IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF THE SEARCH OF INFORMATION THAT IS STORED AT THE PREMISES CONTROLLED BY GOOGLE, LLC	Case No. 21-MJ-5064-ADM

MEMORANDUM AND ORDER

This matter comes before the court on the United States' Application for a Warrant by Telephone or Other Electronic Means. The government seeks a geofence warrant directed to Google, LLC for location history data covering a defined area that surrounds and includes a building where a federal crime allegedly occurred. Applications for geofence warrants are becoming more commonplace and have drawn scrutiny because of the possibility that they will reveal the identities of potentially numerous individuals who happened to be in the vicinity when a crime was committed but who were not involved in and did not witness the crime. *See Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2511–12 (2021) (listing examples). "As a result, it is easy for a geofence warrant, if cast too broadly, to cross the threshold into unconstitutionality because of a lack of probable cause and particularity, and overbreadth concerns under Fourth Amendment jurisprudence." *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation ("Arson")*, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020).

The court issues this written order not only to address the subject application, but also to provide guidance for future search warrant applications involving geofence technology given the

relatively sparse authority on this issue. Here, the application and accompanying affidavit are not sufficiently specific or narrowly tailored to establish probable cause or particularity. The court therefore denies the application without prejudice.

I. GEOFENCE WARRANTS

The Fourth Amendment requires both probable cause and "particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. AMEND. IV; *Groh v. Ramirez*, 540 U.S. 551, 557 (2004).[1] Its basic purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). Fewer than a handful of cases have addressed the Fourth Amendment's limitations on geofence warrants. Three from the Northern District of Illinois provide helpful guidance.

In *Matter of Search of Information Stored at Premises Controlled by Google ("Pharma I" and "Pharma II")*, two different judges denied the government's original and subsequent applications for a geofence warrant that encompassed two physical locations that an unknown suspect had entered to steal and ship stolen pharmaceuticals. No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020) (denying the first application); 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020) (denying the third application). Both judges were troubled by (among other things) the proposed geographic boundaries of the geofences, which encompassed two physical locations within a busy commercial and residential area on major arterial streets in a major metropolitan area. In *Pharma I*, the court found the geographic scope of the geofence warrant was not

[1] *Arson* contains a helpful and comprehensive discussion of various issues regarding geofence warrants and Fourth Amendment jurisprudence. *See* 497 F. Supp. 3d 345. The court provides only a brief discussion of the case because of the time-sensitive nature of the warrant application that is now before the court.

narrowly tailored in that "the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation." *Pharma I*, 2020 WL 5491763, at *5. Likewise, in *Pharma II*, the court pointed out that the geofence would have captured not only the pertinent business establishments but also the residential units above those business establishments and neighboring sidewalks, streets (including one "busy arterial street"), and a parking lot that served other retail businesses. 481 F. Supp. 3d at 752.

In contrast, the court in *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation ("Arson")* issued a geofence warrant based on a more robust showing of probable cause and particularity. 497 F. Supp. 3d 345. In *Arson*, the government sought geofence data concerning six target locations connected with an arson investigation. *Id.* at 351-352. The government had established probable cause that the crimes were committed by coconspirators, and it was "reasonable to infer that suspects coordinating multiple arsons across the city in the middle of the night, as well as any passersby witnesses, would have cell phones." *Id.* at 354-55. Furthermore, the government had "structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses." *Id.* at 353.

Fundamentally, the difference between the *Pharma* cases and the *Arson* case is that the government's proposed geofence warrant application in *Arson* (1) established probable cause to believe that the results of the warrant would reveal the identities of suspects or witnesses, and (2) was sufficiently particular in time, location, and scope. *Id.*

II. THE APPLICATION BEFORE THE COURT

Because this case concerns on ongoing criminal investigation, the court will not describe in detail the circumstances of the alleged crime other than to say that the affidavit has sufficiently established probable cause to believe that a federal crime occurred at a particular location on a particular date. The application seeks geofence data from an area surrounding the alleged crime location, which is a sizeable business establishment, during a one-hour period on the relevant date. But, unlike in *Arson*, the application and affidavit leave too many questions unanswered for the court to find that the application is supported by probable cause or that the proposed warrant is sufficiently particular in time, location, and scope.

A. Probable Cause

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); *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983) (same). Whether probable cause exists is a "flexible, common-sense standard," and no single factor or factors is determinative. *Illinois*, 462 U.S. at 239. In examining whether the government has established probable cause, the court must determine whether there is probable cause that a crime has been committed and that evidence of the crime will be located at the place to be searched. *Id*. at 238. In the context of a geofence warrant application, "[t]he government's affidavit must provide sufficient information on how and why cell phones may contain evidence of the crime, as well as credible information based on the agent's training and experience, to support the assertions." *Arson*, 497 F. Supp. 3d at 356.

The application here establishes probable cause that a crime was committed at the subject business establishment during the relevant one-hour time period. However, it does not establish

probable cause that evidence of the crime will be located at the place searched—that is, Google's records showing the location data of cell phone users within the geofence boundaries. To be clear, Google's location data would undoubtedly show that "a certain device was located at a particular place at a particular point in time." *Pharma II*, 481 F. Supp. at 734. However, the application in *Pharma II* provided a more meaningful explanation as to how GPS/location data feeds into Google's location data. The affidavit explained that Google collects location information via its Android operating system and Google accounts and, even as to non-Android devices (like iPhones), when a user enables location sharing. *Id.* The application stated that Google Android phones account for approximately 74% of the smartphone market whereas Apple phones are about 23%, and it gave specific examples of well-known applications (like Gmail, Google Maps, Google Chrome, and YouTube) by which even Apple devices communicate location information to Google. *Id.* at fn.1. Furthermore, "[p]ublished reports have indicated that many Google services on Android and Apple devices store the device users' location data even if the users seek to opt out of being tracked by activating a privacy setting that says it will prevent Google from storing the location data." *Id.* at fn.3. The record therefore established that it would be a "relatively rare" device that would not transmit that device user's location information to Google. *Id.* at 734.

Similarly, the affidavit in *Arson* explained how Google collects location information, including via Google apps that run on non-Android operating systems, like iPhones. 497 F. Supp. 3d at 350. The affidavit provided no evidence that any of the suspects possessed cell phones or used cell phones to commit the offenses, or that they used Google applications or operating systems that would store location data, but the court relied on the agent's training and experience to establish probable cause. *Id.* at 355. The agent's affidavit explained that: (1) it is

common for criminal coconspirators to use cell phones to plan and commit criminal offenses, particularly where, as there, they targeted two different locations on two different dates; (2) "there was a reasonable probability that a cell phone, regardless of its make, is interfacing in some manner with a Google application, service, or platform"; and (3) given the agent's familiarity with the investigation so far, he "believed that anyone passing near or through the target locations during those locations' time parameters could be perpetrators or witnesses to the arsons." *Id.* at 356. From this, the court concluded that "there is a fair probability that location data at Google will contain evidence of the arson crime, namely the identities of perpetrators and witnesses to the crime." *Id.*

The court has considered the agent's statements in the current application based on his training and experience, and finds that they are too vague and generic to establish a fair probability—or any probability—that the identity of the perpetrator or witnesses would be encompassed within the search. For beginners, the affidavit does not suggest that any relevant perpetrator or witness even had a smartphone. In *Arson*, the court relied on an affidavit that explained that that coconspirators probably would have been coordinating their efforts by phone. Here, the affidavit contains no analogous explanation, whether based on the agent's training and experience or based on the facts of the investigation. To the contrary, the affidavit suggests only that the culprit was a lone pedestrian in the early morning hours who was caught on surveillance footage. The affidavit conspicuously omits any suggestion that the surveillance footage shows that the individual had a cell phone.

Even if the court were to assume that most people (including those engaged in criminal activity) possess and use cell phones, the affidavit also does not establish a fair probability that any pertinent individual would have been using a device that feeds into Google's location-

tracking technology. The affidavit states that 85% of the United States' population owns a smartphone; that the two primary operating systems on those smartphones are Android or iOS; that Google provides 68 different applications that can be run on either operating system; that some of those apps will not function properly without access to the device's location; and that "Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services." (Aff. ¶¶ 13, 19-20.) This bears no resemblance to the more detailed explanations provided by the affiants in *Pharma II* or *Arson* explaining how most smartphones, whether Android or iOS, would be sharing location data with Google upon which the court could find at least a fair probability that any such device would be feeding into Google's location data.

The application also does not address the anticipated number of individuals likely to be encompassed within the targeted Google location data. This also goes to the particularity requirement, which is intertwined with probable cause. If a geofence warrant is likely to return a large amount of data from individuals having nothing to do with the alleged criminal activity—as in *Pharma I & II*—the sheer amount of information lessens the likelihood that the data would reveal a criminal suspect's identity, thereby weakening the showing of probable cause.

B. Particularity

The Fourth Amendment's particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84, (1987). The particularity requirement is more stringent if the privacy interest is greater. *See Berger v. New York*, 388 U.S. 41, 56 (1967). The *Arson* court found that the particularity

requirement for a geofence warrant is satisfied if narrowly identifies the place to be searched by time and location so that it is not overbroad in scope. *Arson*, 497 F. Supp. 3d at 357.

The court cannot make the same finding here because the application is missing key information to determine whether the proposed warrant is sufficiently particularized. For one, the geofence boundary appears to potentially include the data for cell phone users having nothing to do with the alleged criminal activity. The boundary encompasses two public streets, so anyone driving their automobile by the target location during the relevant time period could be identified in the data. Google Maps also indicates that the subject building contains another business, which the application does not address. The government is also seeking data within the geofence's "margin of error," meaning that it seeks location-point data outside of the geofence but which could conceivably fall within the geofence if the margin of error would permit the device to be located within the parameters. *See Pharma II*, 481 F. Supp. 3d at 745 n.11 (describing the margin of error). As a result, the warrant may return data from users who are outside of the radius of the geofence. *Id.* Google Maps shows that the area just outside of the perimeter of the geofence includes residences and other businesses that could be implicated by the margin of error. But the application does not explain the extent to which the geofence, combined with the margin of error, is likely to capture uninvolved individuals from those surrounding properties. This stands in stark contrast to the affidavit in *Arson*, where the government identified and explained the surrounding commercial and residential buildings that the margin of error might include outside of the target locations. 497 F. Supp. 3d at 360.

The application also does not adequately justify the time period requested. It seeks an hour of data, which is longer than what was at issue in either *Pharma I & II or Arson*. And the nexus between the alleged criminal activity and this one-hour duration is weak. According to the

affidavit, video surveillance footage shows the suspect at three discrete times. The proposed geofence's temporal scope ranges from just before the second sighting to approximately 10 minutes after the suspect fled the scene. The affidavit does not explain why the government does not seek data from the time period surrounding the first sighting, and it does not explain why the government seeks data for the entire period between the second and third sighting. There could be a reasonable explanation for this. But that explanation is not included in the affidavit, and therefore the court cannot conclude that the proposed geofence warrant is sufficiently particular.

III. CONCLUSION

For the reasons explained above, the court denies the application without prejudice. The court does not foreclose the possibility that the government may be able to adequately demonstrate probable cause to support the warrant and articulate that the proposed geofence is sufficiently particular. There could be good reasons why the government seeks to capture activity from the surrounding area or why it seeks an hour of data while omitting any data associated with the first sighting of the suspect. The government may also be able to lessen concerns that the geofence warrant would return location data for passersby on nearby streets or within the margin of error but who have nothing to do with the alleged criminal activity. The government should adequately account for this in any renewed application, or perhaps redraw the parameters of the requested warrant. The court simply issues this opinion to provide fair notice that geofence warrant applications must sufficiently address the breadth of the proposed geofence and how it relates to the investigation. It is not enough to submit an affidavit stating that probable cause exists for a geofence warrant because, given broad cell phone usage, it is likely the criminal suspect had a cell phone. If this were the standard, a geofence warrant could issue in almost any criminal investigation where a suspect is unidentified. The Fourth

Amendment requires more, particularly where the warrant implicates the privacy interests of individuals who have nothing to do with the alleged criminal activity.

IT IS THEREFORE ORDERED that the government's application for a geofence warrant is denied without prejudice.

IT IS FURTHER ORDERED that this order shall remain sealed until **June 11, 2021**, at which time the court will direct the clerk's office to unseal the order. The government may move to have this order maintained under seal for a longer period, but any such motion must be filed in advance of the above date.

IT IS SO ORDERED.

Dated June 4, 2021, at Topeka, Kansas.

s/ Angel D. Mitchell
Angel D. Mitchell
U.S. Magistrate Judge