

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

In the Matter of the Search of:	)	
	)	No. 20 M 392
Information Stored at Premises	)	Hon. Gabriel A. Fuentes
Controlled by Google	)	U.S. Magistrate Judge

**MEMORANDUM OPINION AND ORDER**

Before the Court is the government’s Amended Application for a Google Geofence Search Warrant (“the Amended Application”) (D.E. 6). While investigating the suspected theft of prescription medications, the government has developed evidence indicating that an unknown individual (“the Unknown Subject”) entered two physical locations to receive and ship the stolen medication at specific times. To try to identify the Unknown Subject, the government wants to know which mobile or smartphone devices that transmit their location information to service provider Google, Inc. (“Google”) can be known by Google to have been at those two locations at the times when the Unknown Subject was there. The government has proposed a “geofence” search warrant to obtain Google’s historical information about what devices were at those locations at those times.

**INTRODUCTION**

The idea behind a geofence warrant is to cast a virtual net – in the form of the geofence – around a particular location for a particular time frame. The government seeks to erect three geofences. Two would be at the same location (but for different time frames), and one would be at a second location. The window for each geofence is a 45-minute time period on a particular day. As to each of these geofences, the government proposes that Google be compelled to disclose a list of unique device identifiers for devices known by Google to have traversed the respective

geofences. The purpose of the geofences is to identify the devices known by Google to have been in the geofences during the 45-minute time frames around the Unknown Subject's appearances on surveillance video entering the two locations on three occasions. By identifying the cell phones that traversed any of the geofences, the government hopes to identify the person suspected in the theft of the pharmaceuticals, under the theory that at least one of the identified devices might be associated with the Unknown Subject.

The government's application is the third submitted by the government in this investigation. The government's first application ("the Initial Application") was denied by U.S. Magistrate Judge M. David Weisman. *See In re Search of Information Stored at Premises Controlled by Google*, No. 20 M 297 (D.E. 4) (N.D. Ill. July 8, 2020) (unsealed on July 16, 2020) ("7/8/20 Order"). The second of the three applications, filed in the above-captioned matter on July 24, 2020 ("the July 24 Application"), narrowed the geographical scope of the three proposed geofences, drawing them more tightly around the two physical locations where the Unknown Subject was seen entering to receive or ship the stolen medication, and attempting to reduce the number of devices (and persons) identified in the search. The undersigned magistrate judge denied the July 24 Application, relying heavily on Judge Weisman's analysis and finding that the warrant failed to meet the Fourth Amendment's particularity requirement and failed to establish probable cause to seize the location information of device users – unidentified and unknown at the time of execution of the warrant – who could not be shown to be involved in the subject offense. (7/24/20 Sealed Memorandum Opinion and Order ("7/24/20 Order"; D.E. 5).)

In the Amended Application now before the Court, the geographical scope of the geofences is unchanged from the July 24 Application, but the government has altered the proposed search protocol to eliminate the third of the three stages proposed in the first two applications. Those three

stages were (1) Google's collection of information it possesses about devices it believes traversed the geofences; (2) Google's production of an "anonymized" list of the unique device IDs for those devices as well as related information including their location coordinates and time stamps; and (3) Google's production of the subscriber information identifying the account holders or users of the devices on the anonymized list, with the government exercising its discretion as to the device IDs for which Google would obtain identifying subscriber information and provide it to the government. Having now eliminated the third stage, the government argues that the proposed warrant in the Amended Application has cured the constitutional infirmities set forth in the 7/8/20 and 7/24/20 Orders because the proposed warrant "does not seek any individual identifying information" and "cannot be used to identify a device's user without further information from Google." (Government's Memorandum in Support of Its Amended Application for Google Geofence Search Warrant ("Gov't Br."; D.E. 10) at 13, 15.) Further, in the Amended Application, the government has amended the description of the information to be seized, in Attachment B to the warrant, by limiting the "anonymized" information to that which "identifies individuals who committed or witnessed the offense." No further methodology or protocol is outlined as to how Google would know which of the sought-after anonymized information identifies suspects or witnesses. The government argues that the proposed warrant's language limiting the "anonymized" information to that which "identifies individuals who committed or witnessed the offense" brings the warrant into compliance with the particularity requirement by limiting *the government's* discretion "to select device information from among the anonymized lists." (*Id.* at 17.) The government also added, after an inquiry by the Court, a representation that the government retains the power to obtain by subpoena the identifying subscriber information for any

of the device IDs on the anonymized list obtained under the proposed warrant, but that the government would do so only after reviewing the anonymized information. (*Id.* at 16-17.)

### DISCUSSION

According to the Amended Application, Google collects location information data from sources including GPS data, cell-site information, wi-fi access points, and Bluetooth beacons within range of a given mobile device. Google offers an operating system known as Android for mobile devices, and devices using the Android operating system have associated Google accounts. Devices that do not run the Android operating system, such as Apple devices, also communicate with Google through Google applications that are available on Apple products. When a device user enables Google’s “location services” on an Android device, or a “location sharing” (with Google) feature on a non-Android device, Google collects and retains location data from that device. The location data can show that a certain device was located at a particular place at a particular point in time. From this information, the government can seek to identify the device’s user, from information the user may have provided to Google. The Amended Application does not quantify an estimated percentage of all devices that communicate with Google in a manner that would transmit location information to Google, but the Amended Application suggests that a device that does not do so would be a relatively rare case.<sup>1</sup>

---

<sup>1</sup> The government represented in the affidavit attached to the Amended Application that Google Android phones comprised approximately 74% of the worldwide smartphone market in 2019, that Apple phones comprised approximately 23% of the smartphone market during that same time period, and that many Apple devices nonetheless communicate with Google due to Google applications that are available on Apple products, such as Gmail, Google Maps, Google Chrome, and YouTube. Accordingly, the government represented, “a person possessing a smartphone likely transmits data to Google.” *See* Amended Application, Affid. ¶ 14. The Court will refer to the at-issue devices, whose connection to Google’s Android operating system or to Google applications on Apple devices causes them to transit location information to Google, as “Google-connected devices.”

The Amended Application requires the Court to review carefully the evolution of Fourth Amendment law, from its longstanding probable cause and particularity requirements to its application to modern electronic devices and to the privacy interests our courts have recognized as arising from such devices' widespread and everyday use.

**I. The Fourth Amendment and Its Applicability to the Amended Application**

**A. The Amended Application Proposes a Search for Fourth Amendment Purposes.**

The Fourth Amendment bars unreasonable searches and seizures. U.S. Const. amend. IV. In describing the Fourth Amendment as a protection of people and not places, the U.S. Supreme Court has stated that what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” *Katz v. United States*, 389 U.S. 347, 351 (1967). A government intrusion into a person’s private sphere qualifies as a “search,” triggering the Fourth Amendment requirement that the intrusion be authorized by a warrant supported by probable cause, when that person “‘seeks to preserve something as private,’ and his expectation of privacy is ‘one that society is prepared to recognize as reasonable.’” *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018), quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979). The Supreme Court also has recognized that an intrusion need not be “trespassory” to be considered a search for Fourth Amendment purposes. *See United States v. Jones*, 565 U.S. 400, 412-13 (2012) (affirming court of appeals decision that required a warrant for a search that tracked an individual’s movements for 28 days with global positioning technology).

In *Carpenter*, the Supreme Court extended the warrant requirement to “cell-site location information” or “CSLI” maintained by cellular service providers, reasoning that the privacy interest in one’s movements, as discoverable through the CSLI, was an interest that modern society

was prepared to recognize as reasonable. 138 S. Ct. at 2217. The Supreme Court in *Carpenter* spoke of the device holder's "anticipation of privacy in his physical location":

Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." These location records "hold for many Americans the 'privacies of life.'"

*Id.*, quoting, among other authorities, *Riley v. California*, 573 U.S. 373, 403 (2014).<sup>2</sup> In *Riley*, the Court held that a search warrant is required to conduct a search, incident to arrest, of the contents of a suspect's cellular telephone. 573 U.S. at 401. *Riley* based its holding in large part on a recognition that given the large amount of data that some electronic devices can store, their owners have a reasonable expectation of privacy with respect to the contents:

Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom. Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.

*Id.* at 393. *Riley* was decided six years ago, but the Supreme Court further observed then that personal electronic devices are characterized by "an element of pervasiveness" not applicable to physical records:

---

<sup>2</sup> *Carpenter* involved judicial review of two orders, one of which resulted in disclosure of CSLI over a seven day period; the Supreme Court stated that its holding was based on CSLI monitoring occurring over at least seven days. 138 S. Ct. at 2217 n.3.

Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.

*Id.* at 395.

*Carpenter* also held that the government's retrieval of CSLI from a third-party service provider qualified as a search for Fourth Amendment purposes, notwithstanding the "third-party" doctrine, under which courts have held that persons lack a reasonable expectation of privacy in information they have revealed to the third party. *Carpenter*, 138 S. Ct. at 2218-20. The third-party doctrine is based on the premise that a person's voluntary sharing of information with the third party defeats an argument that such person has a legitimate expectation of privacy in the information. *See Smith*, 442 U.S. at 743-44; *United States v. Miller*, 425 U.S. 435, 443 (1976). *Miller*, for example, involved checks and other records held by a bank, and the defendant "voluntarily conveyed" such information to the bank. 425 U.S. at 442. In *Carpenter*, the Supreme Court concluded that this same line of reasoning, i.e., that persons voluntarily convey the information about their physical location (based on their devices' contact with cell towers) by virtue of their relationship with the provider as subscribers to the service, did not apply because of the indispensable role mobile technology plays in modern society. 138 S. Ct. at 2220. Unlike bank records, CSLI is something a person using a cellphone (meaning, basically, almost everyone) cannot avoid creating, so the users cannot be said to have voluntarily assumed a risk that they were disclosing "a comprehensive dossier" of their physical movements. *Id.*

The Amended Application presents a different factual setting than did *Carpenter* and *Jones*, in that the Amended Application targets a 45-minute window on three specific days, whereas *Carpenter* involved at least seven days of data and *Jones* involved 28 days, thus

generating the Supreme Court’s concern, for purposes of the third-party doctrine, that persons would not ordinarily expect to have revealed an “all-encompassing record” or a “comprehensive dossier,” as *Carpenter* put it, of their movements and associations. *Id.* at 2217, 2220. The far shorter time frame of government monitoring involved in the proposed geofences here raises questions about the degree to which *Carpenter* may support a conclusion that in this case, the geofences constitute a search for Fourth Amendment purposes. The Supreme Court in *Carpenter* stated that it was not deciding “whether there is a limited period for which the Government may obtain an individual’s CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.” *Id.* at 2217 n.3; *see also Jones*, 565 U.S. at 412 (declining to reach the “novel[]” question of what duration of monitoring in various types of investigations would constitute a search). The opinion in *Carpenter* also stated that its holding was “a narrow one,” in that “[w]e do not express a view on matters not before us: real-time CSLI or ‘tower dumps’ (a download of information on all the devices that connected to a particular cell site during a particular interval).” *Id.* at 2220.

Here, the government has submitted an application for a search warrant and has argued that its search is supported by probable cause and in compliance with the Fourth Amendment’s particularity requirement. (*See Gov’t Br.* at 2.) Accordingly, the government is treating its proposed capture of information as a search, even though the government, in a footnote to its brief, noted the foregoing limiting language from *Carpenter* to suggest that the government’s requested “2.25 hours of anonymized location data (45 minutes of location data over three different dates) . . . would not provide an ‘all-encompassing’ record of an individual’s whereabouts.” (*Id.* at 11 n.2.) By having opted for a search warrant application in lieu of taking a chance that a warrantless



seizure of the information to be yielded by the proposed geofences would not be upheld, and by not having developed further the argument for the Fourth Amendment's inapplicability, the government has forfeited the argument. *United States v. Diggs*, 385 F. Supp. 648, 652 (N.D. Ill. 2019) (finding that government forfeited argument that historical GPS tracking of defendant's car did not give rise to reasonable expectation of privacy because others may have used the car), citing *United States v. Stanbridge*, 813 F.3d 1032, 1038 (7th Cir. 2016). See also *Alioto v. Town of Lisbon*, 651 F.3d 715, 721 (7th Cir. 2011) (stating that forfeiture rule applies to arguments that "a party fails to develop"). In any event, the government's concession that the proposed geofences are a "search" for Fourth Amendment purposes is enough to allow the Court to avoid deciding that question. 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).

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. As far as the third-party doctrine is concerned, the record before the Court suggests that device users connect to Google's location services, or to Google applications that cause them to reveal their location information to Google, with great regularity.<sup>3</sup> The Court finds it difficult to imagine that users of electronic devices would

---

<sup>3</sup> See *supra* n.1. Published 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. See Ryan Nakashima, "AP Exclusive: Google tracks your movements, like it or not," *The Associated Press* (Aug. 13, 2018) ("Even with Location History paused, some Google apps automatically store time-stamped location data without asking. (It's possible, although laborious, to delete it.)") (<https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not>); Ryan Nakashima, "AP NewsBreak: Google clarifies location-tracking policy," *The Associated Press* (Aug. 16, 2018) (reporting that Google, two days after the Associated Press reported that Google stores location information for users who have opted not to have that information stored,

affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government’s ability to obtain – easily, quickly and cheaply – their precise geographical location at virtually any point in the history of their use of the device.<sup>4</sup>

---

clarified its website description of its practices, acknowledging that “some location data may be saved as part of your activity on other services, like Search and Maps”) (<https://apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211/APNewsBreak:-Google-clarifies-location-tracking-policy>).

<sup>4</sup> Google has taken the position that the third-party doctrine should not defeat a cell-phone user’s reasonable expectation of privacy in their location-history information because the user’s sharing that information with a third-party such as Google is not truly voluntary. Brief of Amicus Curiae Google LLC at 20-22, *United States v. Chatrue*, No. 3:19-cr-00130-MHL (E.D. Va. Dec. 23, 2019), ECF No. 73. In the amicus brief Google submitted in *Chatrue*, Google argued that “as in *Carpenter*, the fact that users voluntarily choose to save and share [location-history] information with Google does not on its own implicate the third-party doctrine to the extent that doctrine is still viable.” *Id.* at 20, 22. Drawing a comparison with the Supreme Court’s reasoning in *Carpenter* that the “voluntary exposure” rationale underpinning the third-party doctrine did not justify applying the doctrine to cell-site location information since cell-phone users did not “genuinely ‘share’ such data with phone companies,” Google argued that “the same is true of the location-based services [cell phones provide].” *Id.* at 21-22. These services, Google argued, are “such a pervasive and insistent part of daily life that [they are] . . . indispensable to participation in modern society.” *Id.* at 22 (internal quotations omitted) (quoting *Carpenter*, 138 S. Ct. at 2220). As some scholarly commentary has observed:

The third-party doctrine should not apply with respect to certain technologies because much of the information forfeited by individuals is completed on behalf of their devices. To waive Fourth Amendment protections, the individual must voluntarily provide information to a third party. However, many device users do not voluntarily relinquish information; rather, when the devices are powered on, information is sent on behalf of the individual to third parties. No voluntary action triggers this collection, and warrantless government searches conducted under the authority of the third-party doctrine should be unconstitutional. Because this is similar to the reasoning in *Carpenter*, this data collection should be given the same protections as CSLI [cell site location information].

Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age: Carpenter v. United States and the Fourth Amendment’s Third-Party Doctrine*, 28 Cath. U.J.L. & Tech. 89, 120-21 (2020). See also Chadwick Lamar, *The Third-Party Doctrine Crossroads: Rules and Direction for A Tech-Savvy Fourth Amendment*, 39 Rev. Litig. 215, 241 (2019) (“characterizing *Carpenter* as the new norm [with respect to the third-party doctrine] comports with the Supreme Court’s trend towards providing more protection in light of technological advancement”); Daniel de Zayas, Note, *Carpenter v. United States and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 Am. U. L. Rev. 2209, 2243-45 (2019) (“As technology increasingly integrates into modern society, perpetuating a rigid and unqualified third-party doctrine guarantees increasingly intrusive, ‘absurd and problematic’ government surveillance.”).

In addition, as far as *Carpenter*'s reference to "tower-dump" and "real-time CSLI" decisions is concerned, a review of those decisions yields no firm basis for a conclusion that *Carpenter*'s holding as to "what is a search" should or must be limited to seven days of CSLI. In a "tower dump," CSLI is retrieved for all devices that connected to a cell site tower at a previous point in time. See *United States v. Adkinson*, 916 F.3d 605, 608 (7th Cir. 2019). In *Adkinson*, a private party service provider identified a person believed to have robbed two of its stores by retrieving "tower dump" information from cell sites near the two stores at the time of the robberies under a privacy policy allowing it to disclose information about its phone users. 916 F.3d at 608. The suspected robber's phone was the only device detected by both tower dumps. *Id.* The provider then disclosed the information to the government. *Id.* *Adkinson* noted that *Carpenter* did not invalidate cell tower dumps as unlawful warrantless searches but went no farther, affirming the district court's denial of the defendant's suppression motion on other grounds including the good-faith exception to the warrant requirement. *Id.* at 611. Moreover, the "search" in *Adkinson* is described correctly as a private search, and not a government search. *United States v. Diggs*, No. 18 CR 85, 2020 WL 208826, at \*1 (N.D. Ill. Jan. 14, 2020).

"Real-time CSLI" is generated by devices known as "cell-site simulators," sometimes known by the brand name of "Stingray." *Patrick*, 842 F.3d at 542. Cell-site simulators operate in real time and transmit signals as if they are cell towers, causing cellular devices near the simulator to identify the simulator as the most attractive cell tower in the area and thus to transmit – to the simulator – signals that identify the device in the same way the device's connection to a cell tower would generate CSLI that could be retrieved later by the provider. See *id.* at 542-43. In *Patrick*, which involved a challenge to use of a cell-site simulator, the government conceded that such use was a search, so the Seventh Circuit expressly declined to reach questions including whether the

duration of the real-time CSLI tracking, or its geographical precision, bore upon whether use of the simulator was a search. *Id.* at 544. The *Patrick* opinion nonetheless questioned whether the use of a cell-site simulator qualifies as a search, but in so doing, the opinion relied on the Sixth Circuit's 2016 *Carpenter* decision, *id.* at 543-44, which the Supreme Court reversed in 2018 on the very question of the reasonableness of an expectation of privacy in CSLI data.<sup>5</sup>

The Seventh Circuit has not yet addressed whether tower dumps or the use of cell-site simulators are Fourth Amendment searches. The real-time CSLI cases outside the Seventh Circuit have gone in different directions, but none of those results definitively answers the question of how long a governmental intrusion must be in order for it to trigger Fourth Amendment scrutiny.<sup>6</sup> Nor do the "tower-dump" cases offer much more help in answering that question, and the one such case cited by the government involved an examination of CSLI generated from cell towers for a

---

<sup>5</sup> In a dissent in *Patrick*, Judge Wood wrote that she would have remanded the case for further fact-finding on how the simulator was used, so that its use could receive closer judicial scrutiny. *Id.* at 552 (Wood, C.J., dissenting).

<sup>6</sup> Compare *United States v. Chavez*, No. 15-CR-00285-LHK, 2019 WL 1003357, at \*11 (N.D. Cal. Mar. 1, 2019) ("Post-*Carpenter*, the government must obtain a warrant supported by probable cause to access historical cell-site location information unless an exception to the exclusionary rule applies. Eventually, the same may be expected of real-time cell-site location information, where an individual has arguably an even greater expectation of privacy.") (citing *United States v. Ellis*, 270 F. Supp. 3d 1134, 1145-46 (N.D. Cal. 2017) (holding, before *Carpenter*, that "cell phone users have an expectation of privacy in their cell phone location in real time ... society is prepared to recognize that expectation as reasonable")), and *United States v. Stachowiak*, No. 18-cr-296-SRN-KMM, 2019 WL 3292048, at \*6 n.6 (D. Minn. Apr. 23, 2019) ("[T]he same concerns that motivated the majority's conclusion in *Carpenter* regarding historical CSLI, including the intrusion on personal privacy occasioned by the ability of law enforcement to use cell-phone location data to compile comprehensive information about an individual's past movements ... apply with equal force to real-time GPS monitoring of a cell-phone's location) (citation omitted), with *United States v. Thompson*, No. 13-40060-10-DDC, 2019 WL 3412304, at \*7 (D. Kan. July 29, 2019) ("[E]xtending *Carpenter*'s holding about the seizure of historical CSLI to the seizure of real-time CSLI is far from clear because *Carpenter* emphasized that historical CSLI allowed the government to learn of a person's whereabouts on a nearly 24-hour, seven-day-a-week basis .... [and] seizing CSLI in real-time only reveals a person's whereabouts at the moment of its seizure."), and *United States v. Woodson*, No. 4:16CR541AGF(SPM), 2018 WL 7150388, at \*9 (E.D. Mo. Nov. 21, 2018) (denying, after *Carpenter*, motion to suppress real-time CSLI used to obtain defendant's previously unknown telephone number, so that seizure of CSLI "does not give rise to the same privacy and Fourth Amendment concerns as *Carpenter*").

period of only four minutes.<sup>7</sup> And, importantly, CSLI is *different* than the information proposed to be generated by the geofences. CSLI, as the Supreme Court examined it in *Carpenter*, places a person only within “a wedge-shaped sector ranging from one-eighth to four square miles.” *Carpenter*, 138 S. Ct. at 2218. The proposed geofences in the Amended Application would establish the person’s physical location with *far greater precision*. The government did not provide a square-footage estimate, but at one location, the geofence is to be drawn around a specific business establishment and extends to the sidewalk and street outside it and to at least three residential floors above it; at the second, the geofence encompasses a business establishment and the parking lot next to it, along with at least one set of lanes of a very busy thoroughfare. The government would therefore learn precisely where the devices were used, not just within a city block or a two-mile-long stretch of that block, but within and outside of a single business establishment or set of residences on that block. The information to be generated by the proposed geofence warrant would not be an “all-encompassing record” of a person’s movements, but it is a record of almost exactly where that person was at a particular time.

---

<sup>7</sup> The government, in not further developing the argument against the geofences qualifying as a search, did not discuss the tower dump and real-time CSLI cases, citing two tower-dump cases in which search warrants were obtained. (See Gov’t Br. at 11), citing *United States v. James*, No. 18-cr-216 (SRN/HB), 2018 WL 6566000, at \*1, 4 (D. Minn. Nov. 26, 2018) (finding probable cause to support the tower dump warrant), *aff’d*, 2019 WL 352231, at \*4-5 (D. Minn. Jan. 25, 2019), and *In the Matters of the Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (finding probable cause to support search warrant after having denied application for order under 18 U.S.C. §2703(d)), *overruled on other grounds*, *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 602 (5th Cir. 2013) (holding that tower dump applications for CSLI did not trigger the Fourth Amendment warrant requirement because the information amounted to mere business records to which the third-party doctrine applied). *Carpenter* overruled *Historical Cell Site Data* on whether obtaining historical CSLI was a search triggering Fourth Amendment scrutiny, as the Fifth Circuit has recognized. *United States v. Beverly*, 943 F.3d 225, 233-34 (5th Cir. 2019). The tower dump cases are probably more useful when examined for the respective durations of the tower dumps involved in those cases, at least for purposes of analyzing whether *Carpenter* should be extended to circumstances involving governmental intrusions of shorter duration. Interestingly, the cell tower dumps for which the magistrate judge approved a search warrant in *Cellular Telephone Towers*, a decision ultimately vindicated by *Carpenter* on the broader question of whether CSLI can give rise to a privacy interest triggering the Fourth Amendment, involved five separate towers over a time span of just four minutes. *Cellular Telephone Towers*, 945 F. Supp. 2d at 769.

When a court is presented squarely with the task of settling this “vexing” and “novel[]” question (as the Supreme Court in *Jones* described it, 565 U.S. at 412) about the degree of location monitoring needed to trigger Fourth Amendment protection, that court may have to consider where to draw the line, or whether to impose a bright-line rule. A bright-line rule arguably would be more protective of the types of device-related privacy interests that the Supreme Court has determined are growing expansively greater as the government, through technological advances, is increasingly able to collect more data, and more precise data, about people and their movements. *See United States v. Cairra*, 833 F.3d 803, 808 (7th Cir. 2016) (noting that the two concurring opinions in *Jones*, signed by five Supreme Court justices, “expressed the view that technology has changed the constitutional calculus” about whether monitoring a person’s movements on public streets could amount to a “search”). Hopefully that question could be answered on a far more fully developed record than is before the Court here.<sup>8</sup> *See City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010) (“[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear”); *Patrick*, 842 F.3d at 546 (Wood, C.J., dissenting) (calling for further fact-finding where “[t]he record is painfully – indeed fatally – inadequate with respect to critical details about the way the Stingray was used”).

With the government having treated its proposed geofences as a search as set forth in the Amended Application and the government’s brief, the Court does not reach the questions that *Carpenter* and *Jones* left unanswered about just how much of a privacy interest society might recognize as reasonable in a person’s precise whereabouts for a short or even momentary duration.

---

<sup>8</sup> *See supra* n.3.

Because the government has treated the Amended Application as a proposed search, we move on to whether the Fourth Amendment will permit the geofence search as proposed.

**B. The Fourth Amendment’s Probable Cause and Particularity Requirements**

Probable cause is “a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause is a “practical, nontechnical conception” based on “common-sense conclusions about human behavior,” and courts determine its existence by analyzing the totality of the circumstances surrounding the proposed intrusion. *Id.* at 231, 238. The Fourth Amendment also requires that any warrant must “particularly describe[] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The Court will discuss the particularity requirement in somewhat greater detail.

The particularity requirement operates as a protection against arbitrary government intrusions, as the Fourth Amendment’s very purpose is “to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” *Carpenter* 138 S. Ct. at 2213, quoting *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967). The Fourth Amendment has its roots in colonial resistance to “the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” *Riley*, 573 U.S. at 403. In 1965, the U.S. Supreme Court commented that its past recitations of “the detailed history of the use of general warrants as instruments of oppression from the time of the Tudors, through the Star Chamber, the Long Parliament, the Restoration, and beyond” was so well-trodden that to review it again would be “a needless exercise in pedantry.” *Stanford v. Texas*, 379 U.S. 476, 482 & n.5 (1965). The Court nonetheless recounted:

In Tudor England officers of the Crown were given roving commissions to search where they pleased in order to suppress and destroy the literature of dissent, both



Catholic and Puritan. In later years warrants were sometimes more specific in content, but they typically authorized of all persons connected of the premises of all persons connected with the publication of a particular libel, or the arrest and seizure of all the papers of a named person thought to be connected with a libel.

*Id.* at 482-83.

In *Stanford*, the Supreme Court invalidated, as a “general warrant,” a state-issued warrant allowing law enforcement officers to search a Texas home for books and records evidencing the occupant’s activities in the Communist Party, which was banned under Texas law. *Id.* at 478-79, 486. The Court noted that the words of the particularity requirement of the Fourth Amendment are “precise and clear” and “reflect the determination of those who wrote the Bill for Rights that the people of this new Nation should forever ‘be secure in their persons, houses, papers, and effects’ from intrusion and seizure by officers acting under the unbridled authority of a general warrant.” *Id.* at 481, quoting U.S. Const. amend. IV. General warrants permit “a general, exploratory rummaging in a person’s belongings,” an “evil” that the Fourth Amendment addresses by requiring a particular description of the things to be seized in the search. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The particularity requirement’s bar on general warrants protects not only the sanctity of a person’s home but also “the privacies of life.” *Berger v. New York*, 388 U.S. 41, 58 (1967), citing *Boyd v. United States*, 116 U.S. 616, 630 (1886). The particularity requirement accomplishes this end by “mak[ing] general searches under them impossible,” and “[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Stanford*, 379 U.S. at 485.

Our appeals court has recognized that the required specificity, under the Fourth Amendment’s particularity requirement, need not be “granular” in its detail because often the executing officer cannot know the nature of the things to be seized with “pinpoint” accuracy. *Archer v. Chisholm*, 870 F.3d 603, 616 (7th Cir. 2017). The Seventh Circuit in *Archer* for example,



found no particularity problem with a warrant that identified the petitioner's home as the place to be searched and described "all" documents "relating to" identified contracts or transactions as the things to be seized. *Id.* A warrant authorizing the seizure of "all documents relating to a particular person, place or thing" may be "broadly worded" and "adequately defines the officers' authority [to search for particular items]." 7/8/20 Order at 3, quoting *United States v. Mason*, No. 92-CR-1069, 1993 WL 191806, at \*2 (N.D. Ill. June 4, 1993). But the particularity requirement does not allow the government to rummage through information in search of other information. *See United States v. Sanchez-Jara*, 889 F.3d 418, 421 (7th Cir. 2018). In *Sanchez-Jara*, a pre-*Carpenter* decision in which authorities obtained a search warrant to use a cell-site simulator to identify two specific cellular phones and to track their location, the Seventh Circuit affirmed the conviction and held that the warrant authorizing the disclosure of location information for those two specific phones was not a general warrant:

[A]uthorization to search a whole home for evidence of a crime flunks the particularity requirement. But a warrant authorizing police to follow an *identified* phone, to see where it goes and what number it calls, particularly describes the evidence to be acquired .... [The] warrant is not an open-ended authorization for public officials to rummage wherever they please in order to see what turns up.

889 F.3d at 421 (emphasis added).

## **II. Fourth Amendment Analysis of the Amended Application's Proposed Geofences**

Our analysis of the Amended Application under the Fourth Amendment begins with the denials of the two earlier applications and explores the degree to which the constitutional shortcomings of those applications were addressed or remedied in the Amended Application.

### **A. The Evolution of the Amended Application's Proposed Geofences**

The Amended Application identifies two locations for the three geofences, one of which is at the first location ("Location 1"), and two of which are at the second ("Location 2"). Each of

the geofences has specific geographical and time parameters. The geofence parameters and the protocol for searching them for electronic devices have evolved in the three applications submitted to the Court.

### **1. The Geographical Reach of the Geofences**

The geographical reach of the proposed geofences in the Amended Application are as follows, as set forth in its Attachment A:

Location 1 includes a commercial enterprise where the government contends – and the Court agrees – there is probable cause to believe, based on the agent’s affidavit, that the Unknown Subject received a shipment (“Shipment 1”) of stolen pharmaceuticals. The area proposed for the geofence at Location 1 is a polygon-shaped area around the commercial enterprise, which is located within a mixed-use commercial and residential building; the area covers the commercial enterprise outward to the sidewalk (and apparently at least one adjoining city street at the corner of the building),<sup>9</sup> and upward at least three stories to the top of the building, encompassing residential units above the business enterprise. Without disclosing Location 1 in this Opinion, the Court takes judicial notice of the fact that Location 1 is situated within a busy commercial and residential area on a major arterial street in a major U.S. city, and that more than 100 residential units of varying size are in the whole of the building that houses Location 1. The building around Location 1 houses retail establishments and is near a supermarket. It is not known how many residential units would be within the geofence, in whole or in part, but the geofence appears to

---

<sup>9</sup> The latitudinal and longitudinal coordinates the government provided, when plotted on a satellite-view, Google Earth (<http://earth.google.com/>) map of the Location 1 geofence, show the geofence’s linear boundaries extending into the side street located to the west of the mixed-used building and possibly into a portion of the major thoroughfare located to the north of the building. The coordinates plotted on such a map of the Location 2 geofence show its linear boundaries roughly halfway across the major arterial street that is located to the west of the commercial enterprise. Those boundaries may extend even farther to encompass both directions of travel on the respective major streets alongside Locations 1 and 2 based on the “margin of error” that the government includes within the geofences.

cover about one-eighth of the space in the mixed-use building. The time and date parameters for this first geofence cover a 45-minute span of time on a single day, and the Court finds that there is probable cause to believe that the offense conduct reflected in Shipment 1 occurred at a particular point within this window of time at Location 1, based on the facts the Amended Application proffered about Shipment 1 being involved in the offense, and about the Unknown Subject's appearance on surveillance video at Location 1, receiving that shipment.

Location 2 includes a commercial enterprise where the government contends – and the Court agrees – there is probable cause to believe that the Unknown Subject shipped stolen pharmaceuticals on two separate occasions (“Shipments 2 and 3”). The two proposed geofences at Location 2 cover the same geographical area. The two geofences are proposed for a square-shaped area encompassing the commercial enterprise and a parking lot outside it. The Court takes judicial notice of the fact that Location 2 is situated within a busy commercial area on a major arterial street in a major U.S. city and differs from Location 1 in that the commercial enterprise in Location 2 operates in a stand-alone building where there are no other apparent business users, and no residential users. The geofences apparently also would extend into half of the lanes of the arterial street outside Location 2.<sup>10</sup> Other significant retail businesses are nearby, including one immediately adjacent to the parking lot within the proposed Location 2 geofences. The time and date parameters for the second and third geofences, both around Location 2, are separate 45-minute spans of time on two dates. The Court finds that there is probable cause to believe that the offense conduct reflected in Shipments 2 and 3 occurred at a particular point within those respective windows of time at Location 2, based on the facts the Amended Application proffered about

---

<sup>10</sup> See *supra* n.9.

Shipments 2 and 3 being involved in the offense, and about the Unknown Subject's appearance on surveillance video at Location 2, making those shipments.

The foregoing geographical boundaries of the geofences differ from those proposed in the Initial Application denied by Judge Weisman on July 8, 2020. The boundaries in the Initial Application were defined by circles around the business enterprises within Locations 1 and 2, with each circle having a 100-meter radius. Judge Weisman found the proposed search warrant in the Initial Application overbroad. (7/8/20 Order at 4-9.) He found the proposed geofences encompassed "structures and businesses that would necessarily have cell phone users who are not involved in these offenses," in a "congested urban area encompassing individuals' residences, businesses, and healthcare providers," whereas "the government's evidence of probable cause is solely focused on one user of a cellular telephone." (*Id.* at 4, 6.)

To try to address those concerns, the government submitted the July 24 Application, shrinking the geofences to the square- or polygon-shaped boundaries around Locations 1 and 2 as described above. The boundaries in the July 24 Application were the same as those proposed in the Amended Application now before the Court, except the government added a "margin of error," discussed further below. The undersigned magistrate judge denied the July 24 Application based on overbreadth and lack of particularity, concluding:

Although the government appeared to be following Judge Weisman's suggestions that a narrower search might pass constitutional muster, the modifications the government made to the geofence boundaries do not solve the constitutional problem because although the modifications may well reduce the number of devices Google identifies as having traversed the geofences, the Court still has no idea how many such devices and their users will be identified under the warrant's authority .... All we know is that the information of an undetermined number of uninvolved persons is to be seized.

(7/24/20 Order at 22.)

In addition, the 7/24/20 Order found further fault with the manner in which the government had added to the geographical scope of the geofences, even after drawing them more tightly around Locations 1 and 2. The July 24 Application added, to the information to be seized, the device IDs (and the subscriber information for those devices), of devices that fell not only within the delineated coordinates of the three geofences, but also within a “margin of error,” based on Google’s “calculation as to the location of a device as a meter radius, referred to by Google as a ‘maps display radius,’ for each latitude and longitude point.” The Court noted that the government had not attempted to quantify the degree to which this inclusion of an ill-defined “margin of error”<sup>11</sup> geographically expended the geofences, but the Court observed that in the busy urban

---

<sup>11</sup> Additional information about the Google “margin of error,” though not contained in the Amended Application, may be found in the public record on the docket in *United States v. Chatrie*, No. 19-cr-00130-MHL (E.D. Va.), a matter in which a federal court is considering a motion to suppress evidence obtained by a geofence warrant. According to a declaration filed in *Chatrie*, Google provided the following information:

The location data points reflected in [Google Location History (“LH”)] are estimates based on multiple inputs, and therefore a user’s actual location does not necessarily align perfectly with any one isolated LH data point. Each set of coordinates saved to a user’s LH includes a value, measured in meters, that reflects Google’s confidence in the saved coordinates. A value of 100 meters, for example, reflects Google’s estimation that the user is likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. In other words, if a user opens Google Maps and looks at the blue dot indicating Google’s estimate of his or her location, Google’s goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.

Notwithstanding the confidence interval described above, if a user’s estimated location (*i.e.*, the stored coordinates in LH) falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request, even if the shaded circle defined by the 68% confidence interval falls partly outside the radius of the geofence request. As a result, it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius. To provide information about that, Google includes in the production to the government a radius (expressed as a value in meters) around a user’s estimated location that shows the range of location points around the stored LH coordinates that are believed to contain, with 68% probability, the user’s actual location.

areas of Locations 1 and 2, where the geofences already extended at least slightly into areas where uninvolved persons might have traversed, even small-scale expansions of the geofences increased the likelihood of capturing the identities and locations of uninvolved persons, providing another reason why the warrant was overbroad. (*Id.* at 23.) The Court also found the proposed warrant in the July 24 Application lacking in probable cause as to unknown device users not linked by any of the proffered facts to the subject offenses. (*Id.* at 17-21.)

The undefined “margin of error” remains included in the government’s definition of the geofences it proposes, in the Amended Application, to erect around Locations 1 and 2.

## **2. The Evolution of the Search Protocol**

As noted above in the introduction to this opinion, the government’s Initial Application and July 24 Application sought court authorization for compelling Google to obtain and disclose to the government, under a three-stage prescribed protocol, data generated from the three geofences as to Google-connected devices during the specified dates and time frames as follows:

- First, Google would search for “location history” data, for those time frames, dates and locations, identifying the Google-connected devices 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 July 24 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.

---

McGriff Decl. ¶¶ 24-25, *Chatrie*, No. 19-cr-130-MHL (E.D. Va. Mar. 11, 2020), ECF No. 96-1. It is not clear to the Court, from this declaration or from the Amended Application, how far the margin of error might extend, except perhaps that the additional area outside the geographical parameters of the Location 1 and 2 geofences might be measured in an unknown number of meters.

- Third, the government would review the anonymized information and would communicate to Google the mobile device identifiers (from the anonymized information) as to which the government, under the authority of the warrant, obtains compelled disclosure by Google of the identifying subscriber information for the Google accounts associated with each of those specified mobile devices, identified at the government's discretion.

In denying the Initial Application and the July 24 Application, both Judge Weisman and the undersigned magistrate judge were troubled by the **unlimited discretion the protocol provided** the government with respect to learning the identities of the persons whose devices showed up on the anonymized list(s) in the second stage of the protocol. Judge Weisman found that the requested warrant was “completely devoid of any meaningful limitation” and concluded that the three-stage process proposed in the Initial Application did not satisfy the Fourth Amendment's particularity requirement because it gave law enforcement agents **unbridled discretion to obtain identifying information about each device detected in the geofences.** (7/8/20 Order at 4, 7.) The Initial Application's proposed warrant contained no language objectively limiting the number of devices as to which agents could obtain identifying information. (*Id.*) Importantly, for purposes of this Court's examination of the Amended Application, the 7/8/20 Order added:

If the warrant did contain objective limits as to which cellular telephones agents could seek additional information, or the nature of the probable cause established in the warrant application suggested a very limited number of cellular telephones would be identified, the Court's concern with overbreadth and particularity might be satisfied .... [I]f the government had constrained the geographic size of the geofence *and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences, the government would have solved the issues of overbreadth and lack of particularity.*

(*Id.* at 7, 8-9 (emphasis added).) In addition, Judge Weisman did not agree with the government that *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), supported the government's argument that the Initial Application satisfied the particularity requirement of the Fourth Amendment. As Judge Weisman pointed out, *McLamb* found adequate a warrant that allowed agents to obtain

identifying information “of any user or administrator who log[ged] into” an internet-based dark website where users could download or upload child pornography; in *McLamb*, there was probable cause to believe that anyone reaching the dark website was involved in possessing or trading child pornography, so that agents’ discretion was in fact limited to seizing information about individuals as to whom probable cause was established. (7/8/20 Order at 7-8.) Judge Weisman called that situation “the complete antithesis of the legal underpinning” of the Initial Application, in that:

The government has established probable cause that *one* user of a cellular telephone in the geofence area has committed a criminal offense. The warrant seeks to gather evidence on potentially *all* users of phones in the geofence, completely at the agents’ discretion.

(*Id.* at 8.)

Upon considering the government’s July 24 Application, in which the three-stage protocol was unchanged from the Initial Application, the Court adopted Judge Weisman’s reasoning and concluded that the July 24 Application’s proposed warrant contained the same defects, as to particularity, that Judge Weisman had identified in the 7/8/20 Order. (7/24/20 Order at 21-22.) The Court also concluded that although the government had added to the mix of information the existence of a stay-at-home order in place at the time of the two geofences then proposed for Location 2, the effect of that stay-at-home order on the number of device IDs and identities to be disclosed under the warrant was too speculative to change the analysis. (*Id.* at 23.)

Now, however, the government has changed the protocol significantly by dropping the third stage entirely. (Amended Application, Attachment B.) The government would receive only the “anonymized” device IDs and related information, and it would not have the authority – under the proposed warrant, at least – to compel Google to produce the subscriber information identifying the account holders of the devices identified by Google as having traversed any of the geofences. Further, the Amended Application seeks a warrant compelling Google to produce, in the second



stage, the “anonymized” list of unique device identifiers and related information “where such information identifies individuals who committed or witnessed the violations.” (*Id.*) The information the government states it is seeking to obtain through the proposed warrant is described as “[e]vidence and instrumentalities” of violations of the respective statutes the government views as having been violated, namely 21 U.S.C. § 829(e)(1) (dispensing a controlled substance without a valid prescription); 18 U.S.C. § 670 (the theft of medical products); 18 U.S.C. § 1341 (mail fraud); and 18 U.S.C. § 1343 (wire fraud). (*Id.*)

The elimination of the third stage of the process prompted the Court to ask the government to brief the question of whether the government, once it had the anonymized list of device IDs, could obtain the subscriber information identifying the account holder of those devices without further aid of a search warrant. (7/29/20 Order, D.E. 9.) The government answered in the affirmative, representing that it could lawfully obtain the identifying subscriber information from Google by subpoena. (Gov’t Br. at 16.) The government further represented that its ability to subpoena the identities of the device users does not mean that the government *would* do so, at least “without first looking at and analyzing the anonymized information it would receive from Google” if the Court grants the Amended Application. (*Id.* at 16-17.)

Finally, the government’s most recent changes to its application are significant for what they do not include. The government, although stating that the information seized is to be limited to that which “identifies individuals who committed or witnessed the violations,” has not explicitly limited the seized information to the identification of devices that showed up in more than one of the geofences, or in all three of them. Yet the government has represented to the Court that the anonymized information it would obtain under the proposed warrant in the Amended Application “would still be helpful to the government’s investigation because it (1) would show if the same

unique device ID was captured in more than one geofence referenced in Attachment A of the Amended Application; and (2) would also show the locations and timestamps of one or more devices during the Unknown Subject's receipt and shipment of the stolen prescription medication, which the government might be able to use to later identify the Unknown Subject." (*Id.* at 16.) The Court therefore understands that the government is aware of how the geofences could potentially be used to identify the Unknown Subject through the disclosure of device IDs for devices that show up in more than one of the geofences. The Court also interprets the government's position as suggesting that device IDs for device users other than the Unknown Subject would also be "helpful" to the investigation because the government could potentially identify those persons, investigate them for any connection to the Unknown Subject, and interview them about what they witnessed at Locations 1 or 2 on the dates and times when their devices were detected there. The foregoing passage of the government's brief thus sheds light on the government's goals with respect to obtaining location information that "identifies individuals who committed or witnessed the violations," although the proposed warrant is no more specific than those eight words about precisely how that caveat would operate if the proposed warrant is allowed.

**B. Fourth Amendment Analysis of the Amended Application**

The Court now proceeds to determine whether the Amended Application satisfies the Fourth Amendment's probable cause and particularity requirements. The Court is not aware of any federal decision addressing those issues with respect to a geofence warrant, and the Court has reason to believe that geofence warrants are facing their first round of judicial scrutiny.<sup>12</sup>

---

<sup>12</sup> David Uberti, "Police Requests for Google Users' Location Histories Face New Scrutiny," *The Wall Street Journal* (July 27, 2020) (<https://www.wsj.com/articles/police-requests-for-google-users-location-histories-face-new-scrutiny-11595842201>).

## 1. Probable Cause Determination

As proposed, the Amended Application continues to suffer from the same probable cause problem as did the earlier two applications. The government has argued that by dropping the third stage of its earlier three-stage protocol, its proposed warrant satisfies the probable cause requirement based on the following:

- Probable cause is established that the Unknown Subject “was involved in the receipt and shipment of stolen prescription medication” at Locations 1 and 2 within the time frames of the proposed geofences.
- There is a “fair probability” that Google possesses evidence related to “the receipt and sales of that stolen medication, given the general ‘pervasiveness’ and ‘indispensable’ nature of mobile telephones,” the nature of such electronic devices, the likelihood of their transmittal of location information to Google, and Google’s retention of that information.
- There also is a fair probability, then, that “anonymized information about the devices that were or could have been located at or close to [Locations 1 and 2] immediately before, during, and after the receipt and shipment of the stolen prescription medication is evidence of the Subject Offenses, namely, information about the device(s) the Unknown Subject used during those times.”

(Gov’t Br. at 10.) The Court agrees with these three propositions. (*See* 7/24/20 Order at 17.) But the analysis does not end there.

Further, the government argues that because it now seeks information about only the devices within the geofences, without the information identifying the users of those devices, the proposed warrant in the Amended Application is akin to a “tower dump,” in which the CSLI for multiple persons not known to the government at the outset of the search is disclosed to the government, based on such persons’ devices having been near or in contact with particular cell towers. (Gov’t Br. at 10-11.) The government relies on a recent Minnesota federal district court decision denying a motion to suppress CSLI obtained through tower dumps authorized by warrant. (*Id.*, citing *James*, 2018 WL 6566000, at \*4-5.) In *James*, in which the magistrate judge’s report and recommendation on the suppression motion was adopted in full by the district court, *James*,

2019 WL 325231, at \*1-3, the government obtained multiple search warrants for tower dumps from towers near the scenes of six robberies over a three-month period. 2018 WL 6566000, at \*1. The tower dump CSLI revealed that the same electronic device was near at least five of the six crime scenes, and this information led to the identification of the defendant. *Id.* In finding probable cause for these tower dumps, the *James* court found that there was a fair probability that the location data from the towers in question would “include” the cellular data related to the suspect in the robberies, and “that by cross-referencing the data, that individual could be identified.” *Id.* at \*4. In addition to arguing that the proposed warrant does not seek any individualized subscriber identity information, the government relies on *James* for the proposition that it has established probable cause not just to believe that the Unknown Subject’s device ID or identity will be revealed through execution of the proposed warrant, but also for “each device that was or could have been located within the three geofences referenced in Attachment A during the specified dates and times.” (Gov’t Br. at 12.)

The Court respectfully disagrees.

First, as to the proposed warrant’s requested authority for disclosure of just the anonymized information and not the actual subscriber records disclosing the identities of the account holders for those devices, the Court sees no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities. The government’s candor in disclosing that it does not need a search warrant to obtain the subscriber information, once armed with the device IDs and the lawful authority to subpoena the subscriber information (*see id.* at 16), is to be commended. The government even goes so far as to suggest that it will *not* subpoena

subscriber information for devices that, likely based on their time stamps, would not tend to identify the Unknown Subject or possible witnesses to his offense conduct at Locations 1 and 2. (*Id.*)

The Court does not suggest that the government intentionally seeks to make an end run around the Court's denial of the two earlier applications, but the principle that the government may not accomplish indirectly what it may not do directly is well-settled in the jurisprudence of constitutional rights.<sup>13</sup> The fact remains that the warrant as proposed in the Amended Application

---

<sup>13</sup> This principle finds judicial expression not only in the “unconstitutional conditions” doctrine involving public benefits, *see Planned Parenthood of Indiana, Inc. v. Commissioner of Indiana State Dept. Health*, 699 F.3d 962, 986 (7th Cir. 2012) (“Understood at its most basic level, the doctrine aims to prevent the government from achieving indirectly what the Constitution prevents it from achieving directly.”) (citing *Perry v. Sindermann*, 408 U.S. 593, 597 (1972)), but also in the context of applying constitutional rights in criminal cases, where the principle is part of the exclusionary rule prohibiting the admission of evidence obtained unconstitutionally:

An offshoot of the [exclusionary] rule is the “fruit of the poisonous tree” doctrine, which bars evidence which, though not obtained in the illegal search, was derived from information or items obtained in the search. *See Murray v. United States*, 487 U.S. 533, 536–37, 108 S. Ct. 2529, 2533, 101 L.Ed.2d 472 (1988) (doctrine “prohibits the introduction of derivative evidence, both tangible and testimonial, that is the product of the primary [illegally obtained] evidence”). The doctrine ensures that the government cannot achieve indirectly what it is forbidden to accomplish directly. As Justice Frankfurter articulated, “To forbid the direct use of methods but to put no curb on their full indirect use would only invite the very methods deemed inconsistent with ethical standards and destruction of personal liberty.” *Nardone v. United States*, 308 U.S. 338, 340, 60 S. Ct. 266, 267, 84 L.Ed. 307 (1939).

*United States v. Leake*, 95 F.3d 409, 411 (6th Cir. 1996). Federal courts also have applied the principle in multiple other contexts to limit government conduct that indirectly accomplishes some end that the government was barred from accomplishing directly by operation of a judicial ruling, a rule of criminal or civil procedure, or a contractual obligation in a criminal case. *See United States v McGann*, 951 F. Supp. 372, 379 (E.D.N.Y. 1997) (dismissing government's civil complaint where government was barred from bringing those claims in an earlier, separate action but included them in the complaint in the second action, as government had “attempt[ed] to accomplish indirectly what it could not accomplish directly. The law's response to such attempts is generally a negative one.”); *United States v. Barone*, 81 F. Supp. 1072, 1078 (E.D. Pa. 1991) (allowing criminal defendant to withdraw guilty plea where government had caused New Jersey to bring state criminal charges that the government was barred from bringing federally under the plea agreement); *United States v. Howell*, 466 F. Supp. 835, 837-38 (D. Ore. 1979) (denying government's application for search warrant seeking documents that the government could not obtain by grand jury subpoena because a judge had quashed the subpoena on grounds of Fifth Amendment production immunity); *United States v. Melvin*, 258 F. Supp. 252, 254 (S.D. Fla. 1966) (granting motion to suppress,

would authorize just such a move by compelling Google to disclose any device ID information the government requests, qualified only by the too-vague, eight-word caveat that the information is limited to that which “identifies the individuals who committed or witnessed the violations.” That caveat, conceivably, could be construed by Google to include *all* of the devices captured within the geofences, as Google would have no way of determining which of the devices traversing the geofences identify the Unknown Subject, any co-conspirators or accomplices,<sup>14</sup> or any witnesses, who could include anyone in the two business enterprises at the time of the geofences or anyone in the surrounding streets, parking lot, sidewalks, or other parameters (including the residential building in Location 1), as any such person conceivably could have happened past the Unknown Subject on their way in or out of the locations, or while their devices were or could have been in the locations. Google, again, would have no way of excluding device IDs based on whether the information identifies the offender(s) or any witness. Moreover, the utility of the warrant itself is practically indistinguishable from the three-stage protocol proposed in the first two applications: Once the government has the device IDs and time stamps, it may proceed to identify the users by subpoena, based entirely upon its own discretion. Without the Amended Application’s proposed warrant, the government would not be able to identify the device subscribers by subpoena, because it would have no way of knowing what devices to include in the subpoena. The proposed warrant, and the application of the geofence technology embedded in it, therefore give the government all the tools it needs to learn individuals’ location histories, which, as we have said, are treated here – in the government’s search warrant application – as information

---

in federal prosecution, evidence seized by state authorities in violation of federal Fourth Amendment standards, stating: “that which cannot be done directly cannot be accomplished indirectly”).

<sup>14</sup> As Judge Weisman was the first to observe, the proffered facts in support of probable cause nowhere indicate that accomplices or co-conspirators might be identified by the geofences. (*See* 7/8/20 Order at 5.)

that cannot be obtained without full Fourth Amendment compliance. (*See* 7/8/20 Order at 8 (denying Initial Application based on applicable Fourth Amendment standards and finding “no compelling reason to abandon Fourth Amendment principles in this case”).)

Second, with the Amended Application seeking a form of authority that will harness geofence technology to cause the disclosure of the identities of various persons whose Google-connected devices entered the geofences, the government must satisfy probable cause as to those persons. On the Amended Application now before the Court, along with the related briefing, the government has not established probable cause to believe that evidence of a crime will be found in the location history and identifying subscriber information of persons *other than the Unknown Subject*. There is likely a fair probability that the Amended Application’s proposed warrant will generate location information, and device IDs that are the functional equivalent of the identities of the device users, that will *include* the identification of the Unknown Subject and will thus *include* evidence of the crime, but it will include other information as well: The location information of persons not involved in the crime. The same appears to have been the case with the CSLI sought and obtained in *James* based on a probable cause analysis that failed to account for whether probable cause could exist as to these other persons. The analysis in *James* stops before reaching the question of whether probable cause could exist as to the CSLI of uninvolved persons and found probable cause for all of the seized information because there was probable cause to believe the offender’s CSLI was “include[d]” in what was to be seized. *James* is therefore unhelpful in the determination of probable cause here, where the information to be captured through the proposed geofence warrant will *include* the precise geographic location of persons as to whom no showing has been made as to their involvement in the offense or with the Unknown Subject.

The other decision upon which the government relies (Gov't Br. at 12), *Cellular Telephone Towers*, is similarly unhelpful. In *Cellular Telephone Towers*, the magistrate judge found probable cause for five tower dumps of CSLI over a four-minute period, based on the government's having demonstrated "that the subject of the investigation used a cell phone during the criminal activity and in furtherance of the offense," so that "there is a nexus between the telephone records sought and the criminal activity being investigated, especially in light of the narrow, specific date and time that are sought." 945 F. Supp. 2d at 771. But *Cellular Telephone Towers*, like *James*, stopped the analysis once the court found probable cause in the "nexus" between the offense and *all* the requested cell phone records, without analyzing whether probable cause existed to obtain all of those records. In *Cellular Telephone Towers*, the records to be received by the government amounted to "hundreds, or even thousands of telephone numbers for that time period, and the expectation is that the narrow criteria that they have developed will limit the relevant numbers to only about fifteen to twenty individuals who will then get further scrutiny." *Id.* In other words, probable cause was found for the CSLI of persons whose information and identities would need to be sorted through to find the information that was truly "relevant." Accordingly, the asserted probable cause for the search of location information of uninvolved device users resembles an argument that probable cause exists because those users were found in the place to be searched, i.e., the place as to which probable cause exists to believe the offense happened.

The U.S. Supreme Court rejected that very argument in *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), a case not discussed in *James* or *Cellular Telephone Towers*. Other federal decisions also have rejected warrants known as "all persons" warrants. See *Marks v Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996) (stating that "a warrant to search 'all persons present' for evidence of a crime may only be obtained when there is reason to believe that *all* those present will be participants in the



suspected criminal activity,” and that such warrants “might be appropriate for a different kind of locale – one dedicated exclusively to criminal activity”) (emphasis added); *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (“[A]n ‘all persons’ warrant can pass constitutional muster if the affidavit and information provided to the magistrate [judge] supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity.”). Decisions like *Marks* and *Owens* have allowed “all persons” warrants only when the affidavit establishes that there is probable cause to believe every person who entered the location engaged in the criminal activity.

No such predicate is established here. Here, the proposed warrant would admittedly capture the device IDs (from which the subscriber information could easily be derived with no further court authority) for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone – other than the Unknown Subject – entering those locations is involved in the subject offense or in any other crime.<sup>15</sup> As to Location 1, the proposed warrant will allow the seizure of location and identity information of any person whose Google-connected device entered the geofence around the commercial enterprise within the 45-minute window, as well as anyone with such a device who walked along the sidewalk outside the business or drove past the street next to it, or who was present in one of the residential units above the business and within the geofence. As to Location 2, the warrant would allow the seizure of the same information as to any Google-connected device user who entered the geofence around the

---

<sup>15</sup> The government’s unsuccessful reliance on *McLamb* before Judge Weisman (*see* Government’s Legal Memorandum in Support of Its Application for Google Geofence Search Warrant at 13, No. 20 M 297 (D.E. 3)), gives an inadvertent nod to this point. The search in *McLamb* was constitutional because there was probable cause to believe all persons in the child pornography dark website were engaging in criminal activity, but there is no such all-inclusive probable cause as to the persons whose location history and identifying information would be authorized to be seized under the Amended Application’s proposed warrant.

commercial enterprise during either of the 45-minute windows, including such persons who used the parking lot outside the business and any customers of the retail business that immediately abuts the parking lot (if they entered the parking lot and came within the boundaries or “margin of error” of the geofence), as well as drivers on the busy arterial street outside the business establishment but within the geofence or its “margin of error” boundaries at Location 2.

The Seventh Circuit has not yet spoken explicitly on “all persons” warrants, but *Ybarra* remains good law and remains instructive in the analysis of whether a warrant allowing a seizure of information about all persons who traverse the three geofences can pass constitutional muster. *Cf. Owens*, 372 F.3d at 275 (stating that *Ybarra* “sheds additional light on our analysis” of “all persons” warrants). In *Ybarra*, police obtained a warrant to search a public tavern and the bartender for narcotics, but the police expanded the warrant’s terms and searched a bar patron who was present there. 444 U.S. at 91. The Supreme Court held that a search of everyone in the bar, including the patron, violated the Fourth Amendment, concluding:

[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. 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*. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.

*Id.* (emphasis added) (citation omitted). In effect, the government in the Amended Application seeks the same type of authority, based only on device users’ “propinquity” to the crime scenes or to the Unknown Subject, that *Ybarra* held was not supported by individualized probable cause. Armed with the warrant it seeks, the government would have unlimited discretion to obtain from Google the device IDs (and derivative subscriber information) of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on

nothing other than the “propinquity” of these persons to the Unknown Subject at or near the time of Shipments 1, 2 and 3.

The Seventh Circuit’s treatment of *Ybarra* teaches us that more is required, or that at least some evidence of a person’s involvement in the suspected crime is required, in order for the Fourth Amendment to allow the seizure of that person – or, by analogy the seizure of that person’s things, such as location information, in which the person has a constitutionally protected expectation of privacy. See *United States v. McCauley*, 659 F.3d 645, 649-50 (7th Cir. 2011) (distinguishing *Ybarra*, in which officers knew “nothing in particular” about the defendant they searched, from matter in which officer knew that McCauley matched the defendant’s description and was identified by a witness as having participated in a beating hours earlier); *United States v. Reed*, 443 F.3d 600, 604 (7th Cir. 2006) (“[T]he totality of the circumstances in this case similarly leads to an inference of a common enterprise to which an innocent person would not likely be admitted.”); *United States v. Price*, 184 F.3d 637, 642 (7th Cir. 1999) (finding warrant complied with the Fourth Amendment where it was “not a sweeping search of everyone who happened to be on the premises – this was a search of one of four individuals who exited a car that was suspected of transporting cocaine”); *United States v. Pace*, 898 F.2d 1218, 1240 (7th Cir. 1990) (holding that probable cause existed to arrest suspects present in close proximity to drugs in a drug house maintained by a third person who could be assumed not to have entrusted unknowing persons to be in the drug house). Because the proposed warrant here seeks information on persons based on nothing other than their close proximity to the Unknown Subject at the time of the three suspect shipments, the Court cannot conclude that there is probable cause to believe that the location and identifying information of any of these *other* persons contains evidence of the offense.

**B. Particularity Determination**

The Supreme Court in *Ybarra* also cited the Fourth Amendment’s particularity requirement and the bar on general warrants for the proposition that “a warrant to search a place cannot normally be construed to authorize a search of each individual in that place.” 444 U.S. at 92 n.4. In denying the July 24 Application, this Court adopted Judge Weisman’s reasoning, as stated in the 7/8/20 Order, in finding that the proposed warrant in the July 24 Application, like the one appended to the Initial Application, was overbroad and failed to comply with the particularity requirement. (7/24/20 Order at 21-23, citing 7/8/20 Order at 4-8.) The Court finds the Amended Application similarly in violation of the particularity requirement, for the reasons stated below.

The government relies again on *James* for its argument that the Amended Application’s warrant satisfies the particularity requirement of the Fourth Amendment. (Gov’t Br. at 14-15.) The government notes that the proposed geofences here are “constrained both geographically and temporally to the receipt and shipment of stolen prescription medication that the government is investigating.” (*Id.* at 14.) In *James*, the magistrate judge described the challenged “tower dump” data as having been “constrained” in the same way and added that those “constraints” were justified by the nature of the investigation, given that multiple robberies had occurred in separate locations at specific times, likely by the same person. 2018 WL 6566000, at \*5. From there, the *James* court stated the following in support of its finding that the search warrants obtained for the tower dump met the particularity requirement:

The search warrants were not directed at general searches of the data from those towers, nor did they seek data from towers not geographically relevant to the locations of the robberies during the pertinent time periods, but were instead carefully tailored to the justification of the search—to identify a cellular phone used either in connection with the robberies or by the individual responsible for each of the robberies occurring at specific places and times matching the same *modus operandi*.

*Id.*, citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).<sup>16</sup>

This Court cannot agree that the particularity requirement is met here by virtue of the proposed geofences being narrowly tailored in a manner justified by the investigation. Attachment B to the proposed warrant, listing the items to be seized, does not identify any of the persons whose location information the government will obtain from Google. As such, the warrant puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences. A warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize, *Stanford*, 379 U.S. at 485, but the warrant here gives the executing officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the identifying subscriber information, and thus, those persons' location histories. *James* is unpersuasive on particularity, and the Court declines to follow *James*.

The Seventh Circuit's opinion in *Sanchez-Jara* offers far better guidance. In *Sanchez-Jara*, a defendant challenged the use of a cell-site simulator, where the search warrant had authorized the government to use the simulator to identify two specific phones and to follow those phones and thus determine the user's physical location or movements. 889 F.3d at 419, 421. The Seventh Circuit held that the warrants did not fail to meet the Fourth Amendment's particularity

---

<sup>16</sup> *James* did not discuss its reliance on *Garrison* any further. In *Garrison*, the Supreme Court held that information coming to light after a warrant's execution and revealing the warrant's authority to be "ambiguous in scope" does not render the warrant invalid under the particularity requirement, where there was no claim in *Garrison* that the persons or things to be seized were inadequately described, or that there was no probable cause to believe that those things might be found in the place to be searched as it was described in the warrant. 480 U.S. at 85. This Court does not find any support in *Garrison* for the idea that in this case, the proposed warrant sufficiently states the nature of the information to be seized, based on the notion that the warrant particularly states the time and place from where it is to be seized – no matter how narrowly tailored that time and place happens to be.

requirement: “[A] warrant authorizing the police to follow *an identified phone*, to see where it goes and what numbers it calls, particularly describes the evidence to be acquired” and “is not an open-ended authorization for public officials to rummage where they please in order to see what turns up.” *Id.* at 421 (emphasis added). The warrant upheld in *Sanchez-Jara* met the particularity requirement because it specified the phones to be identified by the simulator. But the proposed warrant in the Amended Application does not come close to doing so. Instead, it would authorize the seizure of the device IDs (and derivative subscriber information and associated location histories) of multiple devices, none of which is described in the warrant. The proposed warrant, like the two earlier applications, leaves to the executing officer’s discretion the identifying information that is to be obtained, based on the officer’s review of the device IDs and time stamps to determine not only which devices might belong to the Unknown Subject, but also those who might be witnesses to the offense. Accordingly, the proposed warrant is unlike the warrant approved in *Sanchez-Jara*, which suggests that where a warrant allows the tracking of a phone (and thus of a person) *not identified* in the warrant, not to mention such tracking of an unknown number of such persons, the warrant does not comply with the Fourth Amendment’s particularity requirement.

In addition, more needs to be said about the government’s eight words of qualifying language, in the proposed warrant’s Attachment B, purporting to limit Google’s production of the “anonymized” list of unique device IDs of Google-connected devices within the geofences (including their “margin of error”) to information which “identifies individuals who committed or witnessed the offense.” Coupled with the passage in the government’s brief stating that the government would not necessarily subpoena the identifying subscriber information of the devices on the anonymized list “without first looking at and analyzing the anonymized information it

would receive from Google” under the warrant, and with the government’s representation that the anonymized information would show if the same unique device ID “was captured in more than one geofence” (Gov’t Br. at 16-17), the eight words at the end of Attachment B might be read to indicate that the warrant seeks to obtain from Google only the anonymized information of devices that do appear in more than one of the geofences. But the proposed warrant is not that clear because it makes no mention of cross-referencing device IDs in the respective geofences. The Court cannot resort to the government’s brief for greater clarity, even if the brief supplied such clarity (and it does not), because the scope of the warrant must be stated in the warrant itself. Moreover, even in the brief, the government adds that the anonymized information “would also show the locations and timestamps of one or more devices during the Unknown Subject’s receipt and shipment of the stolen pharmaceutical medication, which the government might use to later identify the Unknown Subject.” (*Id.* at 16.) In the warrant, the eight words of limitation include information not just identifying “individuals who committed ... the offense,” which might be an oblique description of cross-referencing, but also identifying “individuals ... who witnessed the offense.” The warrant spells out no procedure at all for Google to figure out who may have witnessed the offense other than to turn over all device IDs within the geofences and their “margin(s) of error.”

Accordingly, the warrant requested in the Amended Application does not do what Judge Weisman initially suggested might pass muster in the 7/8/20 Order, namely that the warrant authorize the government to obtain “the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three geofences ....” (7/8/20 Order at 8.) The likelihood of the same device showing up in more than one of these three geofences is extremely low, indicating that probable cause may well exist for the government to seize the device ID, location information, and identifying subscriber information of devices present at more than

one of the geofences, or in all three. The government may well be able to describe, with the requisite Fourth Amendment particularity, the device IDs (and their corresponding subscriber information) as those for devices present in two or three of the geofences. It is also possible to imagine other applications of geofence technology that might comport with Fourth Amendment standards. Say, for example, that the government develops information supporting probable cause to believe that its geofences will not capture the information of uninvolved persons, such as a scenario in which the government can establish independently that only the suspected offender(s) would be found in the geofence, or where probable cause to commit an offense could be found as to all present there. Those scenarios might be similar to one in which a geofence warrant generates identifying and location information only of persons as to whom probable cause can be established because the warrant yields disclosure only as to devices present in multiple geofence times and locations. But the proposed warrant would grant the government far greater discretion, namely, to sort through the location information and derivative identifying information of multiple people to identify the suspect by process of elimination. This amount of discretion is too great to comply with the particularity requirement, and the proposed warrant thus suffers from the same fatal particularity flaw as did the proposed warrants in the first two applications.

### CONCLUSION

The technological capability of law enforcement to gather information, from service providers like Google and others, continues to grow, as demonstrated here by the Amended Application. Our appeals court has recognized, for quite some time now, that “[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive.” *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007). In *Carpenter* and *Riley*, the Supreme Court recognized that as the use of mobile electronic devices

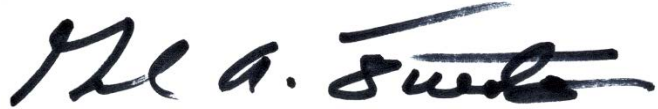


becomes more and more ubiquitous, the privacy interests of the general public using these devices, including the privacy interest in a person's physical location at a particular point in time, warrants protection. 138 S. Ct at 2217; *see Riley*, 573 U.S. at 393. Longstanding Fourth Amendment principles of probable cause and particularity govern this case, and the technological advances making possible the government's seizure of the type of personal information sought in this case must not diminish the force and scope of Fourth Amendment protections with roots in the reviled abuses of colonial times. Simply because Google *can* collect this information, or because the government *can* obtain it from Google under a "constrained" approach "justified" by the investigation's parameters, does not mean that the approach clears the hurdles of Fourth Amendment probable cause and particularity. But nor does the Court intend to suggest that geofence warrants are categorically unconstitutional. Each specific proposed application must comply with longstanding Fourth Amendment constitutional protections of individual privacy rights, which should not be diminished by increased technical capability for intrusion, or by how effective those capabilities might be at solving crimes. The potential to use Google's capabilities to identify a wrongdoer by identifying everyone (or nearly everyone) at the time and place of a crime may be tempting. But if the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to "rummage where they please in order to see what turns up," *Sanchez-Jara*, 889 F.3d at 421, even if they have reason to believe something will turn up, a federal court in the United States of America should not permit the intrusion. Nowhere in Fourth Amendment jurisprudence has the end been held to justify unconstitutional means.

For the foregoing reasons, and by applying the Fourth Amendment to the government's proposed warrant in the Amended Application, the Court must deny the Amended Application and the warrant requested under it.<sup>17</sup>

**SO ORDERED.**

**ENTER:**

A handwritten signature in black ink, appearing to read "G. A. Fuentes", written over a horizontal line.

**GABRIEL A. FUENTES**  
**United States Magistrate Judge**

**DATED: August 24, 2020**

---

<sup>17</sup> This Memorandum Opinion and Order was issued initially on August 17, 2020, in a document filed under seal (Sealed Memorandum Opinion and Order, D.E. 11). The government having not objected to the unsealing of that opinion, this unsealed Memorandum Opinion and Order has been issued on today's date.