IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In the Matter of the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation	20 M 525 Magistrate Judge Sunil R. Harjani

MEMORANDUM OPINION & ORDER

The government has presented an application for a warrant for location data, also known as geofence data, that is stored at the premises of Google. Once novel, applications for warrants for geofence data are now more frequent in criminal investigations, but have also come under scrutiny, resulting in two recent opinions in this district about the scope of these warrants and their permissibility under the Fourth Amendment to the United States Constitution.[1] In this particular case, the Court finds that the government's application for location data within six geofence areas relating to an arson investigation satisfies the probable cause and particularity requirements of the Fourth Amendment. The Court issues this opinion to explain the reasons why it has authorized the warrant and contribute to the continuing discussion about the constitutionality of geofence warrants.

[1] *Matter of Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020) (Weisman, J.) (Google I); *Matter of Search of Info. Stored at Premises Controlled by Google*, No. 20 M 392, 2020 WL 4931052, at *18 (N.D. Ill. Aug. 24, 2020) (Fuentes, J.) ("*Google II*").

Background

In order to fully examine the issues involved in this geofence warrant application, it is necessary to recount the technology at issue, the way it operates, and the nature of the government's request for the information. [2]

I. Cell Phones and Location Data

Cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. Warrant Aff. ¶ 7. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called "cell sites," which can be mounted on towers, buildings, or other infrastructure. *Id.* Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. *Id.* As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point. *Id.*

Cellular devices such as mobile telephones have the capability to connect to wireless Internet (Wi-Fi) access points if a user enables Wi-Fi connectivity. *Id* ¶ 8. Wi-Fi access points, such as those created through the use of a router and offered in places such as 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. *Id.* Many cellular devices also feature Bluetooth functionality. *Id.* ¶9. Bluetooth allows for short-range wireless connections between

[2] The facts of this case are detailed in the Application and Affidavit for a Search Warrant ("Warrant Aff."), which remains under seal. As a result, the Court has only generally described the crime and its suspects.

devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect. *Id.*

Many cellular devices, such as mobile telephones, include global positioning system (GPS) technology. Using this technology, the phone can determine its precise geographical coordinates. *Id.* ¶ 10. If permitted by the user, this information is often used by applications (apps) installed on a device as part of the its operation. Google is a company that, among other things, offers an operating system (OS) for mobile devices, including cellular phones, known as Android. Nearly every cellular phone 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. *Id.* ¶ 11. Google also offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google), online file storage (including Google Drive, Google Photos, and Youtube), messaging (Google Hangouts), and video calling (Google Duo). *Id.* ¶ 12. Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. *Id.* An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and YouTube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account. *Id.*

Google also offers an Internet browser known as Chrome that can be used on both computers and mobile devices. *Id.* ¶ 13. 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

synced across the various devices on which they 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. *Id.* 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, phones that do not run the Android operating system, such as Apple devices. *Id.* ¶ 14.

II. Google Geofence Data

When a Google user opts in to a service known as "Location History," that user can keep track of locations visited while in possession of the mobile device. *Id.* ¶¶ 15, 17. Like a journal or log, Google Location History Information enables a user to record where she has traveled with her phone and when, and the Google User has the ability to review or delete Location History information at will. *Id.* ¶ 15. If the Google user takes additional steps, including enabling a "Location Reporting" feature for at least one mobile device, the resulting data is transmitted to Google for processing and storage on Google's servers. *Id.* ¶ 17. When activated in such a way, Google can calculate the device's estimated latitude and longitude using inputs from (1) nearby cell sites, (2) GPS signals, and (3) signals from nearby Wi-Fi networks and Bluetooth devices. *Id.* ¶ 16. 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 "map's display radius," for each latitude and longitude point. *Id.* Google also retains subscriber information associated with a user's account, which can include the subscriber's full name, address, telephone number, and other identifiers. Id. ¶ 19. Thus, a "geofence warrant" provides the government the ability to obtain location data for a Google user for a particular area and, eventually, subscriber information for the account holder using Google-

based devices or applications in that area.

III. The Arson Investigation

In this case, the government seeks geofence data in connection with an arson investigation. Warrant Aff. ¶ 21. In 2019, there was a series of approximately 10 arsons in the Chicago area, which appeared to target specific commercial lots. *Id.* In most of the arsons, incendiary fires burned vehicles in the lots. *Id.* Two companies had vehicles in their lots burned twice. *Id.* Two vehicles (Subject Vehicles A and B) are both seen on surveillance camera footage at Target Location 1 and 3 and are suspected of carrying the perpetrators of the arsons. Id. ¶ 76. As further discussed below, various surveillance and investigative techniques led law enforcement to believe that the fires were connected and that geofence data for six "target locations," will contain evidence pertaining to the identity of the arson suspects and their co-conspirators. *Id.* ¶¶ 96-101.

A. Target Location 1

The government represents that Target Location 1 is Company A's commercial lot. Warrant Aff. ¶ 22. To illustrate the physical zone, the government provides a satellite map of Target Location 1 and the surrounding area with a bold yellow outline identifying the boundaries of Target Location 1. *Id.* The yellow triangle representing Target Location 1 appears to be about a quarter to a third of the size of the block that Target Location 1 is located in. *Id.* At each point of the triangle, there is additionally a red dot with a number, which corresponds to particular coordinates specified by the government in an attachment to the warrant. *Id.* ¶ 22 n.1. Within Target Location 1, in addition to Company A's lot space, there is an event hall and garage. *Id.* ¶¶ 25, 26. At the time of the arson, there was additionally a trailer Company A was using for office space. *Id.* ¶ 27. Outside of Target Location 1 and bordering it is an alley on the East side, and a combination of empty lots and commercial buildings on the West. *Id.* To the general North and

South of Target Location 1 are streets. *Id.* ¶ 22. The request for geofence data for Target Location 1 is limited in time. Specifically, the Government requests a time parameter for the 24-minute period in July 2019 starting at 2:00 a.m., during which time the government approximates the first arson was committed at Company A's commercial lot. *Id.*

B. Target Location 2

Target Location 2 is an area of roadway in which the individuals believed to be involved in the arsons at Target Location 1 and Target Location 3, drove through. Warrant Aff. ¶ 33. The satellite map for Target Location 2 includes a bold yellow outline of an "L" shape, which includes a portion of the alley that bordered Target Location 1 on the East. *Id.* Each segment of the "L" is approximately half the length of a city block. *Id.* The yellow outline for Target Location 2 includes the red points corresponding to specific coordinates. *Id.* Within Target Location 2, there is a street, alley, and grass or landscaping bordering the street or alley. *Id.* ¶ 35. Outside the area of Target Location 2, there are yards of residences, a commercial building, and residential garages. *Id.* ¶¶ 34, 42-44. The time parameter is for a 17-minute window within the 24-minute period of the first arson at Company A's commercial lot. *Id.* ¶ 33.

C. Target Location 3

Target Location 3 comprises Company B's commercial lot, in which another arson was committed on the same date as the as the arson committed at Target Location 1. Warrant Aff. ¶ 45. The satellite map for Target Location 3 includes a bold yellow outline, this time in the shape of a square *Id.* Like the other yellow-outlined zones, the shape has four red points corresponding to specific location coordinates. *Id.* Target Location 3 appears to be about the size of half of a block. *Id.* Within the interior of Target Location 3, there is the lot space, a two-story mixed use building, and two garages. *Id.* ¶¶ 48, 49. Outside of Target Location 3 is a street to the North, an

alley to the South, a two-story mixed building and garage and storage structures to the East, and a one-story building to the West. *Id.* ¶¶ 50-55. The time parameter for Target Location 3 is a 15-minute window subsequent to the time allocation for Target Location 1, during which time, the government estimates the first arson at Company B's lot was committed. *Id.* ¶ 45.

D. Target Location 4

Target Location 4 is a roadway area near Target Location 3 where the government believes the arsonists drove through around the time of the first arson at Company B's lot. Warrant Aff. ¶ 56. The yellow-outlined shape in the satellite map for Target Location 4 is a long, horizontal rectangle running East/West with four red coordinate points, and is approximately the length of 1.25 city blocks. *Id.* Target Location 4 only consists of street and sidewalk bordering the street. *Id.* ¶ 59. Outside of Target Location 4, to the North and South of the roadway, there are several buildings, including two-story mixed use buildings, an event hall, a garage, and a church. *Id.* ¶ 58. The time parameter for Target Location 4 is a sixteen-minute period that overlaps with the time parameter for Target Location 3. *Id.* ¶ 56.

E. Target Location 5

Target Location 5 matches the geographic area of Target Location 1 but contains a different time parameter correlating with the second arson committed at Company A's commercial lot in December 2019. Warrant Aff. ¶ 71. So while the physical zone of Target Location 5 is exactly the same as Target Location 1, the time parameter is for a 37-minute period starting at 12:00 a.m. occurring months later. *Id.*

F. Target Location 6

Similarly, Target Location 6 comprises the identical physical space as Target Location 3 and has a time parameter approximating the second arson committed at Company B's commercial

lot. Warrant Aff. ¶ 72. Specifically, the time parameter is for the half hour directly prior to the time parameter of Target Location 5, with a minute of overlap. *Id.* ¶¶ 71, 72.

G. The Two-Step Process

The government's warrant contemplates that Google will disclose its geofence data in two steps. Warrant Aff. ¶ 102. In the first step, Google will provide the government with anonymized lists of devices with corresponding device IDs, timestamps, location coordinates, margins of error, and data sources for the devices that Google calculates were or could have been (*i.e* the margin of error) within each target location during the time periods described. *Id.* In the second step, the government, at its discretion, will identify to Google the devices from the anonymized lists for which the government seeks the Google account identifier and subscriber information. *Id.* Google will then disclose to the government that information. *Id.*

Discussion

The issue presented here concerns the scope of law enforcement's ability to seize geofence location data from Google in its search for criminal suspects under the Fourth Amendment's search and seizure clause. Courts have expressed concern about requests for geofence data that sweep too broadly and capture vast amounts of location data on uninvolved individuals. For example, geofence zones can be drawn, at the government's discretion, to include large swaths of land and buildings, including office and apartment buildings, shopping malls, churches, and residential neighborhoods, which could result in revealing location data of hundreds, if not thousands, of individuals that are uninvolved in the underlying crime. This is because the nature of a geofence warrant does not target an individual, but rather an area that captures location data for cell phones within that area. 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.

However, when considering this issue, it is also important to recognize that the Fourth Amendment does not deal in precision, but rather in probability. That is, the government must demonstrate a fair probability that evidence of a crime will be located at a particular place, and a search warrant need not be rooted in pinpoint accuracy. In this particular case, the government has 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. Indeed, in this case, there is a fair probability that almost all location data retrieved will be for individuals who are either the perpetrators, co-conspirators, or witnesses to the crime. Thus, the warrant application for the six geofence locations in this case is supported by *probable cause* and is particular in *time, location, and scope*. The Court evaluates each of these issues below.

I. Probable cause

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," except "upon probable cause." U.S. Const. amend. IV; *Missouri v. McNeely*, 569 U.S. 141, 148 (2013). Probable cause is a "practical, nontechnical conception" based on "common-sense conclusions about human behavior[.]" *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (internal quotation marks and citations omitted). "[A]s the very name implies," probable cause "deal[s] with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Id.* (internal quotation marks and citations omitted). The ultimate touchstone of the Fourth Amendment is reasonableness. *Riley v. California*, 573 U.S. 373, 381 (2014).

Put simply, probable cause is a fair probability that contraband or evidence of a crime will

be found in a particular place, based on the totality of the circumstances. *Gates*, 462 U.S. at 238. Probable cause thus requires "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.; see also Florida v. Harris*, 568 U.S. 237, 243 (2013). In examining an application for a warrant, the Court must therefore inquire as to whether probable cause exists that a crime has been committed, and that evidence of the crime will be located at the place to be searched. *Gates*, 462 U.S. at 238; *United States v. Hall*, 142 F.3d 988, 995 (7th Cir. 1998).

Here, there is ample probable cause that the crimes of arson and conspiracy to commit arson have occurred. Specifically, the Chicago Fire Department (CFD) has determined that on a specific date in July 2019, a commercial lot had multiple cars set on fire in the early hours of the morning. Warrant Aff. ¶¶ 74, 75. CFD's investigation concluded that the cars were ignited as a result of an open flame set to the vapors of a flammable liquid poured on vehicles. *Id.* Two white plastic lighter fluid containers were recovered by CFD. *Id.* ¶ 74. Similarly, CFD determined that a second commercial location was the subject of an arson, near the same timeframe, when six vehicles were ignited in a similar manner. *Id.* ¶ 75. In that case, bottles of gas-line antifreeze and water remover containing methly alcohol, which is an ignitable liquid, were recovered at the scene. *Id.* Furthermore, from street camera footage, two vehicles (Subject Vehicles A and B) were seen circling the area of the first arson location near the time of its occurrence, and then the same two vehicles were seen headed towards the second location of the arson. *Id.* ¶ 76-91. One of the vehicles had a red object that, according to the affiant, appears consistent with the size and shape of a gasoline container. *Id.* ¶¶ 84, 88. These two vehicles were then identified at the second arson

location. *Id.* ¶ 92. The vehicles also appear on camera to be following each other. *Id.* ¶ 84. Remarkably, those two locations were again subject to additional fires, using almost identical methods described above, in December 2019. *Id.* ¶¶ 93, 94.

The above provides sufficient evidence that there is probable cause that the crimes of arson and conspiracy to commit arson occurred. Title 18, United States Code, Section 844(i) makes it a crime to: "maliciously damage[] or destroy[], or attempt[] to damage or destroy, by means of fire or an explosive, any building, vehicle, or other real or personal property used in interstate or foreign commerce[.]" The federal conspiracy statute, Title 18, United States Code, Section 371, states it is an offense: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy[.]" As the facts supplied by the affidavit demonstrate, there is a fair probability that the fire was set maliciously, *i.e.* intentionally, by multiple persons in coordination, on vehicles that are stored in commercial businesses on multiple dates.

There is also probable cause that evidence of the crime will be located at Google because location data on cell phones at the scene of the arson, as well as the surrounding streets, can provide evidence on the identity of the perpetrators and witnesses to the crime. Warrant Aff. ¶¶ 95-101. Once the location data is produced and reviewed, the government can obtain subscriber information on those cell phones, which will reveal the identifiers of the potential culprits and witnesses to the events. *Id.* ¶ 103. In this case, it is important to note that there is no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense. Nor is there any additional evidence that perpetrators or witnesses of the crime used Google applications or operating systems that would store location data. Nevertheless, courts

have recognized that an agent's training and experience can provide information necessary to help establish probable cause in an affidavit. *See United States v. Zamudio*, 909 F.3d 172, 176 (7th Cir. 2018) (agent's statement that drug traffickers generally store drug-related paraphernalia, records, and currency at their residences, based on his training and experience, permitted search of the residence).

Under that principle, courts have authorized searches and seizures of cell phones based on statements made about their use in crime grounded in the agent's training and experience. *See United States v. Beckley*, No. 15-20127, 2016 WL 5791455, *3 (E.D. Mich. October 4, 2016) (internal quotation marks omitted) (agent's training and experience that criminals use cell phones to "plan crimes in advance, communicate with accomplices before, during, and after the crime, and to coordinate an alibi," along with the agent's belief that the cell phone records would pinpoint the perpetrator's location during the robbery was sufficient to support warrant for phone records); *United States v. Mompie*, 216 F. Supp. 3d 944 (S.D. Ind. 2016) (agent's statement about the use of cell phones in crimes supported issuance of search warrant for cell phones); *United States v. Gholston*, 993 F. Supp. 2d 704 (E.D. Mich. 2014) (agent's affidavit established probable cause to support search of defendant's cell phone where investigation showed defendant was one of two participants involved in robbery and agent's cited training and experience indicated the cell phone could contain evidence of the robbers' identities and their possible pre-planning and coordination of criminal activity).

Moreover, probable cause does not require conclusive evidence that links a particular place or item to a crime. *United States v. Anderson*, 450 F.3d 294, 303 (7th Cir. 2006) (citation omitted). "Rather, issuing judges may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the offense." *United States v. Zamudio*, 909 F.3d 172, 175

(7th Cir. 2018), cert. denied, 140 S. Ct. 108, 205 L. Ed. 2d 25 (2019) (citations omitted). In other words, "[t]he Fourth Amendment does not require certainty that a search will uncover the sought-after evidence; a fair probability is enough." *United States v. Aljabari*, 626 F.3d 940, 946 n. 1 (7th Cir. 2010). The nature of the crime, and the means by which it was committed, allow courts to make reasonable inferences about where evidence may be found. Finally, the ubiquity of cell phones and their common usage was aptly described by the Supreme Court in *Riley v. California* and *Carpenter v. United States*. *See Carpenter v. United States*, 138 S. Ct. 2206, 2211 (2018); *Riley v. California*, 573 U.S. 373, 395 (2014). Unlike virtually any other item, it is rare to search an individual in the modern age during the commission of a crime and not find a cell phone on the person. Thus, it is 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.

This is not to say that cell phones, and subsequently location data, can be automatically searched with respect to every federal crime imaginable. The 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. Here, the affidavit provided several statements supporting probable cause that evidence of the crime would be located at Google. The affiant, who is a 19-year veteran of the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), averred that it is common for criminal coconspirators to use cell phones to plan and commit criminal offenses. Warrant Aff. ¶ 97. The agent stated that the latter is "particularly true where, as here, there appears to be two different locations that were targeted on two different dates." *Id.* The agent further stated that, based upon training and experience, 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. *Id.* ¶ 98. The agent

surmised that the coconspirators could have used their cell phones to communicate with each other and may have used other applications to facilitate the crime, such as a GPS maps application. *Id.* ¶ 99. Finally, in light of the agent's review of traffic videos, law enforcement's interviews of witnesses, the agent's observations of the arson scenes, the agent's training and experience, as well as the investigation and training and experience of the other law enforcement agents, the agent believed that anyone passing near or through the target locations during those locations' time parameters could be perpetrators or witnesses to the arsons. *Id.* ¶ 100. As a result, the agent concluded that the identities of the perpetrators and witnesses may be located within the possession of Google. *Id.* The Court finds that the affidavit, when considering the totality of the circumstances and the agent's training and experience, allows the Court to conclude 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.

II. Particularity and Overbreadth

The Fourth Amendment requires that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The 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); *see also Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."). While warrants "must describe the objects of the search with 'reasonable specificity,' the Constitution does not insist that they be 'elaborately detailed.'" *Archer v. Chisholm*, 870 F.3d 603, 616 (7th Cir. 2017). Importantly, particularity turns on what is realistic

or possible for the investigation at hand. *Id.* "When granular detail is impossible, generic descriptions of the items to be seized are sufficient so long as they particularize the types of items to be seized." *Id.* (citation omitted). "[E]xact precision in a search warrant's description" is not required. *United States v. Kelly*, 772 F.3d 1072, 1081 (7th Cir. 2014).

The Court finds that the warrant in this case particularly describes the place to be searched because it narrowly identifies the place by time and location and is also not overbroad in scope.

First, the warrant is limited in time – the government has identified an approximately 15-30 minute time frame for each target location where it believes location data will reveal evidence of the crime. For instance, the time parameters for Target Locations 1 and 2 correlate to the approximate time surrounding the July 2019 arson at Company A's commercial lot, which the government's investigation has narrowed to a 24-minute period. Warrant Aff. ¶¶ 22, 33. The time parameters for Target Locations 3 and 4 likewise connect to the approximate time surrounding the July 2019 arson at Company B's commercial lot, for which the investigation has identified a 15-minute period. *Id.* ¶¶ 45, 56. Target Location 5's time parameter relates to the 37-minute approximate time surrounding the December 2019 arson committed at Company A's commercial lot. *Id.* ¶ 71. Target Location 6's time parameter is for the 31-minute approximate time associated with the December 2019 arson committed at Company B's commercial lot. *Id.* ¶ 72. These approximate timeframes of the arsons are based on the government's investigation. Thus, the warrant does not seek location data for days or even hours to track the whereabouts of the perpetrators, but rather location data that is tailored and specific to the time of the arson incidents only.

Second, the warrant is limited in its location. The target locations have been narrowly crafted to ensure that location data, with a fair probability, will capture evidence of the crime only.

Target Location 1 is Company A's commercial lot that was the subject of the first July 2019 arson. Warrant Aff. ¶ 22. Within Target Location 1 is the lot where cars are stored, a garage that is used by the business and its owner, a trailer used by the business, and an alumni event space for a high school in the area. *Id.* ¶¶ 24, 25-27. Target Location 3 is the location of the second arson that same morning, the second company's commercial lot, and includes the commercial lot where the cars were parked, two garages, and one mixed-use building that may contain a residence at the top floor. *Id.* ¶¶ 45-49. Target Locations 2 and 4 are only the streets leading to and from the commercial lots where the arsons were committed. *Id.* ¶¶ 33, 56. Target Location 2 comprises an "L" shape of roadway, with each segment of the "L" being approximately the length of half a city block. *Id.* ¶ 33. Target Location 4 consists of a segment of roadway running East/West, and is approximately the length of 1.25 city blocks. *Id.* ¶ 56. Target Location 5 is the first company's commercial lot, and Target Location 6 is the second company's commercial lot, with the same physical boundaries as Target Locations 1 and 3, but this time for the time periods concerning the second arsons at these locations in December 2019. *Id.* ¶¶ 71, 72. Each of these target locations is drawn to capture location data from locations at or closely associated with the arson. In each of these locations, there is a fair probability that the location data of perpetrators, co-conspirators and witnesses to the incidents will be uncovered. More specifically, because of the visible nature of the crime, namely arson, it is likely that individuals that happen to be in the commercial lot at that hour or on the street would have information about the crime. For example, an individual in the residence at Target Location 3 may have seen suspicious activity and may be able to describe the physical characteristics of the perpetrators in the lot, the vehicles driven by the perpetrators, or may even have information about how and where the fire started. Similarly, individuals not involved in the crime driving on the streets at approximately 2:30 a.m. in the morning (the

approximate time of the first two arsons) or 12:00 a.m. (the approximate time of the second two arsons), may provide information about the vehicles driving to and from the incident. *Id.* ¶¶ 22, 45. Finally, as stated above, the government has identified two vehicles, Subject Vehicles A and B, as the vehicles of the potential arsonists. *Id.* ¶¶ 76-92. Location data at the location of the arsons (Target Locations 1, 3, 5, and 6), as well as streets that lead to and from the arson sites (Target Locations 2 and 4), may help identify these individuals, once their subscriber information is obtained, and can either inculpate or exculpate those individuals.

Third, the warrant request is also limited in scope. One of the concerns that has been expressed about geofence warrants is their potential to capture vast swaths of location data of individuals not connected to the crime. *See Google I*, 2020 WL 5491763; *Google II*, 2020 WL 4931052. Here, the scope of the warrant has been sufficiently narrowed by its construction and through the agent's investigation. As discussed above, the geofence zones have been constructed to focus on the arson sites and the streets leading to and from those sites. Residences and commercial buildings along the streets have been excluded from the geofence zones. The approximate time of the crimes also limits the warrant's scope – the crimes occurred in the early hours of the morning when commercial businesses are usually closed and unoccupied. Streets in the wee hours of the morning in the City of Chicago are generally sparsely populated by pedestrians, and roads have few cars traversing through them. Furthermore, the affiant has provided additional information obtained through the investigation to support the conclusion that location data from uninvolved individuals will be minimized. For Target Location 1, the affiant stated that law enforcement agents interviewed the owner of the lot during the investigation, and the owner also owns the garage and the trailer on the property. Warrant Aff. ¶¶ 26-27. The owner, of course, is clearly an individual connected to the crime as the potential victim. The remaining

building, through investigation, was determined to be a high school event space, which is highly unlikely to be occupied between midnight and 3:00 a.m. *Id.* ¶ 25. Target Location 2 consists of street, alley, and landscaping. *Id.* ¶ 35. A Police Observation Device ("POD") camera is located near Target Location 2, and, according to the affiant, has captured images for certain portions of Target Location 2 during the relevant timeframe. *Id.* ¶¶ 36-41. According to the affiant, the POD camera captured only three other vehicles, other than the Subject Vehicles, driving on those streets. *Id.* ¶ 40. One appears to be a tow truck, one a fire truck responding to the fire, and the other is not identified. *Id.* The POD camera also showed no pedestrians walking through the portions of Target Location 2 filmed by the POD camera. *Id.* ¶ 41. Target Location 3 consists of the second company's commercial lot and includes two garages and one mixed-use building. *Id.* ¶¶ 45-49. According to the affiant, the upper floor of the mixed-use building may contain a three-bedroom apartment, per Cook County property records. *Id.* ¶ 48. However, during the investigation on the date of the arson in July 2019, the affiant attempted to make contact with any individual in the mixed-use building and was unable to find anyone. *Id.* In addition, the affiant remained on the scene for several hours and did not observe anyone enter or leave the building, leading to a reasonable conclusion that the premises was unoccupied at the approximate time of the arson. Target Location 4 is a street on the route between the first and second companies' commercial lots. *Id.* ¶ 56. Target Location 4 consists only of the street and sidewalk, and a POD camera nearby captured four minutes of video during the relevant timeframe that revealed only three vehicles, other than the Subject Vehicles, and no foot traffic. *Id.* ¶¶ 59-62. Target Locations 5 and 6 are the same geographic areas as Target Locations 1 and 3. *Id.* ¶¶ 71, 72. Thus, through on-site investigation, open source searches, and surveillance footage, the government has satisfied overbreadth considerations by ensuring that there is probable cause that location data of

perpetrators, co-conspirators and witnesses will be collected from Google, and that the scope of the warrant would not result in the collection of a broad sweep of data from uninvolved individuals for which there is no probable cause. *See United States v. Bentley*, 825 F.2d 1104, 1110 (7th Cir. 1987) (internal quotation marks and citations omitted) ("The Constitution requires that the warrant particularly describe the things to be sought and seized, but when there is probable cause to seize every business paper on the premises, a warrant saying seize every business paper particularly describes the things to be searched for and seized.").

III. Additional Considerations

Some additional observations warrant comment. First, the Court does not reach the issue of whether a warrant is a necessary requirement to request Google location data. In *Carpenter*, the Supreme Court determined that the government was required to obtain a warrant and meet the requirements of the Fourth Amendment when requesting a broad time-period of location data that tracked an individual and allowed the government to recreate a person's movement for 127 days. *Carpenter*, 138 S.Ct. at 2221. In so doing, the Court distinguished the third-party doctrine identified in *United States v. Miller*, 425 U.S. 435, 443 (1976), and noted that cell phones were such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society. *Id.* at 2220. The *Carpenter* Court further observed that a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up. *Id.* The Court explicitly stated its decision was narrow and did not express a view as to whether a warrant was required for a "tower dump," which is "a download of information on all the devices that connected to a particular cell site during a particular interval," and similar in some respects to a geofence request. *Id.* Google, however, has taken the position that individuals do have privacy interest in their location data in the context of a geofence request, and thus will only produce the

information upon presentation of a warrant. Brief for Google as Amicus Curiae, *United States v. Chatrie*, No. 3:19-cr-00130-MHL, 2020 WL 4551093 (E.D. Va. May 22, 2020), ECF No. [59-1] ("Google Amicus Brief"). As the courts did in *Google I*, 2020 WL 5491763 and *Google II*, 2020 WL 4931052, the Court does not need to reach this question because the government has chosen to obtain a warrant to obtain the geofence data based on a showing of probable cause. *See United States v. Patrick* , 842 F.3d 540, 544 (7th Cir. 2016) (declining to reach question of whether use of cell-site simulator was a search where government had conceded that it was a search). As a result, this Court, when presented with a warrant application, must apply Fourth Amendment principles to determine whether the warrant passes constitutional muster.[3]

Second, the Court recognizes that the target geofence zones drawn have a margin of error. That is, the boundaries of a geofence warrant are not perfect and there is the possibility that location data outside of the target locations may be captured. The government has noted this possibility and has also identified the buildings, both commercial and residential, that surround the target locations, in full candor. *See, e.g.*, Warrant Aff. ¶¶ 16, 28-30, 102. The exact scope of the margin of error for each device in each geofence zone is unknown. Google has identified that a user's location, when a strong GPS signal is available, can be estimated within approximately twenty meters. Google Amicus Brief at 10. Google has also attested to the accuracy of its location data, and that it is significantly more precise than the location data considered in *Carpenter*. *Id.* at 10. One only needs to look at one's location on Google Maps to know that the location data is remarkably accurate. At the same time, the margin of error is also evident in the common scenario

[3] The warrant in this case also involved public locations, such as streets, but the Supreme Court in *Carpenter* emphasized that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere" and the Court "has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 138 S. Ct. at 2217 (internal quotation marks and citations omitted). Thus, the fact that geofence data is sought partly in public areas does not change the analysis for this Court.

of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake. Google maps describes this as follows: "The blue dot shows you where you are on the map. When Google Maps isn't sure about your location, you'll see a light blue circle around the blue dot. You might be anywhere within the light blue circle."[4] Importantly, the government does not intentionally seek information outside the geofence zones, and if produced, it is the product of the technological limitations of location data tracking. A device which appears to be slightly outside of the target location's physical boundaries in the list of anonymized devices produced by Google might actually be within the target location – the margin of error helps account for this – and it is this data that the government seeks, not devices that are actually outside the geofence boundaries. However, location data outside the geofence boundaries and within the margin of error could be captured by the government's geofence warrant. Nevertheless, it is important to recognize that the Fourth Amendment deals in probabilities and reasonableness, and not exactness and pinpoint accuracy. *See e.g.*, *Brinegar v. United States*, 338 U.S. 160, 176 (1949) ("Because many situations which confront officers in the course of executing their duties are more or less ambiguous, room must be allowed for some mistakes on their part. But the mistakes must be those of reasonable [people], acting on facts leading sensibly to their conclusions of probability."); *Brinson v. Syas*, 735 F. Supp. 2d 844, 852–53 (N.D. Ill. 2010) (internal quotation marks and citations omitted) ("While many formulations for probable cause exist, all of them refer to the exercise of judgment, which hinges on the assessment of probabilities in particular factual contexts. Hence, the touchstone of reasonableness under the Fourth Amendment is sufficient

[4] *See Find and Improve your Location's Accuracy*, https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&hl=en (last visited Oct. 26. 2020).

probability, not certainty.") Thus, the fact that warrants for location data have margins of error does not invalidate them – only reasonableness is required, not surgical precision. A margin of error, in light of the remarkable accuracy of Google location data, is reasonable given the nature of the evidence being sought and what is possible with the technology at issue. *Archer*, 870 F.3d at 616 ("the particularity inquiry turns on what was realistic or possible in *this* investigation").

Furthermore, a criticism of geofence warrants is the potential that privacy concerns of uninvolved individuals are impacted, but again the issue is probable cause and particularity, not precision. As an initial matter, the fact that one uninvolved individual's privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual. For example, when a court authorizes the search of a house, the entire house is subject to the search, and this includes the most private areas of a house, such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children. *See United States v. Reichling*, 781 F.3d 883, 888 (7th Cir. 2015) (internal quotation marks and citation omitted) ("Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found."); *United States v. Percival*, 756 F.2d 600, 612 (7th Cir. 1985) ("[A] lawful search of fixed premises generally extends to every part of the premises in which the object of the search may be found, notwithstanding the fact that separate acts of opening or entry may be required to complete the search."). As another example, when a court authorizes the search of an individual's email account, it includes private emails sent by non-perpetrators that were not intended to be seen by the government, and may contain intimate and personal details, but are nonetheless viewed by government agents in the search for evidence of the crime. *See In Matter of Search Warrant Application for the Search of a Townhome Unit*, 20 M 106, 2020 WL 1914769,

at *1 (N.D. Ill. Apr. 20., 2020) (describing search protocol in electronic evidence searches). In another context, a search of a person's cell phone reveals calendar entries of meetings, events, and text messages with uninvolved individuals, along with pictures that identify that uninvolved individual's location.[5]

In other words, it is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are impacted. Similarly, in the geofence context, there is no way to exclude the possibility that at any given time, a delivery truck may drop off a parcel within the geofence location. The proper line of inquiry is not whether a search of location data could impact even one uninvolved person's privacy interest, but rather the reasonableness of the search, the probability of finding evidence at the location, and the particularity of the search request. Furthermore, it is also vital to repeat that the so-called "uninvolved individual" may actually be a *witness* to the crime. For example, the delivery truck driver, if present, could be a witness to the arson or suspicious vehicles driving to and from the arson site. The government is entitled to search for evidence of the crime pursuant to a valid warrant and that evidence includes the identity of witnesses to the offense.[6]

Third, the government has proposed a two-step process here, but it is important to recognize that this process does *not* ameliorate any constitutional concerns. The government, in

[5] In contexts outside of this search warrant, City of Chicago street surveillance cameras capture location and activities of innocent residents 24-hours a day. So do banks and grocery stores when open. Our location data is captured and stored in multiple places, even when unconnected to criminal activity.

[6] *Ybarra v. Illinois* is often cited for the proposition that probable cause must be particularized for all persons that are subject to a search. 444 U.S. 85, 91 (1979). In *Ybarra*, police obtained a warrant to search the public tavern and the bartender for narcotics, but the police *expanded* the search to include a bar patron that was present. *Id.* at 92-93. There are two key distinctions present here from the situation in *Ybarra*. First, the government is not expanding the scope of the warrant because it *explicitly* seeks location data for all individuals present in the geofence within the scope of the warrant. Second, as stated above, the government has established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence, and the request is sufficiently particular to avoid any concerns resulting from *Ybarra*.

the past, has suggested that the multi-step process minimizes overbreadth implications, but that is incorrect. *See Google I*, 2020 WL 5491763, at *5-*6; *Google II*, 2020 WL 4931052, at *2, *11-*13. In this Court's view, the fact that the government has requested anonymized data in the first step, and then at its discretion, can request subscriber information for all or some of the location data, is merely a process established for practical concerns rather than constitutional necessity. Google has established this procedure, which avoids the need for Google to produce large amounts of subscriber data to the government at the outset. *See* Google Amicus Brief at 12-13. Simply because the government is obtaining anonymized data at the outset does not minimize constitutional concerns because the government retains the discretion of obtaining all subscriber data should it so choose. The Supreme Court has made clear that a constitutionally permissible warrant does not leave open the opportunity for the government agent to use his discretion in conducting a search and seizure. *Stanford v. Texas*, 379 U.S. 476, 485-86 (1965). As a result, while the Court has authorized the warrant using the two-step process, it should not be viewed as in any way supporting the constitutionality of the warrant. Rather, the government has established probable cause to seize all location and subscriber data within the geofence locations identified. Whether it chooses to obtain all that information, or partial information, is of no matter to the Court's consideration of the constitutionality of the warrant under the Fourth Amendment.

Fourth, it is important to recognize that, in the discussion of geofence warrants, that no court has held that a geofence warrant is categorically unconstitutional. Rather, the issue is whether the warrant is supported by probable cause and is particular in time, location and scope to ensure that there is a fair probability that evidence of the crime will be obtained. In the course of that analysis, courts are concerned with overbreadth, namely, whether the warrant sweeps too broadly to capture location information that has no connection to the crime. This is not a unique

analysis, even though the technology employed here is new. When the court grants a warrant for a unit in apartment building for evidence of a wire fraud offense, it does not grant a warrant for that entire floor or the entire apartment building, but rather the specific apartment unit where there is a fair probability that evidence will be located. *See, e.g.*, *Lott v. City of Chicago*, No. 18 C 1278, 2020 WL 1503590, at *1 (N.D. Ill. Mar. 30, 2020); *Doe v. City of Chicago*, 580 F. Supp. 146, 148 (N.D. Ill. 1983). However, the government need not limit its warrant request to the home office within the apartment unit, or a particular file cabinet in the home office, but rather the apartment unit as a whole. The apartment unit is particular enough if supported by probable cause that evidence exists at that location.

In the geofence context, the same principles apply. There are numerous ways in which the government can satisfy analogous concerns about particularity and overbreadth. For example, in *Google I*, the Court recognized that a broad geofence request could be more particularized by seeking only location data of cell phones that overlapped in the various geofences, which would make it more likely, *i.e.* probable, that the perpetrator's location data is being disclosed. Overlapping data on all six geofence target locations here would certainly make it even more likely that the perpetrators' data will be collected, as it could pinpoint the specific individuals who committed the four arsons at separate times. However, in this case, an "overlapping request" is unnecessary because the warrant here is sufficiently particular in time, location and scope. Beyond that, it is important to recognize that a cell phone is not always sending location information to Google. For example, a Google user could configure a device, so that location services are only enabled for certain applications.[7] In that situation, it is possible that a user could have a location-activated application, such as Google Maps, open in one target location, but not at the others. The

[7] *See Choose Which Apps Use Your Android Phone's Location*, https://support.google.com/nexus/answer/6179507?hl=en (last visited Oct. 26. 2020).

phone could alternatively be in a dead zone or area where data connectivity is low for some target locations while having a better signal or data connectivity in other target locations. In such cases, an overlapping warrant could eliminate devices that are likely to have evidence of the crime. Thus, an overlapping warrant request may not be the best option for every situation. Another example to satisfy particularity is exactly what the government did here: draw narrowly tailored geofence zones for a sufficiently limited amount of time (approximately 15-30 minutes), and minimize through that zone design and subsequent investigation the possibility of sweeping in large amounts of location data for uninvolved individuals. All this is to say that, as with any warrant request, the Fourth Amendment principles of probable cause and particularity will guide the analysis rather than proclamations about whether requests for evidence impacted by new technology are *per se* unconstitutional. The Supreme Court, when considering the impact of new technology, has done exactly that in deciding whether a warrant is necessary to obtain data stemming from new technology. *See United States v. Jones*, 565 U.S. 400, 132 (2012) (GPS tracker); *Kyllo v. United States*, 533 U.S. 27 (2001) (thermal cameras); *Riley*, 573 U.S. 373 (cell phone); *Carpenter*, 138 S. Ct. 2206 (location data). And while *Riley* and *Carpenter* expressed concern over the ability of cell phones to track and recreate an individual's entire life stored on the cell phone, it is important to recognize that the privacy interests at stake in those cases were violated because warrants were not obtained from a neutral and detached judicial officers upon probable cause showings. *Carpenter*, 138 S. Ct. at 2221; *Riley*, 573 U.S. at 379-80. That is not the case here. The Fourth Amendment's search and seizure clause has been satisfied.

Conclusion

For the reasons stated above, the Court finds that the government's proposed search warrant satisfies the requirements of the Fourth Amendment, and thus the Court grants the government's application for the warrant.[8]

SO ORDERED.

Dated: October 29, 2020

Sunil R. Harjani
United States Magistrate Judge

[8] The warrant was authorized and signed by the Court on October 8, 2020.