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'S REPLY TO GOVERNMENT'S RESPONSE MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, replies as follows to the government's response to his motion to suppress evidence obtained from a "geofence" general warrant. *See* ECF No. 29.

I. Obtaining Mr. Chatrie's Google location information was a search.

Mr. Chatrie presents two arguments as to why the government's acquisition of his Google location data was a search. The government responds to only one of them on the merits. First, Mr. Chatrie argues that the government's conduct was a search under the *Katz* reasonable expectation of privacy test. The government contends that he had no privacy interest in two hours of his location information, failing to appreciate the significance of the Supreme Court's landmark decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and seeking to create a *de minimis* exception to the Fourth Amendment. Second, Mr. Chatrie argues that it was a search under a property rights theory of the Fourth Amendment. This understanding of the Fourth Amendment predates *United States v. Katz*, 389 U.S. 347 (1967), and has been repeatedly identified by the Supreme Court as an equally valid and independent test. *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 409 (2012); *Kyllo v. United States*, 533 U.S. 27, 37 (2001); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992). The government, however, brushes it aside as if it were a recent invention of Justice

Gorsuch, offering no response on the merits. ECF No. 41 at 12. Under both theories, however, the acquisition of Mr. Chatrie's Google location data was a search.

A. Obtaining Mr. Chatrie's Google location information infringed on his reasonable expectation of privacy.

The government contends that Mr. Chatrie had "no reasonable expectation of privacy in any of the information disclosed by Google" because the location data covered two hours instead of seven days. ECF No. 41 at 6. But *Carpenter* did not gift the government a free pass from the Fourth Amendment for any such "limited period." 138 S. Ct. at 2220. On the contrary, the Court made it clear that it would not "grant the state unrestricted access to a wireless carrier's database of physical location information," describing such information as "deeply revealing," "comprehensive," and "inescapable" *Id.* at 2223. Mr. Chatrie had a reasonable expectation of privacy in his Google location information, which was at least as private as the records in *Carpenter*.

Carpenter involved two orders for historical cell site location information ("CSLI"): one seeking 152 days, and a second for seven days. 138 S. Ct. at 2212. In holding that a warrant is required for seven days or more of CSLI, the Court merely decided *Carpenter* on the facts before it. There is no higher constitutional significance to seven days, and *Carpenter* does not suggest that the Fourth Amendment would condone warrantless searches for a shorter period of time. In fact, the second CSLI order only produced only two days of records, not seven. *Id.* at 2212. Likewise, the Court did not express a view on real-time CSLI or "tower dumps" because those facts were not present in the record. *Id.* at 2220. But it would require misreading the rest of the Court's opinion to view this judicial restraint as an invitation to engage in warrantless surveillance. It is not enough to suppose, as the government does, that it might be possible to replicate this

location information given enough time and resources.[1] ECF No. 41 at 8. While some physical searches may be permissible without a warrant, the Court has been clear that "any extension of that reasoning to digital data has to rest on its own bottom." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

Applying the *Carpenter* framework, it is clear that obtaining Google location data was a search that infringed on Mr. Chatrie's reasonable expectation of privacy. Like the CSLI in *Carpenter*, Google location information is deeply revealing, comprehensive, and inescapable. 138 S. Ct. at 2223. It its revealing because it can expose the location of devices inside constitutionally protected areas, including "private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2218. Indeed, Google uses it for that very purpose when serving advertisements. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. And in this case, it located 11 users inside the Journey Christian Church, a quintessentially protected space that raises additional First Amendment concerns. *See Stanford v. Texas*, 379 U.S. 476, 485 (1965) (requiring courts to apply Fourth Amendment requirements with "the most scrupulous exactitude" when searches implicate First Amendment concerns).[2] In sum, two hours of Google location information is capable of revealing the same type of sensitive, private information as CLSI.

[1] Mr. Chatrie maintains that the data obtained through this warrant could not have been obtained through visual surveillance alone. In addition to subscriber information and account details, which are not observable, it would have been impossible to reconstruct all of the location data obtained from Google. Even if the government had unlimited time and resources, they would not be free to enter constitutionally protected spaces to log the devices located inside. Mr. Chatrie does not concede his privacy interest in the non-location data obtained through the geofence warrant.

[2] The government fails to adequately address these First Amendment concerns, just as it failed to recognize or address them when seeking a geofence warrant that fully encompassed a large church. The affiant simply described the church as "an adjacent business" without telling the Court that the "business" was actually a church.

The fact that the government obtained a smaller quantity of this location data than in *Carpenter* does not diminish its potentially revealing nature. *Carpenter* emphasized the long-term privacy implications of cell phone location tracking only because those were the facts before the Court. Elsewhere, the Justices have expressed concern with even short-term monitoring. In *United States v. Karo*, for example, the use of a beeper to track a drum of ether inside a private residence was sufficient to trigger Fourth Amendment scrutiny. 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device . . . whether a particular article—or a person, for that matter—is in an individual's home *at a particular time*.") (emphasis added). Just a small window of GPS monitoring still creates a "precise, comprehensive record of a person's movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Indeed, it takes little imagination to conjure the privacy implications of even a single trip to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)).

Far more troubling is the breadth of the search in this case. Whereas *Carpenter* concerned the search of just one person's location data, the geofence warrant authorized the search of an unlimited number of people's location data. Neither the government nor the magistrate knew in advance how many devices would be swept up as a result of the search. Indeed, the fact that it would yield information about 19 different devices was unknowable at the time of the government's application. This was not a problem the *Carpenter* Court had occasion to consider,

but it is one that has repeatedly troubled the Court.[3] Indeed, "dragnet" searches are a perennial Fourth Amendment fear. That is why the Constitution prohibits general warrants and requires both probable cause and sufficient particularity. Even if obtaining two hours of location data for a single person would not trouble the Court, obtaining two hours of data for every person in an area is a very different story. In this sense, it arouses the same fears of "too permeating police surveillance" and exercise of "arbitrary power" that motivated the *Carpenter* Court. 138 S. Ct. at 2214. Although the concerns in *Carpenter* are not identical, the potentially unlimited breadth of a geofence search makes up for the comparatively shorter duration of a geofence search. Consequently, the data obtained are highly revealing and deserving of Fourth Amendment protection, as much if not more so than the CSLI in *Carpenter*.

Similarly, Google location data has a comprehensive reach that is comparable to CSLI. In fact, CSLI *is* one of the data sources that Google collects and uses to determine users' locations. But Google also includes GPS location data as well as "additional information from nearby Wi-Fi, mobile networks, and device sensors." Google Policies, *supra*. As a result, Google location information is significantly more precise than CSLI alone. The government puts no stock in this distinction because the *Carpenter* Court "t[ook] account of more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." [G. at 8-9 (quoting *Carpenter*, 138 S. C.t at 2218-19).] But because Google uses multiple sources of location data, it locates devices even in places where GPS is unavailable or unreliable, such as indoors. If GPS data is not

[3]*See, e.g.*, *United States v. Knotts*, 460 U.S. 276, 284 (1983) (reserving the question of whether "different constitutional principles may be applicable" to "dragnet-type law enforcement practices"); *see also Jones*, 565 U.S. at 408 n.6 (quoting *Knotts*); *Karo*, 468 U.S. at 716 ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."); *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 327 (1972) (Douglas, J., concurring) ("[T]he recurring desire of reigning officials to employ dragnet techniques … lies at the core of [the Fourth Amendment]."); *Davis v. Mississippi*, 394 U.S. 721, 726 (1969) ("Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry").

available, Google will then approximate location information based on the signal strength of known nearby Wi-Fi networks, which have a short range. Google is capable of doing this by referencing the billions of data points it gathers each day from other Android phones that report on the availability of Wi-Fi networks in range. *See* Tr. at 29, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019) (Ex. D). Only when Wi-Fi and GPS are unavailable does Google fall back to using CSLI, the least precise method. Consequently, Google location data is likely to be *more* comprehensive than GPS, locating devices where GPS is unavailable.

And finally, Google location data is "automatic and inescapable." For Android users like Mr. Chatrie, there is no practical way to avoid transmitting location information to Google, even if "Location History" is turned off. Location History only controls whether location data gets added to a user's "Timeline" feature, not whether Google sees or stores the data. Likewise, disabling Google Location Services does not actually stop a device from determining its location and creating a record. As Google explains, "Your device's location will continue to work even if GLS [Google Location Services] is turned off, but the device will rely only on GPS to estimate device location for apps with the necessary permission." Google Policies, *supra*. Those apps include basic, built-in Google services like Search and Maps. Thus, because "Google Location Services is distinct from your device's location setting," some location information still flows to Google even when it is off. *See* Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb. And while Google notes that there are separate controls for "Web & App Activity," this setting is isolated and unaffected by the restriction of other location information. Furthermore, the government is incorrect that Mr. Chatrie "had to affirmatively opt in" to sharing his location information with Google. As the user of an Android phone, Google Location Services is enabled

by default. *See* Verizon, Samsung Galaxy S9 / S9+ - Activate / Set Up Device, https://www.verizonwireless.com/support/knowledge-base-216675/ (showing Google location services on by default at step eight). Location History, by contrast, is an opt-in feature, but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity.[4] While it is technically possible to disable the phone's location functions altogether by activating "airplane mode" or powering off the device completely, such drastic steps are not required by *Carpenter*. 138 S. Ct. at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."). Rather, collection of Google location data is "inescapable" because, as in *Carpenter*, it relates to services one needs to be a functioning member of today's society. *Id*. In addition the ubiquity of Google services such as Search, Maps, and Mail, all Android phones—such as the one Mr. Chatrie had—run on Google's operating system and regularly transmit location data back to Google without any affirmative user action at all. The collection is therefore just as automatic and inescapable as CSLI.

In sum, Google location data is at least as revealing, comprehensive, and inescapable as CSLI. Thus, as in *Carpenter*, the fact that "such records are generated for commercial purposes . . . does not negate [Mr. Chatrie's] anticipation of privacy in his physical location." 138 S. Ct. at 2217. Mr. Chatrie had a reasonable expectation of privacy in his Google location data and obtaining those records was therefore a Fourth Amendment search. This is especially true because

[4] The government also draws a confusing and unsupported distinction between "incidental" disclosure of location information and disclosure as a "central prerequisite" to obtaining services. CSLI, however, is in fact essential to the use of a cell phone – required to route information to the correct tower and device. It is both central to the way cell phones function and a prerequisite to using their features.

of the "dragnet-style" search used to get them, a longstanding fear of the Court even when long-term surveillance is not at issue.

B. Obtaining Mr. Chatrie's Google location information infringed on his property rights in that data.

The *Katz* reasonable-expectation-of-privacy test has been in place since 1967, but the Supreme Court's Fourth Amendment jurisprudence is not so young. Throughout the late-19th and early-20th centuries, the Court hued closely to a literal reading of the constitutional text, focusing on the property rights attached to "persons, houses, papers, and effects." U.S. Const. amnd. IV; *see, e.g., Agnello v. United States*, 269 U.S. 20, 32 (1925) ("The search of a private dwelling without a warrant is in itself unreasonable and abhorrent to our laws."); *Weeks v. United States*, 232 U.S. 383, 391 (1914) (recognizing that the essence of a Fourth Amendment violation is "the invasion of his indefeasible right of personal security, personal liberty, and private property."); *Ex parte Jackson*, 96 U.S. 727, 732-33 (1878) (holding that postal mail is just as protected under the Fourth Amendment as those papers and effects kept in the safety of one's home). Indeed, the invasion of property rights was at the heart of Lord Camden's judgment in *Entick v. Carrington*, one of the pillars of English liberty and a catalyst for the Fourth Amendment. 19 How. St. Tr. 1029 (K.B. 1765) ("Papers are the owner's goods and chattels. They are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection"); *see also Boyd v. United States*, 116 U.S. 616, 626 (1886) (describing *Entick* as a "monument of English freedom" and "the true and ultimate expression of constitutional law"). On this side of the Atlantic, the founding fathers specifically designed the Fourth Amendment to assure security "in person *and property*" against unlawful searches. *Adams v. New York*, 192 U.S. 585, 598 (1904) (emphasis added). In short, the "traditional," property-based theory of the Fourth Amendment has a pedigree that long predates *Katz* and, given the Court's recent jurisprudence, is as valid as ever.

When the Court decided *Katz*, there was a palpable worry that property rights alone would not be sufficient to implement the Fourth Amendment in an age when communications could occur without an in-person meeting, but through electronic whispers miles apart. Justice Harlan embodied this concern in his famous concurrence, declaring that the Fourth Amendment protects "people, not places." 389 U.S. at 351. This understanding of the Fourth Amendment has served the Court well for decades, but it "did not repudiate [the] understanding" held for "most of our history" that the Fourth Amendment embodies "a particular concern for government trespass" on one's "papers" and "effects." *Jones*, 565 U.S. at 406-07.

Thus, for example, the Court in *Soldal* unanimously held that removal of a tenant's mobile home was a Fourth Amendment seizure even though the owner's "privacy" was not invaded. 506 U.S. at 62 ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Likewise, in *Kyllo*, Justice Scalia avoided the *Katz* doctrine in finding that the use of a thermal imager on a home was a search. 533 U.S. at 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Indeed, the *Kyllo* Court noted that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." *Id.* at 40. And finally, in *Jones*, the opinion of the Court rested on trespass grounds. 565 U.S. at 404-05. The *Jones* Court found that placement of a GPS tracker on a car was a "physical intrusion" that "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id*. Reaffirming *Soldal*, the *Jones* Court unequivocally stated that "the *Katz* reasonable-expectation-of-privacy test had been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 409; *see also Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

Justice Gorsuch's dissent in *Carpenter* was a clarion call for courts and counsel to reassert the central role that property rights have played in the history of Fourth Amendment jurisprudence. 138 S. Ct. at 2272 ("Carpenter pursued only a *Katz* 'reasonable expectations' argument. He did not invoke the law of property or any analogies to the common law, … [and therefore] forfeited perhaps his most promising line of argument."). Mr. Chatrie does not ask this Court to adopt a novel theory, but to apply a deep-rooted one. *See id.* at 406-07. Mr. Chatrie takes Justice Gorsuch's warning seriously and seeks to fully assert his Fourth Amendment rights. The government, however, simply does not engage with the merits of Mr. Chatrie's property-based argument. ECF No. 41 at 12-13. Instead, the government chooses to ignore over a century of Fourth Amendment jurisprudence and merely quip that "a solo dissent is not the law." *Id.* at 12.

II. The warrant lacked probable cause and was even more unparticularized than previously thought.

The government responds that the geofence warrant was supported by sufficient probable cause and particularity. *Id.* at 13-21. But their arguments are even less persuasive in light of additional discovery showing that they twice requested additional location data on all 19 devices initially identified by Google, in contravention of the warrant itself. *See* Ex. A (First Step 2 Request) at 1; Ex. B (Second Step 2 Request) at 1. Indeed, Google twice rebuffed this request, ultimately sending additional information on nine devices. This development underscores why such an ad hoc, back-and-forth negotiation with the recipient of a warrant is no substitute for judicial oversight and a particularized warrant supported by probable cause.

More fundamentally, the government's response appears to misunderstand the significance of the Fourth Amendment's particularity requirement. Particularity is not just about how clearly a warrant identifies the object of a search for which there is probable cause to seize, but whether it adequately constrains law enforcement's discretion in the execution of that search and seizure. Its

basic purpose is to prevent general warrants by ensuring that "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). The government contends that the information it sought was "constrained" based on location, date, and time to the robbery under investigation. ECF No. 41 at 18. But it is not enough to simply name the crime and identify the general area where it occurred. Rather, such a warrant is more akin to the general warrant in *Wilkes v. Wood* that identified the crime of seditious libel but did not specify the places to be searched, the papers to be seized, or the persons to arrest. 98 Eng. Rep. 489, 490 (1763). Drawing a circle around the neighborhood to be ransacked does not change the analysis.

The government contends that the initial search ("Step One") satisfied the particularity and probable cause requirements because it specified information "directly tied" to a particular robbery, which of course occurred "at a particular place and time." ECF No. 41 at 13. But it failed to individualize its suspicion and tie that robbery to a particular account or accounts to be searched. That is like permitting the police to search for stolen goods in any place near a theft, to pat down every person in a bar where a crime had been committed, or to search every person in an apartment where illegal drugs may be present--all of which courts have found to be unconstitutional. *See Grumon v. Raymond*, 1 Conn. 40, 43 (1814); *United States v. Glenn, 2009 WL 2390353*, at *5 (S.D. Ga. 2009); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007). It is also strongly reminiscent of the facts in *United States v. Curry*, in which this Court held that police did not have reasonable suspicion to stop Mr. Curry or any of the other men in a group after shots were fired in the general vicinity of where he was walking. No. 3:17CR130, 2018 WL 1384298, at *11 (E.D. Va. Mar. 19, 2018), *rev'd and remanded*, 937 F.3d 363 (4th Cir. 2019), *reh'g en banc granted*, No. 18-4233, 2019 WL 6133704 (4th Cir. Nov. 18, 2019) ("[G]eneralized suspicion and fear cannot substitute for specific and articulable facts . . . that support a

particularized and objective basis for suspecting *the particular person stopped* of criminal activity.") (internal quotations omitted). The government scoffs at the fact that "19 individuals, rather than hundreds or thousands" were affected by Step One of the warrant, ECF No. 41 at 18, but it gives no indication of how many bystanders would have to be searched before the collateral damage becomes too much for the Fourth Amendment to bear. Indeed, the government did not and could not have known how many devices would be affected by such a high-tech fishing expedition. The only thing certain at Step One was that law enforcement intended to search the Google data of many people who were *not* involved in the robbery.

It is not sufficient to respond, as the government does, that the location records of admittedly innocent people are the proper target of a search warrant on the off-chance that they might be useful in reconstructing the scene, identifying potential witnesses, or rebutting potential defenses raised by the robber. ECF No. 41 at 16. This argument proves too much. The issue is not whether there is some evidence to be had, but where the line is between a general warrant and a particularized one. The boilerplate speculation offered by the government would seemingly justify a search of anyone near any crime.

Moreover, the underlying reason the warrant lacks particularity is because the government does not have probable cause to search an unlimited number of unknown people who were near a crime. Probable cause is what makes particularity possible. Without it, there should be no surprise when a warrant also lacks particularity. As the government notes, the "information specified by a warrant must be 'no broader than the probable cause on which it is based.'" ECF No. 41 at 19 (citing *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006)). But here, the distinguishing feature of the warrant application is the absence of any identifiable suspects. Without some

individualized suspicion, it is trying to imagine how the resulting warrant would be anything other than unparticularized.

Contrary to the government's assertion, the warrant application established no probable cause for any of the Google data it obtained. Mere proximity to crime is not probable cause of criminal activity. The government points to the so-called "Playpen warrant" as precedent for its actions here, *Id.* at 20, but unlike the Playpen cases, there was no honeypot in this case—only a dragnet. The Playpen warrant was "based on probable cause to search any computer logging into [a child pornography website]." *Id.* at 20 (quoting *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016)). The suspicion generated as a result of logging in to such a website has been a critical element in decisions upholding that warrant's constitutionality. See, e.g., *Matish*, 193 F. Supp. 3d at 603 (finding that the "chances of someone innocently discovering, registering for, and entering Playpen were slim" because of the "numerous affirmative steps that one must take to even find Playpen on the Tor network" that make it "extremely unlikely for someone to stumble innocently upon Playpen"); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that to access Playpen, a user must download Tor and enter a 16-character URL consisting of random letters and numbers, as well as enter a username and password to proceed past a welcome page that "was suggestive enough that Playpen's content would be apparent" to any visitor). In this case, however, there is no argument that using Google services or being near the Call Federal Credit Union is somehow inherently suspicious. Instead, a crime was committed, law enforcement had no suspects, and the government simply cast a dragnet. The prevalence of Android phones is not probable cause to search any Google users that happen to be nearby. And

the absence of any individualized suspicion, let alone probable cause, at Step One renders the entire warrant unconstitutional.[5]

The second phase of the warrant ("Step Two") fares even worse. The government asserts that the warrant was "remarkably limited" because it obtained the location information for nine individuals over a two-hour interval, regardless of whether they were inside or outside the 150-meter radius. ECF No. 41 at 13. Indeed, the government commends itself for seizing "less than the maximum quantity of location and identity information that the warrant authorized." ECF No. 41 at 18. But this argument only gives lie to the entire three-step process. According to the government, the warrant authorized the government to seize "identity information and two hours of location data for *all individuals* present at the site of the robbery during the hour of the robbery." *Id.* at 19 (emphasis added). The warrant, however, is not so clear on this point.

The impression one gets from reading the warrant application is that the three-step process matters—that it is a means of protecting the privacy of bystanders by using "anonymized"[6] data to "narrow down the list" before obtaining additional records in Step Two, and then de-anonymized identity information in the third phase ("Step Three"). But the government, in its requests to Google and in a careful reading of Attachment II, said that they were actually entitled to Step 2 and Step 3 data on *everyone* snared in Step 1, no narrowing required. The warrant only says that law enforcement will "attempt" to narrow the list in Steps 2 and 3. *See* Warrant

[5] The government invites this Court to "sever the second step of the warrant and to suppress second-step information" only, ECF No. 41 at 20, but to do so would condone the digital equivalent of a general warrant that lacked particularity from the outset. *See, e.g., United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").

[6] Mr. Chatrie does not concede that this data is not personally identifiable.

Attachment I at 1-2; Warrant Attachment II at 2-3. The verb "attempt" appears six times, doing quite a lot of work.

The government did in fact request the "maximum" amount of data—twice. In two emails to Google following the production of Stage One records, the government asked for "additional location data and subscriber info" for all 19 devices identified in step one. *See* Ex. A at 1; Ex. B at 1. Google did not respond to either of these requests. It was not until the government sent a third email requesting additional data on just nine devices that Google produced more records. *See* Ex. C (Third Step 2 Request) at 1. This is not to suggest that the government did not "attempt" to narrow down the list. Indeed, the government twice tells Google, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but then requested additional information on all 19 anyway. *See* Ex. A at 1; Ex. B at 1.

It is unclear whether the practical realties of the three-step process were apparent to the issuing magistrate. It was certainly not clear to Mr. Chatrie prior to reviewing the negotiations between Google and law enforcement over the data to be produced in Step Two. The critical point, however, is that it was up to Google to decide whether the additional search was "reasonable." *Id.* That is a question that the Constitution makes clear is for a neutral and detached magistrate, not Google. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356). In reality, the government would have obtained the "maximum" amount of data authorized had Google not enforced the warrant's strong suggestion that law enforcement should be required to first "narrow down the list." *See* Ex. A at 1; Ex. B at 1. Google, not the government, deserves commendation

for somewhat limiting the scope of this dragnet search—but it is not and should not be their job to do so.

Put simply, the government lacked probable cause to search any individual's location data, so law enforcement sought to search a broad swath of everyone's data in the area of the robbery. Without sufficient probable cause, the warrant was doomed from the start, as further evinced by its equal lack of particularity. The government's "attempt" to "narrow down the list" was merely cosmetic, masking its multiple grabs for the "maximum" amount of data that it believed investigators was entitled to. Law enforcement's emails to Google clearly demonstrate how the government viewed the three-step process as no more than window dressing. Instead, the government put Google in the role of magistrate, deferring to Silicon Valley to determine what was "reasonable." *See* Ex. A at 1; Ex. B at 1. Such a delegation of constitutional authority is contrary to the Fourth Amendment, demonstrating the profound absence of probable cause or particularity in this case.

III. The warrant was *void ab initio*.

The government seeks to sidestep the unlimited breadth of the warrant by arguing that Mr. Chatrie "lacks standing to challenge the government's acquisition of others' location information." ECF No. 41 at 12. But Mr. Chatrie is not asserting the Fourth Amendment rights of others; he is asserting his own. The unlimited breadth of the warrant bears directly on its absence of particularity, rendering it an unconstitutional general warrant that was *void ab initio*—invalid from the beginning. *See Groh*, 540 U.S. at 558 (finding a warrant "so obviously deficient" in particularity that "we must regard the search as 'warrantless' within the meaning of our case law.").

The history of the Fourth Amendment and the framers of the Constitution make this very clear. For example, "[w]hen James Otis, Jr., delivered his courtroom oration against writs of

assistance in 1761," he argued that "the writs … were void as a form of general warrant." *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting). Lord Camden's judgment in *Entick*, one of the pillars of English liberty and a catalyst for the Fourth Amendment, similarly held a general warrant to be "illegal and void." 19 How. St. Tr. 1029; *see Boyd*, 116 U.S. at 616 (citing this holding and noting that "the principles laid down in [*Entick*] affect the very essence of constitutional liberty and security."); *State Tax Comm'n v. Tenn. Coal, Iron & R. Co.*, 89 So. 179, 182 (Ala. 1921) (noting *Entick*'s holding that "the general warrants issued by the Secretary of State were, under such circumstances there outlined, declared illegal and void."). And when a warrant is void, "potential questions of 'harmlessness'" do not matter. *United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring). The geofence warrant violated Mr. Chatrie's Fourth Amendment rights, not just the rights of bystanders.

IV. The good faith doctrine does not apply.

The *Leon* good faith exception to the exclusionary rule does not apply to evidence discovered as a result of an arrest premised upon a warrant that was *void ab initio*. As the *Leon* Court explained, "in so limiting the suppression remedy, we leave untouched the probable-cause standard and the various requirements for a valid warrant." 468 U.S. 897, 923-24 (1984). Thus, the good-faith exception is inapplicable to warrants that do not meet the probable cause and particularity requirements. While the Fourth Circuit has applied the good faith exception to warrants authorized by magistrates lacking jurisdiction, *McLamb*, 880 F.3d at 691, the Circuit did so because suppression would not have appreciably deterred police misconduct. *See United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019). By contrast, the Fourth Circuit has never applied the good faith doctrine to a general warrant, as suppression serves the goal of deterring police from seeking such intentionally overbroad and unparticularized warrants in the future. *Leon* may excuse

a deficiency in the language of a warrant that is subsequently invalidated, but it cannot excuse a general warrant that is void at its inception. To hold otherwise would incentivize the kind of "systemic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring v. United States*, 555 U.S. 135, 144 (2009).

Even if *Leon* were to apply in this case, evidence from an unconstitutional search should still be suppressed in at least four circumstances, three of which are relevant here. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

First, magistrate issuing the geofence warrant "abandoned his judicial role" by granting immense discretion to the executing officers to decide what Google data to search, and so "no reasonably well trained officer should [have] rel[ied] on the warrant." *See id.* (citing *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979)). *Lo-Ji Sales* determined that a "Town Justice" abandoned his judicial role when he accompanied the police to execute a warrant for obscene material at a store and granted the police immense discretion in seizing materials. 442 U.S. at 326-27. "When he ordered an item seized because he believed it was obscene, he instructed the police officers to seize all 'similar' items as well, leaving determination of what was 'similar' to the officer's [sic] discretion." *Id.* at 327. "The Fourth Amendment does not permit such action," nor such "open-ended warrants." *Id.* at 325. Among other problems, this grant of discretion prevents the magistrate from "verify[ing] that the inventory prepared by the police . . . accurately reflected what he had ordered seized." *Id.* at 327. Here, the warrant left it up to law enforcement and Google to decide which devices would be subject to further search in Steps 2 and 3. "The Fourth Amendment does not permit such action," reserving this function for the judiciary. *See id.* at 325. Here, the court would have no way of determining whether the data obtained in Steps 2 and 3 "accurately reflected" what the magistrate had ordered seized because there were no separate court orders

authorizing them. Instead, it was effectively an "open-ended warrant," *id.*, in which the magistrate abandoned his judicial role.

Second, the good faith exception should not apply because the government's generalized assumptions about cell phone use rendered the geofence warrant "so lacking in indicia of probable cause" to search Mr. Chatrie's data that "official belief in its existence [was] entirely unreasonable." *See Leon*, 468 U.S. at 923 (internal citations and quotations omitted). In *United States v. Doyle*, for example, the Fourth Circuit Court of Appeals held that good faith did not apply when the police searched a house for child pornography with a warrant that contained "remarkably scant evidence … to support a belief that [the defendant] *in fact* possessed child pornography." 650 F.3d 460, 472 (2011) (emphasis added). The district court incorrectly "opined that '[t]he magistrate could reasonably infer'" this possession from the affidavit's recitation of allegations of sexual assault by children and second-hand allegations of possession of child pornography. *Id*. at 471-72. In *Seerden*, by contrast, good faith did apply where the affidavit contained allegations and admissions of the actual crime for which evidence was sought (sexual assault). 916 F.3d 360, 367-68 (4th Cir. 2019). Here, the police presented no evidence that the robber "in fact" had a smartphone, used Android or Google services, and opted-in to location services, and thus that his data was "in fact" in Google's Sensorvault. *See Doyle*, 650 F.3d at 472; ECF No. 41 at 14. Per *Doyle*, this Court cannot "reasonably infer" this fact from the government's generalized assumptions about cell phone use and should instead hold that any "belief in [the] existence [of probable cause for the warrant was] entirely unreasonable." *See Doyle*, 650 F.3d at 471; *see Leon*, 468 U.S. at 923.

Third, good faith should not apply because the geofence warrant was "facially deficient." *See Leon*, 468 U.S. at 923. It sought unfettered discretion to search deeply private data of an

unlimited number of people, and was so lacking in probable cause and particularity that "the executing officers [could not have] reasonably presume[d] it to be valid." *See id*. The government's attempt to evade this problem with *McLamb* is unpersuasive. In *McLamb*, the court found that "the boundaries of a magistrate judge's jurisdiction in the context of remote access warrant" was not clear at the time the agent applied for the warrant. 880 F.3d at 691. In those very limited circumstances, the court looked to the agent's consultation with attorneys from a specialized section within DOJ as evidence of good faith. Here, the watershed decision in *Carpenter* provided significant guidance for officers in this case. This Court cannot allow a reference to consulting with a government attorney to subsume the Fourth Amendment's requirement that a neutral and detached magistrate decide whether to issue the warrant.

As the Supreme Court recognized many decades ago, the Fourth Amendment requires a "neutral and detached" judge to find probable cause because the investigating officers are engaged in "the often competitive enterprise of ferreting out crime." *Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971). "[T]he whole point of the basic rule . . . is that prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations—the 'competitive enterprise' that must rightly engage their single-minded attention." *Id.* at 450. Thus, it is the role of only the courts to enforce the constitutional requirement of particularity. To adopt the government's position here that consulting with members of the prosecution team is sufficient to establish good faith would completely eviscerate a clear protection that the Fourth Amendment in its own words requires.

CONCLUSION

The geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, the unconstitutionality of which should have been

readily apparent. For the foregoing reasons, Mr. Chatrie requests that this Court find the warrant void and suppress all of the fruits thereof.

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 December 9, 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