IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR SUPPRESSION OF EVIDENCE OBTAINED PURSUANT TO GOOGLE GEOFENCE WARRANT

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's supplemental motion to suppress evidence obtained from Google, LLC ("Google") pursuant to a search warrant for GeoFence location information (the "GeoFence warrant"). ECF No. 104. This Court should deny the defendant's motion for three reasons. First, investigators did not infringe the defendant's reasonable expectation of privacy when they obtained this information from Google. Second, the GeoFence warrant complied with the Fourth Amendment, as it was issued based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. INTRODUCTION

Agents investigating the armed robbery of the Midlothian Call Federal Credit Union had good reason to believe that Google was a witness and had evidence of the crime: surveillance video showed the robber with a cell phone, and investigators knew that there was therefore a fair probability that Google had stored the robber's cell phone location information. They also knew that Google likely had other location information that would provide them with a fuller understanding of the time and place of the events of the robbery, as well as help them identify

other witnesses and suspects. Federal Bureau of Investigation Task Force Officer Josh Hylton put these facts in an affidavit, and he obtained a GeoFence search warrant for a narrowly focused set of evidence: a two-hour interval of Google location information (and associated identity information) for devices that Google's records placed within 150 meters of a point near the bank during the hour of the robbery. *See* ECF No. 54-1.

The investigators were correct: Google had been a witness to the robbery. Pursuant to the warrant, Google produced to the United States a small set of records: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. This information was sufficient for investigators to recognize that the defendant's Google account likely belonged to the robber, and subsequent investigation led to his indictment.

The defendant argues that the Fourth Amendment bars Google from being a witness in an investigation like this one: that even where a judge finds probable cause to believe that Google has evidence concerning unidentified individuals present at the scene of a serious crime, the Fourth Amendment bars issuance of a warrant to obtain that evidence. Fortunately, the defendant is wrong, and his arguments that the United States violated the Fourth Amendment by obtaining his location information are without merit.

II. BACKGROUND

The United States' initial Response in Opposition to Defendant's Motion for Suppression sets forth the basic facts of the bank robbery, the GeoFence Affidavit, the GeoFence Warrant, and the warrant's execution. *See* ECF No. 41 at 1-5. In addition, Google has now submitted two affidavits relevant to the defendant's motion. *See* ECF No. 96. The United States and the defendant have agreed to stipulate to the accuracy of these affidavits. One, by Google Location

History Product Manager Marlo McGriff, describes the Google Location History service, including steps the defendant took to opt in to Google's storage of his location information. *See* ECF No. 96-1. The other, by Google Team Lead for Legal Investigations Support Sarah Rodriguez, provides further information about the execution of the GeoFence warrant. *See* ECF No. 96-2. The United States will not repeat these facts here, but will reference them below in explaining why the GeoFence warrant was consistent with the Fourth Amendment. In addition, the arguments made now by the defendant remain similar to his initial suppression arguments. The United States therefore incorporates by reference the arguments made in its initial opposition to the defendant's suppression motion and in its response to the Google amicus brief. *See* ECF No 41 at 6-24; ECF No. 71 at 1-9.

III. ARGUMENT

A. The Defendant Had No Reasonable Expectation of Privacy in Two Hours of Google Location Information

It is a fundamental Fourth Amendment principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the government. This principle has deep roots: when an individual discloses information to a third party, the third party becomes a witness, and it is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixon*, 418 U.S. 683, 709 (1974). The Supreme Court has repeatedly rejected Fourth Amendment arguments contrary to this principle in cases ranging from private conversations to business records. *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (statements made in the presence of an informant); *Couch v. United States*, 409 U.S. 322, 335-36 (1973) (information disclosed to an accountant); *United States v. Miller*, 425 U.S. 435, 443 (1976) (bank records); *Smith v. Maryland*, 442 U.S. 735, 742-44

(1979) (dialed telephone numbers); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (financial records).

Based on this fundamental principle, the defendant had no reasonable expectation of privacy in the location information he disclosed to Google. As discussed below, the multiple steps that the defendant took to opt in to Google's receipt and storage of his location information confirm this result. But even without the defendant's explicit agreement to disclose his location information to Google, the defendant's voluntary disclosure of his location would be evident from the nature of the services Google provides to customers. Courts often infer that information is voluntarily disclosed to a third party based on the nature of the relationship between the third party and the one making the disclosure. For example, in *Miller*, the Supreme Court did not need to consider Miller's explicit agreements with his bank in order to conclude that he had voluntarily disclosed his financial information. Instead, the Court's conclusion was based on "examin[ing] the nature of the particular documents sought" and concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442. Similarly, the Supreme Court's analysis of the disclosure of dialed phone numbers in *Smith v. Maryland* began by observing that telephone users "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Smith v. Maryland*, 442 U.S. at 742.

Here, similar analysis demonstrates that the defendant voluntarily disclosed his location information to Google. Google does far more than provide a storage service for its customers' location information. Instead, Google customers disclose their location to Google to obtain location-based services such as mapping, traffic updates, and help finding their phones. *See* ECF No. 96-1 at 2. For example, customers who use Google's mapping services to assist them with

driving from one place to another realize that they must convey their location to Google. Thus, because the defendant provided his location to Google to obtain its location-based services, the United States did not infringe his reasonable expectation of privacy when Google conveyed that information to the United States.

The fact that the defendant voluntarily disclosed his location information to Google is confirmed and reinforced by the multiple steps he took to enable Google to obtain and store his location. The McGriff affidavit establishes that Google users "must explicitly opt in to the [Location History] service." ECF No. 96-1 at 2. McGriff sets forth the multiple steps that a user must take before Google stores the user's Location History: Location History "functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it." ECF No. 96-1 at 3.

The McGriff affidavit further explains both that Google users may delete their location information and that users are informed of this fact in the Google Privacy Policy. *See* ECF No. 96-1 at 5. Google's Privacy Policy also explains to users that Google has access to their location information for purposes ranging from providing them with targeted advertising or driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). The defendant concedes that he "agree[d] to Google's terms and conditions during the initial setup process of his phone." ECF No. 104 at 19. As part of these terms and conditions, he agreed that Google could use his data "data in accordance with our privacy policies." *See* October 25, 2017, Google Terms of Service (available

at https://policies.google.com/terms/archive/20171025).

These facts confirm that the defendant voluntarily conveyed his location information to Google. Significantly, they also distinguish with respect to voluntary disclosure the location information here from the cell-site records of *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected "without any affirmative act on the part of the user beyond powering up," because "there is no way to avoid leaving behind a trail of location data," and because carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store the defendant's location without his undertaking multiple affirmative acts. He had to opt in to Location History in his account settings, and he had to enable Location Reporting for his phone. *See* ECF No. 96-1 at 3. The defendant had discretion regarding whether Google stored his location information, and he retained the ability to delete it. *See* ECF No. 96-1 at 5. And none of the services associated with Google's storage of location information are indispensable to participation in modern society. The defendant thus voluntarily disclosed his location information to Google, and Google's conveyance of that information to the United States did not infringe his reasonable expectation of privacy.

The defendant makes multiple arguments in support of his claim that he had a reasonable expectation of privacy in the location information he disclosed to Google. All of them lack merit.

First, the defendant argues that *Carpenter* protects even the brief period of his location information obtained by investigators. *See* ECF No. 104 at 10-11. But this argument ignores both *Carpenter*'s explicit limitations and its reasoning. As an initial matter, the Court in *Carpenter* did not abolish the third-party doctrine or "disturb the application of *Smith* and *Miller*." *Carpenter*,

138 S. Ct. at 2220. Thus, because the defendant voluntarily disclosed his location to Google under the reasoning of *Carpenter*, the government did not conduct a search when it obtained his location information.

Even absent the third-party doctrine, *Carpenter* does not support the defendant's claim that obtaining two hours of his location information was a search. *Carpenter* protects only a privacy interest in long-term, comprehensive location information. The Court explicitly limited its holding to its conclusion "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 U.S. at 2217 n.3. The Court emphasized that *Carpenter* was "not about 'using a phone' or a person's movement at a particular time." *Carpenter*, 138 U.S. at 2220. Instead, it was "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* The government conducted a search in *Carpenter* because the cell-site records the government obtained created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. By this standard, the government did not conduct a search when it obtained only two hours of the defendant's location information pursuant to the GeoFence warrant.

Significantly, although the Supreme Court decided *Carpenter* nearly two years ago, the defendant fails to cite a single case interpreting *Carpenter* broadly to protect a brief period of location information. Instead, courts have agreed that *Carpenter* protects only long-term, comprehensive location information. *See, e.g.*, *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))" (emphasis in original)); *Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) ("[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest

which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case."); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under *Carpenter* because "the information in the database did not reveal 'the whole of [Yang's] physical movements.'").[1]

Second, the defendant continues to cite the fact that the United States obtained location information regarding other Google users, *see* ECF No. 104 at 12, but he still provides no explanation of how this fact supports his claim that he had a reasonable expectation of privacy in his location information. Such an argument would be foreclosed by Supreme Court precedent. The Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Courts have agreed that defendants lack standing to challenge the government obtaining others' cell phone location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016); *United States v. Forest*, 355 F.3d 942, 948 (6th Cir. 2004), *vacated on other grounds by* 543 U.S. 1100 (2005) (vacating in light of *United States v. Booker*, 543 U.S. 220 (2005)).

[1] The defendant also cites *United States v. Karo*, 468 U.S. 705 (1984), for the proposition that the government conducts a search when it obtains "information about the interior of a constitutionally-protected space, such as a home." ECF No. 104 at 11. However, both *Smith v. Maryland* and *Hoffa* demonstrate that the government does not conduct a search when it obtains information voluntarily disclosed to another from within a protected space and then conveyed by that party to the government. *Smith v. Maryland*, 442 U.S. at 743; *Hoffa*, 385 U.S. at 301. Moreover, the defendant does not claim that the GeoFence warrant revealed any such information about him.

Third, the defendant argues that he has a reasonable expectation of privacy in the location information he disclosed to Google because Google considers it to be "'contents' for purposes of the Stored Communications Act." ECF No. 104 at 12. As the United States previously explained, Google's analysis of how the Stored Communications Act applies to location information may be incorrect. *See* ECF No. 71 at 8. But regardless, the statutory classification of Google's location information does not affect whether a user has a reasonable expectation of privacy in it. As *Hoffa* demonstrates, one has no reasonable expectation of privacy in the contents of communications disclosed to a third party when the third party conveys that information to the government. *See Hoffa*, 385 U.S. at 302. Here, because the defendant conveyed his location information to Google to obtain location-based services, his Fourth Amendment rights were not infringed when Google conveyed that information to the United States.

Fourth, the defendant argues that his Google location information should be protected because "it is at least as accurate" as the cell-site information in *Carpenter* and thus "capable of revealing the 'privacies of life.'" ECF No. 104 at 13. The United States agrees that the Google information here was at least as accurate as the cell-site information in *Carpenter*, but *Carpenter* nevertheless does not protect it both because of its short duration and because the defendant disclosed it to Google.

Fifth, despite the defendant's stipulation to the Google affidavits, he attempts to argue that he did not voluntarily disclose his location information to Google. *See* ECF No. 104 at 15-17. As an initial matter, the defendant's argument that he did not voluntarily disclose his location focuses entirely on the opt-in procedures for Google's storage of location information. He thus ignores that his voluntary disclosure of location information to Google is evident from the nature of the

location-based services (like mapping) that Google provided him.[2]

The defendant bases his argument that he did not voluntarily disclose his location information to Google in large part not on the McGriff affidavit, but instead on his own description of the setup process for an Android phone. *See* ECF No. 104 at 15-17. As an initial matter, the United States does not believe that the steps described by the defendant fully and accurately describe the steps he would have taken to create a Google account, set up the phone he used at the time of the robbery, and opt in to Google Location History. For example, the defendant does not address the steps involved in the initial creation of his Google account or signing into that account using his phone.

Nevertheless, assuming for the sake of argument that the defendant's description of his cell phone setup process is accurate, the defendant voluntarily disclosed his location information to Google. The defendant concedes that during setup, a screen on his phone informed him that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." ECF No. 104 at 15. He does not dispute that in response to this warning, he clicked "YES I'M IN." *See id.* He also concedes that this screen of his phone linked to a web page containing Google's Terms of Service and Privacy Policy, *see id.* At 15-16, which describe

[2] Although the defendant might object that a user of Google's location-based services cannot tell that Google will store her location information, the Supreme Court held in *Smith v. Maryland* that the third-party doctrine applies to information voluntarily disclosed to a third party regardless of any expectations regarding subsequent storage. In *Smith*, the defendant argued that the third-party doctrine should not apply to his dialed numbers because the phone company did not usually store information concerning local phone calls. The Supreme Court rejected his argument: "The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record." *Smith*, 442 U.S. at 745. Thus, the defendant would have no reasonable expectation of privacy in information he disclosed to Google even if he had not been informed that Google would store that information.

Google's use, storage, and deletion of location information. He further concedes that he "would have had to agree" to these terms and conditions. ECF No. 104 at 19.

These concessions are fatal to the defendant's argument that he did not voluntarily disclose his location information to Google. The defendant attempts to evade the consequences of his agreements through an argument worthy of Goldilocks: that the language on his phone screen was too short, and that the Terms of Service and Privacy Policy were too long. He complains that the language on his phone screen did not use the phrase "Location History" or inform him "of the privacy implications of turning it on," and he complains that the Privacy Policy was "27 pages long." *See* ECF No. 104 at 15-16. But the language on his phone screen was just right—in brief, clear language, it informed him of what Google would do: periodically store his location to provide him with services. Moreover, the Supreme Court has never limited voluntary disclosure under the third-party doctrine to circumstances where one is informed of the Fourth Amendment implications of disclosure. And the Privacy Policy was also just right, because it gave the defendant the opportunity to obtain a more detailed explanation of Google's use and storage of his location information.

Sixth and finally, the defendant cites cases addressing whether Internet Terms of Service create binding contacts, including a case within this district enforcing such a contract. *See* ECF No. 104 at 18-20 (citing *Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033 (E.D. Va. Jan. 28, 2020)). Although Google's Terms of Service likely creates a binding contract with customers, the defendant cites no cases holding that this contracts question plays any role in determining whether information is voluntarily disclosed to a third party for Fourth Amendment purposes. For example, the Supreme Court in *Smith v. Maryland* relied on statements in phone books to support its conclusion that "telephone users realize that they must 'convey' phone numbers to the telephone

company," *Smith v. Maryland*, 442 U.S. at 742-43, but phone book statements are not likely part of a contract between a phone company and its customers.

Moreover, courts rely on terms of service in evaluating whether a service provider's disclosure of information to the government violates the Fourth Amendment. *See, e.g.*, *Adkinson*, 916 F.3d at 610 (holding that that T-Mobile's disclosure of cell-site information to the government did not violate Adkinson's Fourth Amendment rights because Adkinson "agreed to T-Mobile's policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests, property, or safety"). Here, the defendant agreed that in order to obtain Google's location-based services, he would share his location with Google, and he chose for Google to store it. Google's conveyance of that information to investigators did not infringe his reasonable expectation of privacy.[3]

B. The Fourth Amendment's Protection of Property Does Not Restrict Google from Conveying to the United States Information Disclosed to it by the Defendant

The defendant continues to argue that obtaining location records from Google was a search under "a property based theory," *See* ECF No. 104 at 20, but his argument flies in the face of the fundamental principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443. The Supreme Court has recognized that a physical trespass for purposes of obtaining

[3] The defendant also cites European complaints regarding Google's storage of location information. For example, the defendant cites a complaint by a Norwegian individual whose name is redacted in which that unknown person alleges that Google "uses different means to nudge the user into turning on" Location History. *See* ECF No. 104 at 17 (citing complaint available at https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf). Here, where this Court has the benefit of an expert from Google, as well as experts provided by the United States and the defense, this Court should not rely on unproven allegations from an anonymous person abroad.

information is a search. *See United States v. Jones*, 565 U.S. 400, 404-05 (2012). But the investigation in this case involved no physical trespass; instead, the GeoFence warrant directed Google to produce specified information that its customers had disclosed to it. The defendant cites no case—and the United States is aware of no case—in which a court has relied on a "property-based theory" to discard the third-party doctrine of *Smith* and *Miller* or prevent witnesses from providing evidence to the government. Justice Gorsuch's solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on some sort of property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding law.

In addition, the defendant's assertion that Google is a "mere bailee" of location information ignores how Google uses location information to provide services to its customers. ECF No. 104 at 20. Google does not merely store its customers' locations; it uses that information to provide location-based services. *See* ECF No. 96-1 at 2. Under these circumstances, Google's disclosure of its customers' location information to investigators does not implicate the Fourth Amendment. For example, the owner of documents may retain a property interest in documents shared with an accountant, but the owner's Fourth Amendment rights are not infringed when the accountant conveys them to the government. *See Couch*, 409 U.S. at 335.

C. The GeoFence Search Warrant Satisfied the Fourth Amendment

The GeoFence warrant satisfied the Fourth Amendment because it was issued on a showing of probable cause and specified its object with particularity. The defendant's arguments that the search warrant did not "meet the probable cause or particularity requirements demanded by the Fourth Amendment" are without merit. ECF No. 104 at 22.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). Here, the affidavit in support of the Geofence warrant established an ample basis for the issuing magistrate's finding of probable cause. In particular, the affidavit established: (1) that an unknown subject committed an armed bank robbery at a particular place and time; (2) that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) that the majority of cell phones were smartphones; (4) that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (5) that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." State GeoFence Warrant at 4-5. From this information, there was a substantial basis for the magistrate to find probable cause to believe that Google possessed evidence related to the robbery.

The defendant argues that the warrant lacked probable cause because it "did not identify any individuals or accounts to be searched because investigators did not know who they were searching for, or even if Google would have relevant data." ECF No. 104 at 22. However, a warrant for evidence of crime need not identify specific individuals or establish with certainty that evidence will be found—all it must do is establish a fair probability that specified evidence will be found in the place to be searched. Indeed, the warrant here is similar in this respect to the search warrant approved by the Supreme Court in *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978), which authorized seizure from a newspaper of photographs of unidentified individuals who had

assaulted police officers.

The defendant also ignores the standard for probable cause when he argues that probable cause was lacking because "the application rested on broad conjecture based on the popularity of Google and cell phones generally." ECF No. 104 at 22. As an initial matter, the affidavit included specific facts supporting the finding of probable cause, including the robbery itself and that the armed robber had a cell phone. Moreover, it is entirely appropriate in the Fourth Amendment context to rely in part on probabilistic inferences. For example, *in United States v. James*, No. 18-cr-216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019), the court relied on inferences about cell phone use to conclude that a warrant for a cell tower dump was based on probable cause, even though it was "unknown whether a phone was used by the suspect before or after the robbery."[4] As required by the Fourth Amendment, the GeoFence affidavit established a fair probability that Google had evidence pertaining to the robbery.

2. The GeoFence Warrant Was Not Overbroad

Under the Fourth Amendment, "a valid warrant must particularly describe the place to be searched, and the persons or things to be seized." *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). The Fourth Amendment constrains a warrant so that it is "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). It protects against "exploratory rummaging in a person's belongings." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v.*

[4] The recent Supreme Court case *Kansas v. Glover*, 140 S. Ct. 1183 (2020), provides an example of the Court upholding probabilistic reasoning in the Fourth Amendment context. The Court held that a police officer had properly made a "commonsense inference" that the owner of a vehicle was likely its driver. *Id.* at 1188. *See also Illinois v. Gates*, 462 U.S at 240 (noting the authority of a magistrate issuing a search warrant "to draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant").

Maryland, 427 U.S. 463, 480 (1976)). Moreover, the test "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)).

Here, the GeoFence warrant was limited based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of an armed robbery during a one-hour interval. The warrant was appropriate for its investigatory purpose, which was to obtain evidence to help identify and convict the robber. The warrant's breadth is also supported by *James*, in which the district court held that a cell tower dump warrant was sufficiently limited because it was constrained geographically and temporally to robberies under investigation. *James*, 2019 WL 325231 at *3. The GeoFence warrant here is narrower than the warrant upheld in *James*: its geographical area was smaller than a cell site, and it produced information about only 19 individuals, as opposed to "hundreds if not thousands." *Id.*

The defendant argues that the GeoFence warrant was overbroad because Google reviewed a large body of data in order to comply with it, *see* ECF No. 104 at 22-24, but this argument is without merit. He cites no case law holding that a service provider may not review a large data set in order to produce a narrowly defined set of information. Such process is not new: for example, phone companies may review every call made by all their customers in order to find calls made to a specified phone number. *See Ameritech Corp. v. McCann*, 403 F.3d 908, 910 (7th Cir. 2005). GeoFence warrants are also similar to tower dump warrants: they determine who was present at a particular place and a particular time. If the cell tower is in a busy area, a large set of customers may have used the tower; the phone company in response to the warrant must search

within that data for those who used the tower at the specified time.

Google's review of a large set of data to comply with the GeoFence warrant is a result of Google's internal data storage practices, not an overbroad warrant. It would be possible for Google to create an additional Location History database indexed by location. This database would enable Google to comply with a GeoFence warrant—and produce the exact same data as Google currently produces—without reviewing the data of all customers. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices which are invisible to customers and the government alike. Thus, the appropriate measure for the breadth of the GeoFence warrant is the limited data sought by the warrant, which resulted in the government obtaining location information for only 19 individuals, all of whom were near the bank at the time of the robbery.

3. The GeoFence Warrant Was Sufficiently Particular

The defendant next argues that the GeoFence warrant was insufficiently particular because of its three-step process, but the defendant's arguments are mistaken. First, the defendant complains that "Google decided to search only a portion of its records, specifically 'Location History' records." *See* ECF No. 104 at 25. As an initial matter, even if Google should have reviewed additional databases for responsive information, Google's failure to do so would not demonstrate any infirmity in the warrant or infringe the defendant's Fourth Amendment interests. No Stored Communications Act warrant has even been written that a service provider cannot botch, but a service provider's failure to produce a portion of the information sought pursuant to a warrant does not violate the Fourth Amendment. But as Google explains, it did nothing wrong: Location History was "the only form of location data Google maintains that Google believes to be responsive to a geofence request." McGriff Affidavit at 7. Google's review and production of the

information that it believed fell within the scope of the warrant does not make the warrant insufficiently particular. There was no reason for Google to review information it had concluded was nonresponsive to the warrant. [5]

Second, the defendant complains that Google's response to the warrant was not dependent on Google's estimates of the margins of error associated with its location calculations. *See* ECF No. 104 at 25. It is certainly true that no cell phone location measurement has perfect accuracy. However, a warrant that does not adopt a probabilistic approach to all location information is not insufficiently particular. Here, the warrant directed Google to disclose information for devices "inside the described geographical area" during the time of the robbery, and Google correctly interpreted this to mean it should disclose information concerning devices that its calculations placed within the circle specified by the warrant. Although there always remains a possibility of inaccuracy in Google's location information, and a defendant may certainly challenge at trial the weight given to this information, the possibility of inaccuracy does not make a warrant insufficiently particular.[6]

Third, the defendant argues that the warrant was insufficiently particular based on the correspondence between Google and FBI TFO Josh Hylton regarding step 2 of the warrant, but

[5] Elsewhere in his motion, the defendant states that the 'warrant required Google to produce location data for 'each type' of Google account," and he faults Google for not producing data from the Web & App Activity or Google Location Accuracy databases. ECF No. 104 at 7. The defendant has misinterpreted the GeoFence warrant: Web & App Activity and Google Location Accuracy are separate Google services, not separate types of Google accounts.

[6] The defendant does not dispute that his Google location information would have fallen within the scope of the warrant regardless of how the warrant addressed the uncertainty associated with it. Instead, the defendant highlights a single Google measurement of someone else's phone with a margin of error of 387 meters. *See* ECF No. 104 at 25. Another measurement associated with that person's device, however, had a margin of error of only 84 meters, placing the device within the GeoFence region.

this correspondence provides no evidence that the warrant lacked particularity. *See* ECF No. 104 at 25-26. The warrant was sufficiently particular because it specified the evidence law enforcement was authorized to obtain: two hours of location data (and associated identity information) for all individuals present at the site of the robbery during the hour of the robbery. The step 2 correspondence addresses an entirely separate issue: FBI TFO Hylton's decision to obtain less than the maximum amount of information authorized by the warrant. The Fourth Amendment requires that the information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Indeed, a contrary rule would be perverse: agents executing warrants would be required to engage in more invasive searches than they deemed necessary, simply because they had previously established probable cause for additional evidence.

Agents executing warrants often make choices about the intensity of their execution of a search warrant, and it is not a Fourth Amendment violation if they ultimately leave some evidence behind. The Playpen warrant explicitly included such a provision: it authorized a search of the computer of everyone who visited a specified child pornography web site, but it also stated that "in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016). Courts uniformly agreed that this provision did not violate the Fourth Amendment's particularity requirement. *See, e.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016) ("[T]he fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site"). The defendant attempts to distinguish the Playpen warrant based on its breadth, *see* ECF No. 104 at 23-24, but the United

States cites the Playpen warrant for an entirely different proposition: that it is permissible for a warrant to authorize investigators to seize less than the maximum amount of evidence for which they have established probable cause and which the warrant describes with particularity. FBI TFO Hylton did not violate the Fourth Amendment when he executed the warrant in a manner that provided additional privacy protections for the majority of individuals present at the robbery. [7]

Nor was there anything improper about FBI TFO Hylton's correspondence with Google, in which he ultimately requested that Google produce step 2 location information about nine individuals. Google remains an independent actor, and courts have held that a provider like Google has a due process right to object to an order directing it to comply with a search warrant. *See, e.g.*, *In re Application*, 610 F.2d 1148, 1157 (3d Cir. 1979). Where a service provider produces a portion of the information specified by legal process, the United States does not violate the Fourth Amendment when it chooses not to litigate over the rest. A contrary rule would waste judicial resources and harm privacy. Nothing in the execution of the GeoFence warrant supports the defendant's argument that the warrant was insufficiently particular.

Finally, arguing that "every person takes a 'unique path through life,'" the defendant also faults the warrant for stating that the information produced by Google in step 1 and step 2 would be "anonymized." ECF No. 104 at 27. In the context of the GeoFence warrant, however, "anonymized information" refers to the fact that Google did not produce its subscriber identity information associated with the location information until step 3 of the warrant. The GeoFence warrant's use of the phrase "anonymized information" does nothing to make the warrant insufficiently particular.

[7] As argued in its initial opposition to the defendant's suppression motion, if the three-step process for the GeoFence warrant were insufficiently particular, the proper remedy would be to sever the second step. *See* ECF No. 41 at 20-21.

D. Evidence from the GeoFence Warrant Should Not Be Suppressed Because Investigators Relied upon it in Good Faith

Even assuming the GeoFence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. In its response to the defendant's initial suppression motion, the United States explained that the good faith exception precluded suppression in this case both under the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), and under the Fourth Circuit's standard in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), for good-faith reliance on a search warrant authorizing use of a novel investigative technique. *See* ECF No. 41 at 21-24. The United States will not repeat these arguments here, but they remain fully applicable to the defendant's supplemental motion.

The defendant now advances an additional argument against the good faith exception: he claims that the good-faith exception should not apply here because the GeoFence affidavit omitted "the true scope of the number of people to be searched and the true boundaries of the 'geofence.'" ECF No. 104 at 28. To challenge a search warrant on this basis, the defendant would be required to show "(1) that the officer deliberately or recklessly omitted the information at issue and (2) that the inclusion of this information would have defeated probable cause." *United States v. Andrews*, 577 F.3d 231, 238-39 (4th Cir. 2009). Here, the defendant's argument fails because he cannot satisfy either of these requirements.

To begin, the information that the defendant asserts should have been included in the warrant would not have defeated probable cause. First, information about Google's internal data structures and how it processes GeoFence warrants has nothing to do with either the probable cause that supported the warrant or the information that the warrant authorized to be seized. Instead, it relates to how the warrant was executed, and the Supreme Court has held that "[n]othing in the

language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the three requirements discussed above [a neutral magistrate, probable cause, and particularity], search warrants also must include a specification of the precise manner in which they are to be executed." *Dalia v. United States*, 441 U.S. 238, 257 (1979). Regardless of how Google organized its databases or executed the warrant, the affidavit established a fair probability that Google had evidence of the location of the armed robber and others at the time of the robbery. Similarly, the fact that there is some margin of error in all service provider cell phone location information does not undermine probable cause or particularity: the affidavit still would have established a fair probability that Google stored location information of the robber and other nearby witnesses.[8]

Nor can the defendant establish that any omission by FBI TFO Hylton was deliberate or reckless. There was no reason for TFO Hylton even to know about the organization of Google's internal data structures. The defendant therefore cannot show that any omission regarding that information was deliberate or reckless. And the fact that there is some error in cell phone location measurements is common knowledge; there is no reason Officer Hylton would not have expected the issuing judge to be aware of that fact. In sum, the omissions cited by the defendant were not material to the issuance of the warrant, and in any event the defendant has not shown that any omissions were deliberate or reckless.

Finally, the defendant's argument against the good-faith exception relies heavily on a

[8] For example, the affidavit could have included the fact that many of Google's location points are based on GPS information, and that GPS coordinates are usually accurate to within a few feet. *See* https://www.gps.gov/systems/gps/performance/accuracy. This additional information would not have defeated the affidavit's probable cause. FBI TFO Hylton could not have known in advance Google's confidence radii for its WiFi-based location points. But even if he could have known that the step 1 WiFi location points would end up having a median confidence radius of 25 meters, that fact also would not have affected the existent of probable cause.

district court case from another circuit, *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015). But the warrant in *Winn* was nothing like the warrant here: it authorized seizure of "any or all files" contained on a cell phone. *Winn*, 79 F. Supp. 3d at 918. Here, in contrast, the warrant was remarkably targeted: despite the vast quantity of data stored by Google, it targeted only two hours of location data associated with devices near the bank at the time of the armed robbery, and Google produced data regarding only 19 accounts. Officers' reliance on the warrant was reasonable, and this Court should deny the defendant's motion to suppress.

IV. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 12th day of June, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov