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

UNITED STATES OF AMERICA	**)**	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	**)**	
Defendant	**)**	

DEFENDANT OKELLO CHATRIE'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, moves the Court to suppress evidence that law enforcement obtained pursuant to a warrant authorizing state police to obtain the cell phone location information of 19 Google users who happened to be in the vicinity of a bank robbery on a Monday afternoon in Richmond. This is a "geofence" warrant, and it is an unlawful and unconstitutional general warrant that is both overbroad and lacks the particularity required by the Fourth Amendment. The Court should therefore suppress all evidence obtained from the warrant and all fruit of the poisonous tree, including the identification of Mr. Chatrie.

INTRODUCTION

Law enforcement obtained Mr. Chatrie's cell phone location information from Google using a "geofence" warrant. A geofence warrant requires Google to produce data regarding all devices using Google services within a geographic area during a given window of time. But unlike a typical warrant for location data, this geofence warrant did not identify Mr. Chatrie in any way. In fact, it did not identify any of the 19 people whose personal information was searched by the Virginia state police as a result. Instead, the warrant operated in reverse: it required Google to identify a large cache of deeply private data—held in the "Sensorvault"—and then allowed police

the discretion to obtain private information from devices of interest. This is nothing less than the modern-day incarnation of a "general warrant," and it is prohibited by the Fourth Amendment.

Virginia police obtained a warrant for the Sensorvault data in this case, presumably because they recognized, correctly, that such information is intensely private and constitutionally protected. Like the cell site location information ("CSLI") in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), cell phone users constantly generate Sensorvault location information by either (1) using devices running Google's software ("Android" phones), or (2) interacting with Google services (Maps, Gmail, Search, YouTube, etc.). *See* Background, *infra*. And as in *Carpenter*, users have a reasonable expectation of privacy in their location data, which is sensitive and revealing of the "privacies of life." 138 S. Ct. at 2214. Not only can this data reveal private activities in daily life, but it can also show that someone is inside a constitutionally protected space, such as a home, church, or hotel—all of which are in the immediate vicinity of the bank that was robbed in Richmond. The ability to access data that can locate individuals quickly, cheaply, and retroactively is an unprecedented expansion of law enforcement power, and doing so constitutes a Fourth Amendment search, just as it did in *Carpenter*. *Id* at 2230; *see also Prince Jones v. United States*, 168 A.3d 703, 712 (D.C. 2017) (recognizing that access to cell phone location data permits the "police to locate a person whose whereabouts were previously completely unknown."). In fact, the location data available in Google's Sensorvault is even more precise than the data in *Carpenter*. Google can pinpoint an individual's location to approximately 20 meters compared to "a few thousand meters" for cell site location data. Google, *Find and Improve Your Location's Accuracy* (Oct. 24, 2019), https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&oco=1. Therefore, the third-party doctrine should not apply, and a valid warrant should be required for law enforcement to access any user's Sensorvault data.

Nonetheless, the fact that law enforcement obtained a warrant in this case does not save the search from constitutional infirmity. This is no ordinary warrant. It is a general warrant purporting to authorize a classic dragnet search of every Google user who happened to be near a bank in suburban Richmond during rush hour on a Monday evening. This is the kind of investigatory tactic that the Fourth Amendment was designed to guard against. Geofence warrants like the one in this case are incapable of satisfying the probable cause and particularity requirements, making them unconstitutional general warrants.

In the alternative, should the Court find that geofence warrants are not wholly impermissible under the Fourth Amendment, the warrant in this case fails to satisfy the particularity requirement and fails to establish probable cause to search Mr. Chatrie's Sensorvault data. Despite the prevalence of Google phones and services, there are no facts to indicate that the bank robber used either, whether ever or at the time of the robbery. There is no evidence that the robber used an Android operating system or accessed any Google service in connection with the crime. Instead, based only on Google's popularity and the prevalence of cell phones generally, law enforcement searched a trove of private location information belonging to 19 unknown Google users who happened to be near a local bank on a Monday evening. The government's generalized assumptions about cell phone use, devoid of any specific factual nexus to the criminal activities alleged, are insufficient to establish probable cause for the sweeping and invasive search in this case. Additionally, the discretion afforded to police to determine which accounts to search is the essence of an unparticularized warrant. In short, the warrant both lacks particularity and is fatally overbroad.

Finally, the good faith exception to the exclusionary rule does not apply to evidence obtained from this warrant. Given the lack of particularity and absence of probable cause for any

and all individuals whose data would be searched, no objectively reasonable officer could rely on such a warrant. For these reasons, the Court must suppress all evidence obtained from the geofence warrant and all fruit of the poisonous tree.

BACKGROUND

Over the last few decades, the ability of law enforcement to cheaply and easily access highly sensitive digital data has progressed in leaps and bounds. Requests for user information from cellular service providers and other online service providers like Google have become a powerful investigative tool for law enforcement to locate and identify almost any individual, as 96% of Americans now own cell phones. Pew Research Center, *Mobile Fact Sheet* (Jun. 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/. As a result, "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *Carpenter*, 138 S. Ct. at 2218.

Law enforcement can locate cell phones using user location data, which is collected and maintained by cell phone companies as well as third-party service providers, such as Google. For example, Google regularly collects detailed location information from all phones running Google's "Android" operating system. Android phones routinely transmit their GPS location to Google, but Google can also identify a phone's location based on nearby Wi-Fi networks, mobile networks, and device sensors. Google, *How Google Uses Location Information* (Oct. 25, 2019), https://policies.google.com/technologies/location-data. While it is possible to turn off location history on an Android phone, opening Google Maps or running a Google search will still pinpoint a user's latitude and longitude and create a record with Google. Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb (identifying Google services that register a user's application upon use, including "Location History, Web and App activity, and …

device-level Location Services."). Even non-Android devices, such as Apple iPhones, transmit location information to Google when individuals use a Google service or application, such as Gmail, Search, and Maps. *Id.* Consequently, although Google's Sensorvault does not collect data on every phone, it nevertheless contains an enormous trove of location information on most Android phones and many iPhones in use in the United States.

In recent years, law enforcement has begun requesting this data from Google using geofence warrants to identify devices present in a geographic area during a window of time. Jennifer Valentino-DeVires, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html. Since a geofence warrant identifies a geographic area, and not a suspect, these requests "ensnare anyone who uses Google services at specific times in the . . . areas [near a crime]," sweeping up innocent individuals in an unconstitutional dragnet search. Debra Cassens Weiss, *FBI Asks Google to Turn Over All Data on Users Who Were Close to Robbery Locations*, ABA Journal (Oct. 25, 2018), http://www.abajournal.com/news/article/fbi_asks_google_for_location_data_on_anyone_close_to_robbery_locations_in_t. Individuals may be caught up in this search by merely using an Android phone, conducting an internet search using Google, running a Google application such as Google Maps or YouTube, or even receiving an automatic weather update from an Android service. Nakashima, *supra*, *Google Tracks Your Movements, Like it or Not*.

FACTS

Geofence warrants compel Google to produce location information about devices interacting with Google technology within a geographic area during a given timeframe. In this case, the government requested data from Google regarding all Google devices that were within 150 meters of the Call Federal Credit Union in Richmond, Virginia, during a one-hour period at

the beginning of Monday evening rush hour. Specifically, the warrant sought information on all devices within 150 meters of 37° 26' 18.3" N, 77° 35' 16.4" W between 4:20 and 5:20 p.m. EST. *See* Ex. A State Warrant at 3[1]. In addition to a major thoroughfare (U.S. Route 360), the immediate area includes a Ruby Tuesday restaurant, a Hampton Inn hotel, a mini storage facility, an apartment complex for seniors, another residential apartment complex, and the Journey Christian Church, a very large[2] church located directly across from the Credit Union. The 150-meter radius encompasses both the bank and the church as well as their parking lots.

The warrant describes a three-step process. First, Google provided "anonymized information" about all Google users in the area between 4:20 and 5:20 p.m., including "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source." *See* Ex. A (State Warrant) at 2. This initial search affected 19 unique Google users, yielding 209 location points over an hour. *See* Ex. B (Excel Sheet 1). Law enforcement then reviewed the data and attempted to "narrow down the list" based on other known information. *See* Ex. A (State Warrant) at 2. Next, in a private letter to Google without any additional judicial scrutiny, police requested additional "contextual data points with points of travel *outside* of the [geofence]" and for "30 minutes before AND 30 minutes after the initial search time periods" for a subset of 9 users. *Id*. (emphasis added). This produced 680 location points over a total of two hours. *See* Ex. C (Excel Sheet 2). Finally, police returned to Google once again to obtain

[1] The government has provided the defense with a sealed copy of this search warrant with no explanation as to why it remains sealed. Per the Chesterfield County Circuit Court Clerk's Office, this warrant and its supporting documents will remain sealed absent further intervention from the government until December 19, 2019. Because the document is and will remain sealed until further action by the government, Mr. Chatrie does not attach it here, but refers to it for when the Court is able to review a copy.

[2] In 2017, Outreach Magazine, which tracks church attendance and congregation growth rates, reported that Journey Christian Church had 1,743 people attend its church and ranked as one of the fastest-growing congregations in the country. Outreach Magazine, Journey Christian Church, https://outreach100.com/churches/journey-christian-church.

"identifying account information/CSI" for 3 users, including: usernames, subscriber information, as well as all email addresses, electronic devices, and phone numbers associated with the accounts.[3] *See* Ex. A (State Warrant) at 3.

ARGUMENT

The acquisition of Mr. Chatrie's data from Google was a Fourth Amendment search. In either event, the action intruded upon Mr. Chatrie's reasonable expectation of privacy in his location data. This is critical because the warrant obtained by Virginia police is invalid. It is a general warrant, irredeemably unreasonable and completely impermissible under the Fourth Amendment. Law enforcement simply cannot establish the requisite probable cause and particularity to search a trove of data belonging individuals suspected of no wrongdoing. As a result, the warrant is also fatally overbroad and lacking particularity. Such a warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law.").

I. The Acquisition of Mr. Chatrie's Data from Google Was a Fourth Amendment Search.

In *Carpenter*, the Supreme Court held that individuals have a reasonable expectation of privacy in their cell phone location data, and that the government's acquisition of those records in that case was a Fourth Amendment search. 138 S. Ct. at 2217. This holding applies with equal force in the context of a location data request directed to Google, which involves information that is more precise than the data at issue in *Carpenter*. Regardless of whether the Court analyzes this

[3] The warrant does not define "CSI" at any point in the warrant or application.

claim under the reasonable expectation of privacy framework set forth in *Katz* or a property-based theory, it should reach the conclusion that acquisition of Defendant's location information constituted a Fourth Amendment search.

A. Cell Phone Users Have a Reasonable Expectation of Privacy in Their Location Information.

In considering whether individuals reasonably expect information to remain private, the Supreme Court has crafted "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Carpenter*, 138 S. Ct. at 2219 (applying the *Katz* analysis in the context of historical cell site location information and concluding that users have a reasonable expectation of privacy in this information). Cell phone location information is highly sensitive, as shown by the watershed decision in *Carpenter*, and this classification applies to Google's Sensorvault location data based on the strong similarities between the two types of information. In the majority opinion, Justice Roberts emphasized the revealing nature of historical cell site location information and compared this quality to that of GPS location information. *Id.* at 2217. ("*As with GPS information*, the time-stamped data provides an intimate window into a person's life, revealing … his particular movements" (citation omitted) (emphasis added)). GPS is one of the primary methods that Google uses to compile Sensorvault location data. Google, *supra*, *How Google Uses Location Information*. Google also includes location data from mobile networks, *id.*, the same technology at issue in *Carpenter*.

The fact that Google, a third-party service provider, collects and maintains this location information does not diminish an individual's expectation of privacy in it. *Carpenter*, 138 S. Ct. at 2220. While the third-party doctrine stands for the general proposition that an individual has a

reduced expectation of privacy in information knowingly shared with another, the rule is not to be "mechanically" applied in the digital age. *Id.* at 2219. To do so would "[fail] to contend with the seismic shifts in digital technology that made possible the tracking of not only [Mr. Chatrie's] location but also everyone else's, not for a short period but for years and years." *Id.* Indeed, Google is no ordinary third party: "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Id*. The fact that Google is able to provide location data information for a given place and time in the past is possible only because of its exhaustive and constant collection of user data.

In *Carpenter*, the Court rejected the government's contention that the third-party doctrine applied to historical cell-site information, and this holding applies to cell phone location data acquired through Google. The Court provided two main rationales for its decision: cell-site location information is qualitatively different from types of business records to which the doctrine may apply based on its revealing nature, and users do not voluntarily share their cell-site location information with their service provider. 138 S. Ct. at 2219–20. These two rationales apply with equal force to the location information Google stores, and as such third-party doctrine is inapposite to data gleaned from Google under the warrant.

Google location records are qualitatively different from the business records to which the third-party doctrine traditionally applies. *See Smith v. Maryland*, 442 U.S. 735, 742 (numbers dialed on a landline); *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank deposit slips). Instead, they reveal the same type of information as the cell-site location data considered private in *Carpenter*, and they do so in an even more precise manner. Google, *supra, Find and Improve Your Location's Accuracy.* As the Supreme Court determined, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and [an]

exhaustive chronicle of location information." *Carpenter*, 138 S. Ct. at 2219. Location data from Google is similarly "exhaustive." Google routinely collects detailed location data on every user, not just when criminal activity is suspected. And when police obtain this information with a geofence warrant, it is also comprehensive, revealing every Google user who happened to pass through a given area over a given timeframe. In short, Google location data is qualitatively different from third-party business records, and regardless of the fact that Google stores it, it is entitled to a reasonable expectation of privacy.

Individuals do not voluntarily share their location information with Google, further supporting the notion that the third-party doctrine is inapposite in this context. The third-party doctrine is justified by the assumption that an individual cannot reasonably expect "information he *voluntarily* turns over to third parties" to remain private. *Smith*, 442 U.S. at 44 (emphasis added). In *Carpenter*, the Court held that cell phone users' "sharing" of their location data with their service provider is not done on a truly voluntary basis since "carrying [a cell phone] is indispensable to participation in modern society." 138 S. Ct. at 2220 (quoting *Riley*, 134 S. Ct. at 2484)). Similarly, navigation apps are exceedingly popular, with 77% of smartphone owners using them regularly, and Google Maps is far and away the most popular navigation app. Riley Panko, *The Popularity of Google Maps: Trends in Navigation Apps in 2018*, The Manifest (July 10, 2018), https://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018. This shows that, like owning a smartphone, using navigation software is, for many, "indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2210. Much the same could be said about Gmail or Google Search. Indeed, Google software is ubiquitous on smartphones, with Android operating systems running on 87% of devices sold in 2019. International Data Corporation, *Smartphone Market Share*, https://www.idc.com/promo/smartphone-market-

share/os, Oct. 25, 2019. Likewise, Google Maps is the most popular navigation app, used on 67% of smartphones, making it nearly six times more popular than its closest competitor Waze, which is now also owned by Google.[4] Panko, *supra*, The *Popularity of Google Maps*. And more than 90% of all internet searches use Google. Jeff Desjardins, *How Google retains more than 90% of market share*, Business Insider (Apr. 23, 2018), https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4. In short, it is not reasonable to expect ordinary phone users to avoid Google software. It cannot be that individuals must choose between their privacy and carrying a cell phone, running a Google search, or watching a YouTube video.

B. Geofence Warrants Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

In a series of cases addressing the power of sense-enhancing technologies "to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (last alteration in original); *accord United States v. Jones*, 565 U.S. 400, 406 (2012). As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." 565 U.S. at 429 (Alito, J., concurring in judgment).

Technological innovations, like the ability to locate cell phones (and their users) seemingly out of thin air, remove many of these practical limitations on government surveillance capabilities. *See, e.g.*, *Prince Jones*, 168 A.3d at 714 (describing a cell-site simulator as a "powerful person-locating capability" that the government previously lacked, which is "only superficially analogous

[4] It is unclear whether use of the Waze app also contributes location data to Google's Sensorvault.

to the visual tracking of a suspect"). Recognizing the potential for technologies like these to enable invasive surveillance on a mass scale, the Court has admonished lower courts to remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2223.

1. The data collected through a geofence warrant is extraordinarily detailed and deeply revealing.

The *Carpenter* Court noted that "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 138 S. Ct. at 2216. Google's Sensorvault includes GPS data, which is even more precise than the cell site location information at issue in *Carpenter*. Google, *supra*, *Find and Improve Your Location's Accuracy*. Google also locates users using "device sensors . . . or WiFi" to augment GPS's accuracy when these methods are available. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. As a result, Google can locate a device within approximately 20 meters, compared to "a few thousand meters" for cell site location information. Google, *supra*, *Find and Improve Your Location's Accuracy*. This level of precision can pinpoint a device to a single a building, which is significantly more detailed that the location information available from wireless carriers like AT&T or Verizon. Russell Brandom, *Police Are Filing Warrants for Android's Vast Store of Location Data*, The Verge (June 1, 2016), https://www.theverge.com/2016/6/1/11824118/google-android-location-data-police-warrants.

Indeed, Google location data can reveal information about a user's location inside constitutionally protected areas. Individuals tend to carry cell phones at all times, "into private residences, doctor's offices, political headquarters, and other potentially revealing locales," *Carpenter*, 138 S. Ct. at 2218. In this case, the 150-meter geofence fully encompasses the Journey Christian Church, which has over 3,600 followers on Facebook. Journey Christian Church,

Facebook (Oct. 25, 2019), https://www.facebook.com/JourneyRVA/. A church, like a home, is a constitutionally protected space, especially because of its obvious First Amendment significance. But when law enforcement obtained the list of Google users near the bank, it also obtained the data of Google users inside Journey Christian Church, intruding on this quintessentially protected space and violating churchgoers' reasonable expectation of privacy. Such intrusions are "presumptively unreasonable in the absence of a search warrant." *Katz,* 389 U.S. at 361; *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'") (quoting *Silverman v. United States*, 365 U.S. 505 (1961)).

When Fourth Amendment searches implicate First Amendment concerns, courts should be careful to apply Fourth Amendment requirements with "the most scrupulous exactitude," *Stanford v. Texas*, 379 U.S. 476, 485 (1965). Additional safeguards may be constitutionally required to protect First Amendment freedoms, *Marcus v. Search Warrant of Property*, 367 U.S. 717, 729 (1961). But the warrant application in this case did not even mention[5] the proximity of the church or take into account the sensitive First Amendment associations and activities that the search may reveal. Instead, it unconstitutionally left "the protection of [First Amendment] freedoms to the whim of the officers charged with executing the warrant." *Stanford*, 379 U.S. at 485.

2. A Geofence Warrant Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space.

In *Carpenter*, the Supreme Court distinguished cell site location information from traditional law enforcement surveillance due to "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id.* at 2218. As the Court

[5] In fact, the warrant appears to refer to the church as simply "an adjacent business." *See* Ex. A State Search Warrant at 5.

explained, it is akin to a time machine that allows law enforcement to look at a suspect's past movements, something that would be physically impossible without the aid of technology: "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id*. Geofence warrants likewise represent an unprecedented expansion of law enforcement's ability to locate a person in time and space. They enable law enforcement to reconstruct an individual's historical movements, something that would have been impossible at the time of the adoption of the Fourth Amendment at this level of ubiquity, specificity, and cost. And as with cell cite location information, they now allow the government to "travel back in time to retrace a person's whereabouts, subject only to [Google's] retention polices." *Id.*

The Supreme Court has never blessed anything remotely like dragnet geofence warrants as a permissible means of surveillance. Like the surreptitious GPS tracking in *Jones*, 565 U.S. at 420 (Alito, J., concurring), or the acquisition of historical CSLI in *Carpenter*, 138 S. Ct. at 2217, this search could not have been conducted through visual surveillance alone. It therefore violates a reasonable expectation of privacy and is impermissible under the Fourth Amendment. *Cf. Kyllo v. United States*, 533 U.S. 27, 40 (2001) (use of a thermal imaging device is a search because the information gleaned "would previously have been unknowable without [a] physical intrusion."); *Prince Jones*, 168 A.3d 703, 714 (D.C. 2017) (use of a "cell site simulator" to locate a person through a cell phone is a search because the information is not readily available or in the public view, unlike visual surveillance or older generations of tracking devices).

C. The Acquisition of Defendant's GPS Data from Google Was a Search Under a Property-Based Approach to the Fourth Amendment.

Under a property-based theory of the Fourth Amendment, Mr. Chatrie's GPS data constitutes his "papers or effects," regardless of whether they are held by a third-party service

provider like Google. They therefore cannot be searched or seized without a *valid* warrant. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).

In his dissenting opinion in *Carpenter*, Justice Gorsuch opined that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* Justice Gorsuch drew a strong analogy between cell phone location data and mailed letters, in which people have had an established Fourth Amendment property interests for over a century, whether or not these letters are held by the post office. *Id.* at 2269. (citing *Ex parte Jackson*, 96 U.S. 727, 733 (1877)). Just as Gmail messages belong to their senders and recipients (and not to Google), so too does Google location data belong to the Google users who generate it.

Here, Mr. Chatrie's location information belongs to Mr. Chatrie. Google may be responsible for collecting and maintaining it, but even Google understands that it is the user's private data. For example, Google's privacy policy consistently refers to user data as "your information," which can be managed, exported, and even deleted from Google's servers at "your" request. Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infodelete. These are not "business records." Businesses do not let customers export or delete the company's records at will. These are customer records—Mr. Chatrie's records. Mr. Chatrie merely entrusted his information to Google, as so many people do. He did not forfeit his Fourth Amendment interests in it.

As Justice Gorsuch explained in *Carpenter*, "[e]ntrusting your stuff to others is a bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). Here, Google is the bailee, and it owes a duty to the bailor, Mr. Chatrie, to keep his data safe. This

arrangement is apparent from Google's privacy policy. Google is not allowed to do whatever it wishes with Mr. Chatrie's data. While Google reserves the right to use it for advertising or development purposes, it also promises not to disclose it to "companies, organizations, or individuals outside of Google," subject to a short list of explicit exceptions.[6] In other words, Mr. Chatrie retains the right to exclude others from his location data, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Laws of England *2 (1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things … in total exclusion of the right of any other."); *Loretto v. Teleprompter Manhattan CATV Corp*., 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most treasured strands" of the property rights bundle); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (calling the right to exclude "one of the most essential sticks" in the property rights bundle).

Law enforcement eviscerated Mr. Chatrie's right to exclude others from his location data, which Google held in trust for him. This trespass constitutes a Fourth Amendment search and seizure, no less than a violation of one's "reasonable expectation of privacy."

II. A Geofence Warrant Is an Unconstitutional General Warrant.

A geofence warrant, like the warrant in this case, is a general warrant, repugnant to the Constitution. It is the epitome of the "dragnet" law enforcement practice that the Supreme Court feared in *Knotts*, 460 U.S. at 284, sweeping up the location data of untold innocent individuals in the hopes of finding one potential lead. It is inherently overbroad and lacking particularity by design. It cannot satisfy the Fourth Amendment with "scrupulous exactitude" because it is

[6] Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infosharing. One of these exceptions is "For legal reasons," but this is not a free pass to hand over user data to law enforcement. It is implied that legal process must be valid, which includes establishing probable cause and following the strictures of the Fourth Amendment, not just submitting the proper form. *See* Jim Harper, *The Fourth Amendment and Data: Put Privacy Policies in the Trial Record*, The Champion, Jul. 2019, at 21.

inherently antithetical to the Fourth Amendment. The Court should find that geofence warrants like this one are categorically invalid and void *ab initio.*

A. The Fourth Amendment Forbids General Warrants.

As the Supreme Court has repeatedly recognized, opposition to general warrants "helped spark the Revolution itself," demonstrating the degree to which they offend the most basic principles of American liberty. *Carpenter*, 138 S. Ct. at 2213; *see also Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481; *Marcus*, 367 U.S. at 728. The Virginia Declaration of Rights, like other founding documents, also reflects this colonial hostility to general warrants by explicitly and categorically prohibiting them:

> That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, *or to seize any person or persons not named*, or whose offense is not particularly described and supported by evidence, are grievous and oppressive, and ought not to be granted.

Va. Const. art. I, § 10 (emphasis added); *see also Zimmerman v. Town of Bedford*, 134 Va. 787, 800 (1922). They are likewise forbidden by Virginia Code § 19.2–54 ("no general warrant for the search of a house, place, compartment, vehicle or baggage shall be issued"); *see also Morke v. Commonwealth*, 14 Va. App. 496, 500 (1992) (stating general warrants are proscribed by both the Fourth Amendment and Code § 19.2–54).

At the time of the Revolution, a general warrant meant a warrant that failed to identify the people to be arrested or the homes to be searched. *See Steagald v. United States*, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched."). For example, one of the specific cases that gave rise to the Fourth Amendment was *Wilkes v. Wood*, 98 Eng. Rep. 489, 490 (1763), which concerned a general warrant that ordered

the king's messengers to "apprehend and seize the printers and publishers" of an anonymous satirical pamphlet, the *North Briton* No. 45. The warrant did not specify which houses to search or whom to arrest, but officials ransacked five homes, broke down 20 doors, rummaged through thousands of books and manuscripts, and arrested 49 people. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979, 1007 (2011). The *Wilkes* court condemned the warrant because of the "discretionary power" it gave officials to decide where to search and what to take. 98 Eng. Rep. at 498. The case became wildly famous in the American colonies, one of three influential English cases that led to the rejection of general warrants.[7]

One reason the Founders opposed general warrants was because of the discretion they gave to officials. They placed "'the liberty of every man in the hands of every petty officer'" and were therefore denounced as "'the worst instrument of arbitrary power." *Stanford*, 379 U.S. at 481 (quoting James Otis). The other reason was that general warrants allowed the government to target people without any evidence of criminal activity, turning the concept of innocent until proven guilty on its head. Donohue, 83 U. Chi. L. Rev. at 1317. Instead of having information that the person or place to be searched is engaged in illegal activity, general warrants presume guilt, establishing innocence only after a search. *Id.* Prohibiting such "promiscuous" searches therefore served to protect not only individual rights, but also a cornerstone of American liberty. *Id.*

Thus, for example, no valid search warrant would permit the police to search every house in a neighborhood or pat down everyone in sight. *See United States v. Glenn*, 2009 WL 2390353, at *5 (S.D. Ga. 2009) ("The officers' 'generalized' belief that some of the patrons whom they had

[7]*See generally*, Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1196 (2016). In addition to *Wilkes v. Wood*, the cases were *Entick v Carrington*, 19 How St Tr 1029 (CP 1765), and *Leach v Money*, 19 How St Tr 1001 (KB 1765).

targeted for a systematic patdown might possibly have a weapon was insufficient to justify a 'cursory' frisk of everyone present."); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007) (holding that a warrant "authorizing a search of 'any person present' . . . resulted in an unlawful general search."); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a "warrant to search all suspected places [for stolen goods]" was unlawful because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested"). Yet, with a geofence warrant, law enforcement can do just that, searching inside every home, vehicle, purse, and pocket in a given area, without particularized suspicion to search any of them.

B. A Geofence Warrant Is A General Warrant.

A geofence warrant, like the one in this case, is a modern-day incarnation of the historically reviled general warrant. It is the digital equivalent of searching every home in the neighborhood of a reported burglary, or searching the bags of every person walking along Broadway because of a theft in Times Square. Without the name or number of a single suspect, and without ever demonstrating any likelihood that Google even has data connected to a crime, law enforcement invades the privacy of tens or hundreds or thousands of individuals, just because they were in the area. *Cf. Sibron v. New York*, 392 U.S. 40, 63–64 (1968) (holding that "[t]he suspect's mere act of talking with a number of known narcotics addicts over an eight-hour period" did not give rise to either reasonable suspicion or probable cause to search him).

The Supreme Court has always been "careful to distinguish between [] rudimentary tracking . . . and more sweeping modes of surveillance," in deciding whether a search is constitutional. *Carpenter*, 138 S. Ct. at 2215 (citing *Knotts*, 460 U.S. at 284). Geofence warrants fall on the "sweeping" end of this spectrum, as they potentially affect everyone. They represent

the kind of surveillance that the Supreme Court cautioned against in *Knotts*, noting that "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." 460 U.S. at 283–84. That time is now.

A comparison to the "rudimentary tracking" in beeper cases such as *Knotts* and *Karo* illuminates the drastically different, indiscriminate-dragnet nature of a geofence warrant. In the beeper cases, the government only sought to track *one* individual. To do so, law enforcement first needed to identify the individual, and then to physically install a tracking device on an object that was in their possession. With a geofence warrant, however, the government no longer needs identify a suspect. Instead, "[w]ith just the click of a button, the government can access [Google's] deep repository of historical location information at practically no expense." *Carpenter*, 138 S. Ct. at 2218; *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive"). Because of the ubiquity of Google software on cell phones, Sensorvault includes location data on many of the 400 million devices in the United States—"not just those belonging to persons who might happen to come under investigation," meaning that "this newfound tracking capacity runs against everyone" who uses Google. *Carpenter*, 138 S. Ct. at 2218.

Geofence warrants pose the same type of threat as colonial-era general warrants "which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 134 S. Ct. at 2494. As in this case, they are the product of unrestrained searches of constitutionally protected spaces, like the Journey Christian Church. And they result

in rummaging through the digital papers and effects of large numbers of unknown, unnamed people, all or almost all of whom are admittedly innocent.

C. A Geofence Warrant Cannot Satisfy the Probable Cause or Particularity Requirements.

By design, a geofence warrant does not specify the individuals or individual Google accounts to be searched. Rather, the purpose is to search across millions of unknown user accounts and then identify specific accounts that law enforcement would like to search further. As a result, however, geofence warrants are inherently incapable of meeting the probable cause and particularity requirements of the Fourth Amendment, and are therefore general warrants.

Geofence warrants are intentionally overbroad. In contrast to warrants authorizing the acquisition of location data about a single individual suspected of a criminal offense, geofence warrants identify all Google users merely due to their proximity to a crime scene. But as the Supreme Court has held on more than one occasion, "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) (citing *Sibron*, 392 U.S. at 62–63); *see also United States v. Di Re*, 332 U.S. 581, 587 (1948) (holding that a person, by mere presence in a suspected car, does not lose immunities from search of his person to which he would otherwise be entitled). Consequently, there is an abject absence of individualized suspicion for any, let alone all, of the individuals whose Google data were searched by the warrant. Of course, it would have been difficult to establish probable cause for the location information of every Google user near the bank, as the government acknowledges that most of the data belongs to innocent people. But the convenience of gathering location information on all of those individuals with a single warrant to Google does not obviate the requirements of the Fourth Amendment. *Riley*, 134 S. Ct. at 2493 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)); *Carroll v.*

United States, 267 U.S. 132, 153–54 (1925) ("It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search."). The warrant is void for lack of probable cause.

Similarly, a geofence warrant is not remotely particularized. The purpose of the particularity requirement is to prevent general warrants, which it does by "limiting the authorization to search the specific areas and things for which there is probable cause to search." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). With respect to seizures, the Fourth Amendment demands that "nothing is left to the discretion of the officer executing the warrant." And where, as here, there are significant First Amendment concerns—especially due to the proximity of a church—the particularity requirement takes on heightened importance. *Stanford*, 379 U.S. at 485; *Marcus*, 367 U.S. at 729; *A Quantity of Copies of Books v. Kansas*, 378 U.S. 205, 212 (1964).

A geofence warrants leaves the question of whose data to search and seize almost entirely the discretion of the executing officers. It does not "particularly describe the 'things to be seized,' let alone identify the name of a single suspect Google user, phone number, or account. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Instead, it identifies Google headquarters as the place to be searched and requests location data from *all* Google users near a given location. Although the data is "anonymized" initially, it does not stay that way. Rather, the warrant leaves it up to the police to "narrow down the list" by some unknown or unstated method before the officers decide which accounts to deanonymize and search further. *See* Ex. A State Search Warrant at 2. Law enforcement engage in multiple rounds of back-and-forth with Google—not the independent magistrate envisioned by the Fourth Amendment—

to decide whose data they would review. Paired with the sweeping scope and absence of probable cause, the lack of particularity in geofence warrants make them unconstitutional general warrants.

D. This Geofence Warrant is Overbroad and Lacking Particularity

Even if geofence warrants are not categorically impermissible, the geofence warrant obtained in this case is unconstitutionally overbroad and lacks particularity.

First, Virginia police did not have probable cause to believe that the bank was robbed by a Google user. While the warrant application does state that the robber could be seen using a cell phone, there is no evidence to show that it was an Android phone or that he or she used a Google service within the initial one-hour window identified in the warrant. The application cites the general popularity of cell phones, but does not provide any facts to suggest that Google specifically would have data pertaining to the perpetrator of this crime. It did not allege that bank robbers frequently use Google or state that a teller had noticed the phone's make and model. If the robber had an iPhone and did not use Google services between 4:20 and 5:20 p.m., then Google would not have a record of the phone's location during that time.[8]

Second, the warrant does not specify which Google accounts it seeks to search, presumably due to the lack of probable cause to search any specific Google user. Even the 150-meter radius is not sufficiently particular. Rather than a requesting data for just the bank and parking lot, the warrant included the entirety of the church next door. Furthermore, a three-step, back-and-forth process with the recipient of a warrant is not a substitute for particularizing that warrant at the outset. Instead, it is an unconstitutional delegation of discretion to the executing officers. The

[8] Likely for this reason, the use of geofence warrants elsewhere has frequently failed to identify suspects. *See* Tyler Dukes, *To find suspects, police quietly turn to Google*, WLAR (Mar. 15, 2018), https://www.wral.com/Raleigh-police-search-google-location-history/17377435/ (finding that "only one person has been arrested for any of the crimes in which police approached Google for data on *thousands of users*" across the four investigations).

issuing court had no information on how many people were likely to be initially affected. And it had no role in deciding which of those people would be subject to further search, outside the geofence, wherever they happened to be. Indeed, the warrant permits police to obtain location data from *anywhere outside* the geofence for an unknown subset of users, identified solely by investigators, with no additional showing or judicial involvement. *See* Ex. A State Search Warrant at 2. Finally, the court had no role in deciding which or how many people would have their data deanonymized and searched further still. The warrant left everything up to the discretion of the executing officers, violating the Fourth Amendment's particularity requirement.

III. The Good Faith Exception Does Not Apply

Under the good-faith exception to the exclusionary rule, evidence derived from an unconstitutional search should not be suppressed when it is obtained in reliance on a facially valid warrant. *United States v. Leon*, 468 U.S. 897 (1984). The Supreme Court has emphasized, however, that "in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Id.* at 922-23. There, the good faith exception would not apply, and suppression would be appropriate "if the officers . . . could not have harbored an objectively reasonable belief in the existence of probable cause." *Id.* at 926. Suppression is also appropriate where "a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be searched—that the executing officers cannot reasonably presume it to be valid." *Id.*

Here, a reasonable law enforcement officer could not have presumed that such an overbroad, unparticularized warrant would be valid. The police knew they did not have a suspect, let alone probable cause to search any specific person or place. Instead, they sought every Google user's location data near a bank at rush hour—with no evidence that the robber had ever used

Google. They then exercised complete discretion in deciding which accounts to search further, deanonymize, and obtain additional information about. The deficiencies of this geofence warrant—its absence of probable cause and particularity—are readily apparent, casting it within the circumstances described in *Leon* and making the good faith exception to the exclusionary rule inapplicable.

CONCLUSION

This is a case of first impression, but the Court should treat the geofence warrant here as any other general warrant: repugnant to the Constitution. Geofence warrants represent an unprecedented expansion of the government's surveillance capabilities. *Carpenter*'s emphasis on the degree to which location data obtained by law enforcement is sensitive or "deeply revealing" shows that courts are recognizing the need to treat cell phone data differently from physical records. Based on the sensitivity of these records and the scope of the search, geofence warrants are Fourth Amendment searches of the unreasonable variety. The warrant obtained in this case implicates First Amendment concerns, and as such must withstand "scrupulous exactitude" under the Fourth Amendment. Yet this geofence warrant cannot even survive the probable cause and particularity under the Fourth Amendment. Instead, the warrant functions as a general warrant, thus not meeting the higher First Amendment standard. Finally, because the good faith exception cannot apply to a warrant no reasonable law enforcement officer would in good faith rely on, this geofence warrant is an unconstitutional search, and we therefor request that its fruits be suppressed.

Respectfully submitted,

OKELLO T. CHATRIE

By: /s/
Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant

National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org