

STATE OF MCGEE
DISTRICT COURT
14th Circuit

Criminal No. 24-CR-13-1312

State of McGee,

Plaintiff,

vs.

**MOTION DENYING
MOTION
TO SUPPRESS**

Cheyenne Nez,

Defendant.

The above-entitled matter came before this Court on August 22, 2023, on Defendant's motion to suppress evidence acquired through the exercise of a geo-fencing warrant. The State was represented by Adolfo Flores. Defendant was represented by Madeline Matlock.

In the underlying matter, the State of McGee charged Defendant Nez with three counts of simple battery, disorderly conduct, and two counts of aggravated assault via bodily fluids. The case went to trial, and on the eve of trial, Defendant filed a motion to suppress evidence acquired through a warrant. Defendant asserted that the geofencing warrant violated the Fourth Amendment and lacked probable cause because it was fatally overbroad. This court finds that the search warrant in this matter lacked probable cause but that despite the errors in the warrant the good-faith exception precludes the application of the exclusionary rule and as such this court denies Defendant's motion and

STATE OF MCGEE
DISTRICT COURT
14th Circuit

sets this matter for trial at the Court's earliest available date.

I. Findings of Fact

On August 22, 2023, this matter came before the Court at a hearing on Defendant's pretrial motions. The following facts were established through stipulation and testimony. On January 14, 2023, Cheyenne Nez rode in a van with four other individuals to a political event being held at the federal courthouse in Tulsa, McGee. Evidence uncovered over the course of the investigation showed that this event was planned over several weeks, and Defendant Nez was involved in several of the planning meetings, including an in-person planning meeting on January 13, at a private residence in Tulsa. There were civil rights advocates from a coalition of roughly one dozen groups coming to attend the protest. They had named their coalition "Family Values" and were loosely using the slogan, "Our families deserve to survive your police." The protest was in response to the police shooting of a young black man on December 3, 2022, and rumors that, after the local District Attorney's Office had declined to press charges a month ago, the United States Attorney's Office was going to announce that the Department of Justice would not seek federal charges.

Activists began gathering at the courthouse on January 14, 2023, at 9:00 a.m., in anticipation of an 11:00 a.m. press conference. Activists set up tents and a small stage in a public square in front of the courthouse; they also set up wooden barricades with political slogans written on them. When courthouse security moved the barricades, activists did not put up any protest. The crowd was subdued and allowed people to enter and leave the courthouse with minimal badgering and no physical interference. At 11:00 a.m., the gathering, which had swelled to around 75 people, received the real-time text of the press release. As the message circulated through the crowd, various chants started up, including:

STATE OF MCGEE
DISTRICT COURT
14th Circuit

“We are here,
We are queer,
You should be in fear”

“Hey, hey, ho, ho,
These racists cops have got to go”

“We drove all night,
We know what’s right
We brought our girls
We came to fight.”

As the crowd and the chants gained momentum, some counter-protesters began to gather around the protestors; some of the counter-protesters began yelling: “Do the crime, do the time” and “Blue Lives Matter.” The United States Marshals working security at the courthouse, along with several city police became aware of the confrontation and began to herd the protestors off the front walk and back into the small square to the west side of the front entrance.

As the police line formed, a protester, using a gallon bucket, sprayed the police officers with a red liquid that subsequent investigation determined to be pig's blood and saliva acquired from numerous protesters who spat in the bucket. Later, as the protester was attempting to spray the police a second time, the bucket flew out of their hand and hit a counter-protester in the nose knocking them to the ground and causing significant abrasions. Body-camera footage at the time shows Defendant yelling, “hit ‘em, hit back!” And, it appears, she joined a sing-song chant of “AYYYYYCAB, AYYYYYCAB, AYYYYY CAB,” a phrase coined by anti-police activists meaning, “All Cops Are Bast**ds.”

STATE OF MCGEE
DISTRICT COURT
14th Circuit

Despite the defiant chanting, Defendant appeared to comply with instructions from the police and allowed herself to be directed back into the public square. But after the counter-protester was struck with the bucket, the police put on gas masks, raised their riot shields, and pressed forward aggressively. The protesters, in seeming coordination, turned the signs they were holding upside down and began to strike officers with the wooden 2X2 posts to which the signs were attached. Defendant was shoved with a riot shield and, apparently in response, swung her sign's wooden stake, striking two officers repeatedly. She then reached out and tripped a police officer to the ground, who fell onto the concrete and suffered several abrasions and a contusion to his forehead. Defendant then fled the scene.

On January 18, 2023, the Federal Bureau of Investigation (FBI) sought a geofencing warrant for a three-hour window and a 150-yard radius of the courthouse. (*See Ex. A*). The undersigned agent has been granted geofencing warrants on four distinct occasions in past cases, all with similar or larger temporal and geographic parameters. The agent who submitted the search warrants did not seek legal counsel related to these geofence warrants but has consulted with the United States Attorney's Office on prior cases.

The officers also sought a search warrant for the house where the January 13, 2023, planning meeting was held and a geofencing warrant for a 150-yard radius of the home, with a three-hour window on either side of the meeting time. A judicial officer granted those warrants on January 18, 2023, and they were served on Google promptly.

Documents submitted with the search warrant to Google indicated that the police expected Google to do the following:

First, Google would search for "location history" data, for those time frames, dates, and locations, identifying the Google-connected devices

STATE OF MCGEE
DISTRICT COURT
14th Circuit

that traversed the time, date, and geographic parameters of the geofences. This search by Google would generate “location points,” which would consist of an identification of (a) the devices that were in the two physical locations during the specified date and time ranges, and (b) the devices that generated “location points” *outside* the search parameters but within a “margin of error” that “would permit the device to be located within” the search parameters, as the January 18, 2023, Application described this “margin of error.”

Second, for each of the Google-connected devices identified from the foregoing two sets of “location points,” Google would produce to the government anonymized information specifying the unique device identifier, timestamp, location coordinates, “display radius,” and “data source,” to the extent this information is available.

After Google submitted this information to the government, the government would review the anonymized information and would communicate to Google the mobile device identifiers (from the anonymized information) seeking the identifying subscriber information for the Google accounts associated with each of those specified mobile devices, identified at the government's discretion.

On April 5, 2023, Google submitted the device information for 137 cell phones located within the two requested radiuses, and a list of 18 devices that had been at both locations. Police requested identifying subscriber information from Google for those 18 devices.

Police then sought, and obtained, a search warrant for Nez’s cell phone provider Verizon Wireless for a 48-hour window around the time of the protest. Verizon provided the police with extensive text message records from Defendant.

STATE OF MCGEE
DISTRICT COURT
14th Circuit

The records the State would seek to admit at a trial of this matter are as follows:

- Location data that places Nez within the geofence of the planning meeting from 10:04 p.m.-12:35 a.m. on January 13, 2023, and within the courthouse Geofence from 8:47-11:12 am on January 14, 2023.
- Text messages indicating that the protest had been planned at length and that Nez was aware of multiple individuals' willingness to be arrested, although Nez had not communicated such a desire.
- The following exchange from the morning of January 14:
 - 7:15 a.m. Defendant Nez: "Cannot wait for the cops to get doused in pig's blood."
 - 515-111-2222: "Not sure we got enough to really douse them."
 - Defendant Nez: "I am sure I can add a little something to the mix."
 - 9:20 a.m. Defendant Nez: "A little pig's blood, a little of my spit, we will show them."

Based on the information obtained via the geofencing warrants, a grand jury returned an indictment against Defendant Nez on three counts of Simple Battery, one count of Disorderly Conduct and two felony counts of Assault with Bodily Fluids.

Defendant has filed a motion seeking to suppress all evidence obtained pursuant to the geofencing warrants served on Google and to suppress the cellphone data, both phone calls and text messages, because she contends that the search warrants lacked probable cause because they are overly broad. The State argues that the warrants were a precaution but not strictly necessary because these were not searches that implicate the Fourth Amendment, but even if they did, they have the requisite specificity under the law. The State argues that, moreover, the

STATE OF MCGEE
DISTRICT COURT
14th Circuit

officers were acting in good faith due to the novel nature of the developing science of geofence warrants, and any error the Court finds does not warrant exclusion of any evidence.

II. Statement of Law

The Fourth Amendment protects an individual's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV. The "basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Carpenter v. United States, 585 U.S. 296, 303 (2018) (quoting Camara v. Municipal Court, 387 U.S. 523, 528 (1967)). Not only has the Court long recognized that "the Fourth Amendment protects people, not places," but the Court has "expanded [its] conception of the Amendment to protect certain expectations of privacy as well." Id. at 304 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)). "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Court] ha[s] held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." Id. (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)). In determining whether an expectation of privacy is reasonable, the Supreme Court has adopted the Harlan concurrence in Katz: "There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361.

Geofencing warrants are a recognized law enforcement tool used to work backwards to learn identity from the location of a device rather than to investigate an individual based on specific information about them. See United States v. Rhine, 652 F. Supp. 3d 38, 66 (D.D.C. 2023). Google has been the primary recipient of geofencing warrants because

STATE OF MCGEE
DISTRICT COURT
14th Circuit

Google has obtained location data from users who have opted into allowing their phone to transmit this information to Google. *See generally, Haley Amster & Brett Diehl, Note: Against Geofences*, 74 Stan. L. Rev. 385 (2022). Geofencing warrants cover broad areas and raise constitutional issues about the disclosures of the “privacies of life” recognized as protected. *See United States v. Karo*, 468 U.S. 705, 715-18 (1984); *United States v. Kyllo*, 533 U.S. 27, 37 (2001).

The Fourth Amendment does not protect information voluntarily disclosed to a third party because even a subjective expectation of privacy in such information is “not one that society is prepared to recognize as ‘reasonable.’” *United States v. Graham*, 824 F.3d 421, 427 (4th Cir. 2016) (quoting *Smith*, 442 U.S. at 743) (quotes omitted). This concept is known as the “third party doctrine.” *Id.* If the third-party doctrine is applicable, the government has not engaged in a Fourth Amendment search by obtaining that data. *See id.*

Although the Fourth Amendment does not govern information voluntarily disclosed to third parties, as it relates to electronic surveillance data, the Court has held that “[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance . . . will require particular attention.” *United States v. Jones*, 565 U.S. 400, 450 (2012). Courts have recognized this concern in relation to cellular data asserting that “[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Carpenter*, 585 U.S. at 311. Cell Site Location Information (CSLI), a type of location Data collected from cell phones, has been recognized as a search triggering the warrant requirement. *Id.*

A. Location history is the type of data that carries a reasonable expectation of privacy.

STATE OF MCGEE
DISTRICT COURT
14th Circuit

There is no more expansive tool for collecting and storing location data than Google’s location history. See United States v. Chatrie, 590 F. Supp. 3d 901, 908 (E.D. Va. 2022).

Google Location History “allows[s] users to view their Location History data through its “Timeline” feature, a depiction of a user's collected Location History points over time. According to Google, this permits Google account holders to “choose to keep track of locations they have visited while in possession” of their mobile device... Google's “radius targeting” also allows—again without identifying any user— “a business to target ads to users that are within a certain distance of that business.”

Chatrie, 590 F. Supp. 3d at 907-908 (internal quotations omitted).

Although, as previously noted, the Fourth Amendment does not protect information voluntarily disclosed to a third party, cell phones and cell-tower location information are distinct technological advances that force a specific analysis. See Carpenter, 585 U.S. at 297 (noting that “[a] majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records — which hold for many Americans the ‘privacies of life,’ —contravenes that expectation.”) (quoting Riley v. California, 573 U.S. 373, 403 (2014)). The Supreme Court requires that trial courts “take account of more sophisticated systems that are already in use or in development,” and the implications those new practices have for how expansive the data is that is collected. Kyllo, 533 U.S. at 36.

In Carpenter, the Court held that CSLI data collection needed to cover a minimum time frame to implicate the Fourth Amendment. 585 U.S. at 340. Specifically, the Court held that seven days was long

STATE OF MCGEE
DISTRICT COURT
14th Circuit

enough to implicate the Fourth Amendment, see id. at 396 (Gorsuch, J., dissenting.) while still recognizing that short-term searches may still be capable of revealing the “privacies of life,” Id. at 334.

The main distinction is whether location history data collected over a briefer period is different from CSLI data such that there is a difference in the expectation of privacy. While Carpenter involved a 7-day period, and the Jones GPS case dealt with 28 days, several lower courts have addressed the generally narrower time frame of location information and found that geofences involving much shorter durations involve those same privacies of life. See Matter of Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) (“Nonetheless, there 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.”)

The State argues that the narrow parameters of the search warrants here, and the brief time covered by the geofencing warrant, limits the intrusion by the government and means the Fourth Amendment is not implicated.

But this Court finds, consistent with Carpenter and Riley, the History Location data collected from Google in this case implicates the Fourth Amendment. In other words — location data collected via a geofence for any period carries with it such significant details of an individual's private life that it implicates the Fourth Amendment

B. Turning on location data is not the type of third-party disclosure that invalidates an expectation of privacy.

“The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information

STATE OF MCGEE
DISTRICT COURT
14th Circuit

knowingly shared with another.” Carpenter, 585 U.S. at 296. Individuals have “no legitimate expectation of privacy” in information they have provided for private or commercial reasons to another. Smith, 442 U.S. at 743–44. By “revealing his affairs to another,” the person “takes the risk ... that the information will be conveyed by that person to the Government.” U.S. v. Miller, 425 U.S. 435, 443 (1976).

Carpenter held that the third-party doctrine does not apply as an exception to the Fourth Amendment's warrant requirement when the government seeks cell site location information. See Carpenter, 585 U.S. at 309 (“We decline to extend Smith and Miller to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.”) Google Location History has been analyzed by lower courts similarly to Carpenter's treatment of cell site location information. See United States v. Chartrie, 590 F. Supp. 3d 901, 907-908 (E.D. Va. 2022).

The State argues that, by “opting in” to location services, an individual is on notice that their location is not private and would not reasonably expect that data to be held confidential.

But a user merely has to opt-in one time for Google to collect their location history in perpetuity without regard for whether they are actively using their device. See In re Google Location His. Litig., 514 F. Supp. 3d 1147, 1151 (N.D. Cal. 2021). The user then has no knowledge of the commercial entities with whom Google is sharing their location. Id. As such, it is unreasonable to believe that a user expects that data to be accessed beyond the limited function they are opting in for, and no understanding of the full scope of what they are disclosing. Under these circumstances, this court declines to find that the third-party doctrine undermines the reasonable expectation of privacy surrounding cell

STATE OF MCGEE
DISTRICT COURT
14th Circuit

phone location data and this was a search that implicates the Fourth Amendment.

C. The geofencing warrants did not meet the breadth and particularity requirements of the Fourth Amendment

The Fourth Amendment dictates that only when there is an evidentiary nexus between the area to be searched/item to be seized and criminal activity can there be probable cause to search that place or seize that item. See United States v. Lyles, 910 F.3d 787, 795 (4th Cir. 2018). “[W]hen the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue.” Fisher v. United States, 425 U.S. 391, 400 (1976).

Over-breadth and particularity are both aspects of the probable cause analysis. Particularity requires that there be “a fair probability that contraband or evidence of a crime will be found in a particular place.” Illinois v. Gates 462 U.S. 213, 214 (1983) “[W]hen the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue.” Fisher, 425 U.S. at 400.

A warrant must “confine the executing [officers'] discretion by allowing them to seize only evidence of a particular crime.” United States v. Cobb, 970 F.3d 319, 328 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting United States v. Fawole, 785 F.2d 1141, 1144 (4th Cir. 1986)). A warrant must “identif[y] the items to be seized by their relation to designated crimes,” and the “description of the items [must] leave [] nothing to the discretion of the officer executing the warrant.” United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010) (citation omitted). “So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish

STATE OF MCGEE
DISTRICT COURT
14th Circuit

between those items which are to be seized and those that are not ... the particularity standard is met.” United States v. Blakeney, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted).

Probable cause requires a logical connection, or evidentiary “nexus” between the crime for which probable cause exists and the evidence to be seized. “[A] particular decision to search is tested against the constitutional mandate of reasonableness,” and a reviewing court must “focus upon the governmental interest which allegedly justifies official intrusion” and during a criminal investigation for evidence “only when there is ‘probable cause’ to believe that they will be uncovered in a particular dwelling.” Camara v. Municipal Court, 387 U.S. at 534–535. When a warrant grants wide discretion to officers to search and seize in places that lack a nexus to the crime, it is overly broad and is in danger of running afoul of the Fourth Amendment. See Groh v. Ramirez, 540 U.S. 551 (2004)

Probable cause demands that law enforcement possess “a reasonable ground for belief of guilt ... *particularized* with respect to the person to be searched or seized.” Maryland v. Pringle, 540 U.S. 366, 370 (2003) (emphasis added); See Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (“Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.”) 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, 444 U.S. at 91.

Defendant argues that the lack of particularized suspicion related to the individuals within the geofence violates their constitutional rights. And Courts considering the wide swath of people who fall into broad geofence searches have found that a lack of particularity as to the individuals to be searched creates a fatal flaw in the particularity requirement. See In re Search of Information Stored at Premises, 481 F.

STATE OF MCGEE
DISTRICT COURT
14th Circuit

Supp. 3d 730 (N.D. Ill. 2020); Chartrie, 590 F. Supp. 3d at 907-908. Other courts have cautioned that the individuals whose information is anonymized never come into the possession of the government and as such they are never “searched” and should not be considered in the analysis. See United States v. Davis, 109 F.4th 1320, 1332 (11th Cir. 2024).

The particularity requirement is a highly fact-based analysis and requires consideration of the specific evidence sought and the probable cause to believe that it exists in the location in question.

The FBI certainly had probable cause to believe that evidence related to the assaults in question could be collected based on identifying the parties present during the time frames in question. Furthermore, the ubiquitous nature of cellphones makes it probable that the perpetrators would be carrying the devices that identified them. The warrants in question also requested the data for a narrow time frame and for a tight radius of the area in question, theoretically limiting the number of uninvolved individuals incidentally snagged in their drag net.

However, the search areas in question covered a federal courthouse, a church, legal offices, and a residential neighborhood — all sensitive areas whose patrons may have their own heightened privacy interests. Despite the efforts to limit the breadth of the searched individuals, there were over 100 people whose information was collected by Google and provided to the government for whom the government had no probable cause to search. As such the Court finds that the search warrants were overly broad and thus fatally flawed.

D. Good-Faith Exception

The exclusionary rule does not stem from an explicit Fourth Amendment remedy, but rather is a “prudential” doctrine. Pennsylvania Bd. of Probation and Parole v. Scott, 524 U.S. 357, 363, (1998). The

STATE OF MCGEE
DISTRICT COURT
14th Circuit

Supreme Court created the exclusionary rule to “compel respect for the constitutional guaranty.” Elkins v. United States, 364 U.S. 206, 217 (1960); see Weeks v. United States, 232 U.S. 383 (1914) Exclusion is “not a personal constitutional right,” nor is it designed to “redress the injury” occasioned by an unconstitutional search. Stone v. Powell, 428 U.S. 465, 486 (1976); see United States v. Janis, 428 U.S. 433, 454, n. 29 (1976).

“The rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations.... Our cases have thus limited the rule's operation to situations in which this purpose is thought most efficaciously served. Where suppression fails to yield appreciable deterrence, exclusion is clearly ... unwarranted.” Davis v. United States, 564 U.S. 229, 236–37 (2011) (internal citations and quotation marks omitted). “[C]ourts generally decline to hold a warrant facially deficient where the legality of an investigative technique is unclear, and law enforcement seeks advice from counsel before applying for the warrant.” United States v. McLamb, 880 F.3d 685, 691 (4th Cir. 2018). Further, “consultation [with Government attorneys prior to seeking a warrant] is a relevant consideration in determining whether the warrant was facially deficient.” United States v. Matthews, 12 F.4th 647, 657 (7th Cir. 2021).

In Chartrie, the Court found that the good-faith exception applied to its analysis for two primary reasons: (1) the applying officer was relying in good faith on prior similar warrants he had been granted, and on legal counsel; and (2) the novel legal complexities surrounding geofence warrants are such that police officers could not be expected to have meaningful familiarity with them. Chartrie, 590 F. Supp. 3d at 938. Chartrie was issued in 2022 and while there have been a number of cases clarifying constitutional issues around geofencing warrants since then, it is still an area of developing law.

The FBI Agents who submitted this search warrant did so in

STATE OF MCGEE
DISTRICT COURT
14th Circuit

reliance on prior geofencing warrants that they had been granted. While they did not seek the assistance of outside counsel, there is no indication they did not act in good faith based on prior search warrants that were granted, and in light of the limited authority about the veracity of geofence dragnet warrants. When officers rely on prior magistrates and legal counsel, there is no basis to believe that exclusion would deter similar behavior in the future. As such, despite the warrants being fatally deficient on grounds of over-breadth, this court must conclude that exclusion is not a justified remedy.

Conclusion

The Court finds that Defendant Nez had a reasonable expectation of privacy in her cell location data that implicated the Fourth Amendment. Moreover, the Court finds that the overbreadth of the geofence warrant granted in this manner violated the Fourth Amendment probable cause requirement. However, because there is no reason to believe that the actions of the FBI agents in this matter were in bad faith, this court declines to exclude the evidence obtained via the geofence warrants.

STATE OF MCGEE
DISTRICT COURT
14th Circuit

State of McGee,
Plaintiff

Criminal No. 24-CR-13-1312

vs.

**AFFIDAVIT IN SUPPORT OF SEARCH
WARRANT AND COURT ORDER FOR
PRODUCTION OF RECORDS**

Cheyenne Nez,
Defendant.

BEFORE THE HONORABLE MARGARET FITZPATRICK, JUDGE /
MAGISTRATE:

Affiant, Zebulon Miller, a commissioned law enforcement officer, being duly sworn, deposes and states that I have probable cause to believe that at the place or business entity known or described as:

**Google, LLC
Google Legal Investigations Support
1600 Amphitheatre Parkway
Mountain View, CA, 94043**

Service via Google's Law Enforcement Request System (LERS) on-line

Service may be via email at uslawenforcement@Google.com

STATE OF MCGEE
DISTRICT COURT
14th Circuit

There is now located within or upon said internet service/social media provider the following records, data, information, and technical assistance:

- All records or other information regarding the personal identification of the subject account, to include full name, date of birth, gender, other contact email addresses, physical address, telephone numbers, and any other personal identifiers;
- The date on which the account was created, the length of service, the IP address with associated Port ID(s) used to register the account;
- Any other Gmail addresses associated with the account(s) listed above along with all personal identifiers related to those Gmail accounts;
- All Google/Gmail accounts associated to the above account(s) by device or cookie: to include User ID, subscriber name, cell phone number and email address for such associated accounts;
- All devices(s) used and otherwise associated with the subscriber's account(s) – ESN, ICCID, IMSI, IMEI and MAC address numbers and activation dates;

The above information is being requested in reference to the following Google anonymity device(s):

ANDROID

18-015420-323751-01

54-015420-323751-31

22-015420-323751-44

17-015420-323751-72

STATE OF MCGEE
DISTRICT COURT
14th Circuit

IPHONE

3100001tuw444231266446465345756
3100001231tuddsw266446465345756
31000012312312312asd65345756
3100001231231231266446465345756
31000012312312312qweqweqwe5345756
3100001231231231266446465345756
3100001231231231266446465345756
31004ffyrhhsd1231266446465345756
3100001231231sssdd3126465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756

The above information is being requested during the following time period:

Between the dates of 1-13-2023 12 AM through 1-15-2023 12 AM

The above information is being requested for evidence of:

SIMPLE BATTERY
DISORDERLY CONDUCT
AGGRAVATED ASSAULT

For which a search warrant and court order for production of records may be issued upon one or more of the grounds set forth in 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1, §19-2-504, and Crim. P. 41, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a

STATE OF MCGEE
DISTRICT COURT
14th Circuit

means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state, or the seizure of which is expressly required, authorized or permitted by any statute of this state, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

The facts tending to establish the grounds for issuance of a Search Warrant are as follows:

BACKGROUND OF AFFIANT

Zebulon Miller has been a special investigator with the Federal Bureau of investigations for the last twelve years.

STATEMENT OF PROBABLE CAUSE USED TO OBTAIN GEOFENCE WARRANT:

On January 14, 2023, a group of agitators using the collective title of “Family Values” were agitating outside of the federal courthouse in Tulsa, McGee over a legal decision of the United States Attorney’s Office. At approximately 9:00 a.m., agitators began to gather armed with 2X2s attached to signs with anti-police slogans attached. The agitators set up wooden barricades to prevent courthouse staff from entering the building.

There were approximately 75 protesters who began yelling profane anti-police slogans at 11 am and when the police attempted to move them out of the pedestrian thoroughfare, they responded by throwing pigs blood mixed with saliva on peace officers and striking them with

STATE OF MCGEE
DISTRICT COURT
14th Circuit

the heavy posts attached to their signs. A pedestrian and four officers were struck by the signposts, and two officers were doused with the bodily fluids and pigs' blood.

After the assaults, several agitators fled the scene before they could be identified. During interviews with other subjects present, the FBI determined the conspirators met to plan the uprising the day before at a residential address. However, the subjects were reticent about disclosing the identity of any of the other agitators including Defendant subsequently identified as Cheyenne Nez.

On January 18, 2023, the undersigned affiant sought and was granted a geofencing warrant, attached to this application, for a three-hour window and 150-yard radius of the courthouse where the agitators were located to determine what cellular devices were in that area. At the same time officers sought a geofence warrant for 1423 17th Ave, Tulsa where the conspiracy developed. The warrant covered from 1300-1900 17th Avenue for a 150-yard radius of the home. After the warrant was granted, the undersigned affiant served the warrant on Google promptly.

On January 18, 2023, your affiant submitted the associated Search Warrant, which was signed by the Honorable Magistrate Margaret Fitzpatrick. The search warrant authorized your affiant to obtain Google device locations for 150-yards of Courthouse Square 1, on January 14, 2023, from 0900-1200 and for a 150-yard radius of 1423 17th Ave on January 13, 2023, from 1300-1900.

On April 5, 2023, your affiant received a response from Google, LLC. Your affiant examined the data. Google responded with anonymized information for 147 devices from the courthouse and 26 anonymized devices from 1423 17th Ave. Of those devices 18 devices were at both locations. This warrant is an application to obtain the user information associated with those 18 devices.

STATE OF MCGEE
DISTRICT COURT
14th Circuit

Based on my investigation, your affiant is requesting Google, LLC to provide me with subscriber information for the following devices:

The above information is being requested in reference to the following Google anonymity device(s):

ANDROID

18-015420-323751-01
54-015420-323751-31
22-015420-323751-44
17-015420-323751-72

IPHONE

3100001tuw444231266446465345756
3100001231tuddsw266446465345756
31000012312312312asd65345756
3100001231231231266446465345756
31000012312312312qweqweqwe5345756
3100001231231231266446465345756
3100001231231231266446465345756
31004ffyrhhsd1231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756
3100001231231231266446465345756

Your Affiant has reason to believe evidence pertaining to the subscriber data located in the above requested accounts will further the investigation and will potentially identify the persons who were at 1 Court Square on

STATE OF MCGEE
DISTRICT COURT
14th Circuit

January 14, 2023. This might identify suspect(s), co-conspirator(s), or witness(es), and tend to corroborate or refute statements of persons involved in this investigation.

Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. 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.

Google retains certain transactional information about the creation and use of each account on their systems. 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, email providers often have records of the IP addresses 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 email account.

STATE OF MCGEE
DISTRICT COURT
14th Circuit

This information may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling your affiant to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user’s Internet browser.

Based on these facts, Your Affiant believes there exists probable cause to believe that there is material evidence now located in the above described **Google, LLC** account that is crucial to the investigation of this case and the offenses described above, and a search warrant is requested pursuant to 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41.

Google, LLC is a provider of electronic communication services subject to the Stored Communication Act (SCA), 18 U.S.C. §2703, et seq. The SCA permits a state court with jurisdiction over an offense to issue an extraterritorial warrant for production of electronic communication content and electronic communication records. 18 U.S.C. §2703(g) authorizes service of the warrant via methods other than in-person service by a law enforcement officer. It is the intent of this affiant, consistent with the SCA and the procedures established by Google.com for compliance with the SCA, to serve this warrant via fax and/or email or law enforcement portal.

Further requests:

- 1) Pursuant to Crim. P. 41 and §16-3-304(2), Your Affiant requests that this Court seal the affidavit and search warrant and court order for production of records that has been filed with the Court in this matter. The affidavit establishes grounds to believe that disclosure

STATE OF MCGEE
DISTRICT COURT
14th Circuit

of the affidavit and search warrant and court order for record production would be contrary to the public interest. Such order for sealing does not apply to representatives of law enforcement agencies, and District Attorney's Offices, but those individuals are precluded from further dissemination prior to expiration of this order without an order of the Court handling the case.

- 2) So as not to disrupt this ongoing investigation, Your Affiant also requests that this Court order **Google, LLC** NOT to take adverse action against the subject account, such as disabling or terminating the account, because of this warrant.
- 3) Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), Your Affiant requests that **Google, LLC** be ordered NOT to disclose the existence of this search warrant and court order to the subscriber for a period of one year from receipt of the requested documents, unless otherwise ordered by a court of competent jurisdiction. Based on the information set forth in this affidavit, notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

I believe the above facts to be true from official Federal Bureau of Investigation records, conversations with fellow officers, personal observations, and interviews. I am a Special Investigator with the Federal Bureau of Investigation. I have been trained at the State and local levels regarding my duties. I am authorized by law to execute search warrants in any state of the United States.

_____*Zebulon Miller*_____
AFFIANT

STATE OF MCGEE
DISTRICT COURT
14th Circuit