. p. 71, l. 24 through p. 72, l. 2.
30 Tr. p. 72, ll. 3-17.
31 See, Gov't Exh. No. 3 and 4.

On November 10, 2021, a grand jury returned an Indictment of Defendant on the charge of the Failure to Stop for Accident Involving Death in Indian Country in violation of 18 U.S.C. §§ 13, 1151, 1152 and Okla. Stat. tit. 47 § 10-102.1. Defendant filed the subject Motion to Suppress contending that the Search Warrant served upon Google was devoid of probable cause and was overbroad, unparticularized and constituted a prohibited general warrant.

Analysis

> While the machinery of law enforcement and indeed the nature of crime itself have changed dramatically since the Fourth Amendment became part of the Nation's fundamental law in 1791, what the Framers understood then remains true today—that the task of combating crime and convicting the guilty will in every era seem of such critical and pressing concern that we may be lured by the temptations of expediency into forsaking our commitment to protecting individual liberty and privacy. It was for that very reason that the Framers of the Bill of Rights insisted that law enforcement efforts be permanently and unambiguously restricted in order to preserve personal freedoms. In the constitutional scheme they ordained, the sometimes unpopular task of ensuring that the government's enforcement efforts remain within the strict boundaries fixed by the Fourth Amendment was entrusted to the courts.[32]
>
> - Supreme Court Justice William Brennan

32 United States v. Leon, 468 U.S. 897, 929–30, 104 S. Ct. 3430, 82 L. Ed. 2d 677 (1984)(Dissenting opinion).

The Fourth Amendment to the United States Constitution requires that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., amend. IV.[33] "The touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'" California v. Ciraolo, 476 U.S. 207, 211, 106 S. Ct. 1809, 1811, 90 L. Ed. 2d 210 (1986) quoting Katz v. United States, 389 U.S. 347, 360, 88 S.Ct. 507, 516, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). Justice Harlan established a two-part inquiry in Katz in evaluating whether an expectation of privacy may be found. First, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable? Smith v. Maryland, 442 U.S. 735, 740, 99 S.Ct. 2577, 2580, 61 L.Ed.2d 220 (1979).

Geofence warrants are a different animal brought about by the digital age of information and communication. While the law sometimes struggles to remain relevant in the ever-changing technological landscape, extrapolation of existing precedent may often be justified to arrive at a just result. The Supreme Court in

33 Additionally, the production of information by Google is governed by the Stored Communications Act, 18 U.S.C. § 2703.

Carpenter v. United States, 585 U.S. 296, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) provides such an opportunity in this case.

In Carpenter, the Supreme Court recognized that "[t]he 'basic purpose of [the Fourth Amendment], . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Carpenter, 585 U.S. at 303 quoting Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). The Supreme Court acknowledged the role that cell phones have achieved in the lives of the citizenry in stating

> a cell phone — almost a "feature of human anatomy," Riley v. California, 573 U.S. 373, 385, 134 S.Ct. 2473, 2484, 189 L.Ed.2d 430 (2014) — tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. See id., at 395, 134 S.Ct., at 2490 (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); contrast Cardwell v. Lewis, 417 U.S. 583, 590, 94 S.Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality opinion) ("A car has little capacity for escaping public scrutiny."). Accordingly, when the
>
> Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.
>
> Carpenter, 585 U.S. at 311–12, 138 S. Ct. at 2218.

The Court concluded that the defendant in that case had a "reasonable expectation of privacy in the whole of his physical movements." Id. at 313. In so

doing, it found 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." Id.

The similarity between CSLI data and the Location History data at issue in this case is striking. This brings this Court to the juxtaposition of two schools of interpretation of the data derived from geofence warrants represented in the primary two recent cases at the circuit level addressing the issue – United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024) and United States v. Smith, 110 F.4th 817 (5th Cir. 2024). In Chatrie, the Court found that the geofence location information obtained for the defendant in that case for a two-hour period did not implicate a right to privacy, concluding "[a] record of a person's single, brief trip is no more revealing than his bank records or telephone call logs." Chatrie, 107 F.4th at 331. This would seem to imply that it is not the nature of the privacy right violated – here one's location – but rather the duration of the violation. This position is untenable from a constitutional perspective. Once the Supreme Court recognized a right to privacy in an individual's "physical movements" as it did in Carpenter, the duration of the monitoring became irrelevant to the analysis.

This Court aligns its position with that of the Fifth Circuit in Smith, where the Court concluded "geofence location data is invasive for Fourth Amendment

purposes. Of particular concern is the fact that a geofence will retroactively track anyone with Location History enabled, regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection." Smith, 110 F.4th at 834. There can be little doubt that the execution of the geofence search warrant constitutes a "search" under the Fourth Amendment in light of the mechanics employed to obtain the information and the invasiveness of the information sought.

The Government has implicated the "third-party doctrine" in countering the expectation of privacy in the geofence arena. The "third-party doctrine" provides that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Carpenter, 585 U.S. at 308 quoting Smith v. Maryland, 442 U.S. at 743-44. So the argument goes, since the Google users have opted into the Location History, they have voluntarily allowed their location data to be collected. Again, this Court concurs with the Fifth Circuit in Smith that the opt-in procedures involved with the authorization of the collection of Location History data cannot hardly be considered wholly informed and voluntary. Smith, 110 F.4th at 835. Additionally, this Court is convinced the sheer number of 592 million users who have allegedly "opted in" to the collection of this data reveals the lack of informed consent of these users. Id. at 835-36.

Since the protections of the Fourth Amendment are in play, law enforcement was required to obtain a valid search warrant supported by probable cause and particularity. Id. at 836 citing Carpenter, 585 U.S. at 316. An affidavit in support of a search warrant application establishes probable cause if "it evinces a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Cotto, 995 F.3d 786, 796 (10th Cir. 2021). In this case, law enforcement had a reasonable suspicion that a crime had been committed at a particular location but absolutely no showing in the Affidavit for Search warrant that Google held evidence of a crime in its Location History data since it had no idea who committed the crime. *See* Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153, 1156 (D. Kan. 2021).

Further, law enforcement's inclusion in the Affidavit of studies that ostensibly demonstrate that cell phones are ubiquitous and present in a certain number of vehicles falls far short in establishing probable cause since there was a complete absence of evidence that the alleged perpetrator of the hit-and-run accident possessed a cell phone or that the cell phone that might have been possessed by the perpetrator opted into the location and retention of Google's Location History.

In a similar vein, the Search Warrant was also wanting for particularity. The primary purpose behind a requirement for particularity in a search warrant stems

from a premise that "searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S. Ct. 2022, 2038–39, 29 L. Ed. 2d 564 (1971), *holding modified by* Horton v. California, 496 U.S. 128, 110 S. Ct. 2301, 110 L. Ed. 2d 112 (1990). The geofence search warrant at issue in this case required that Google search through 590 million users in step one of the search and their Location Histories without any direction toward a particular person – only a time and a location. This is the hallmark of a general warrant – aimless searching with only the hope that the result will justify the means. It does not. The support is eroded even more in this case because the Affidavit allegedly bolstering its issuance does not even adhere the three-step process established by the Department of Justice and Google, eliminating the anonymizing step before leaving the matter entirely up to law enforcement before procuring the specific sensitive personal information of the uncovered users at step one. Consequently, this Court must conclude that the geofence Search Warrant employed in this case represents a constitutionally deficient general warrant without sufficient probable cause to support it. This Court is dubious whether a geofence search warrant of this nature may ever pass constitutional muster under the Fourth

Amendment's rubric. Today, the constitutional protections provided herein are applied to this Defendant in this circumstance.

Good Faith Exception

A final possible safe harbor to protect the geofence search and the evidence derived from them lies in the concept of good faith. Although a search warrant may not facially demonstrate probable cause, the evidence seized in the execution of the warrant need not be suppressed if the executing officer acted with an objective good-faith belief that the warrant was properly issued by a neutral magistrate. United States v. Leon, 468 U.S. 897, 922 (1984). Four situations are recognized in Leon which might vitiate the good faith exception to the exclusionary rule: (1) when the issuing magistrate was misled by an affidavit containing false information or information that the affiant would have known was false if not for his "reckless disregard for the truth". Id. at 923; (2) when the "issuing magistrate wholly abandon(s) his judicial role". Id.; (3) when the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable". Id.; and (4) when a warrant is so facially deficient that the executing officer could not reasonably believe it was valid. Id.

Although Thornton attested to numerous facts in the Affidavit for Search Warrant, he had actual knowledge of very little of the information provided to the

neutral Magistrate Judge. His attestation that the information provided was "based upon his training and experience" was simply false. AUSA Montoya ghost wrote the vast majority of the Affidavit without being the party attesting to the veracity of the information provided. Moreover, the Affidavit failed to include information surrounding the search, including the protections of the full three-step process established by the Department of Justice and Google to protect the anonymity of the information produced in the search. Additionally, the Affidavit lacked probable cause on its face for the issuance of the Search Warrant. No facts were presented on the face of the Affidavit to remove the Search Warrant from the ominous shadow of a general warrant. Indeed, the Affidavit was completely lacking any facts to indicate that the perpetrator of the offense possessed a cell phone, such as a view from one of the video surveillance cameras showing a person holding a cell phone or similar independent evidence implicating a cell phone's use – only studies which demonstrate that people in cars have cell phones. This falls short of good faith and mandates the suppression of the evidence derived from the Google search.

IT IS THEREFORE THE RECOMMENDATION OF THIS COURT that Defendant's Opposed Motion to Suppress Evidence Obtained by Google "Geofence" Search Warrant (Docket Entry #39) be **GRANTED** and that the evidence derived from the Location History search by Google be **SUPPRESSED**.

The parties are given fourteen (14) days from the date of the service of these Findings and Recommendation to file with the Clerk of the court any objections with supporting brief. Failure to object to the Findings and Recommendation within fourteen (14) days will preclude appellate review of the judgment of the District Court based on such findings.

IT IS SO ORDERED this 3rd day of September, 2024.

JASON A. ROBERTSON
UNITED STATES MAGISTRATE JUDGE