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	)	

REPLY TO GOVERNMENT'S RESPONSE IN OPPOSITION TO MR. CHATRIE'S MOTION FOR SUPPRESSION

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. 207-2.

I. Introduction

The Government primarily argues that nobody has an expectation of privacy in their Location History information. They do so because they cannot—and do not—contest the fact that the warrant here commanded a search of "numerous tens of millions" of people, none of whom the government had probable cause to search individually. It was astoundingly overbroad and lacking particularity.

The government tries to separate its actions from Google's by seeking refuge in a three-step process that required Google to conduct a dragnet search of Location History users. But the government developed this three-step process in partnership with Google. The government wants to reap the results of the geofence search but take no responsibility for its creation and execution. The fact is the government was responsible for every step of the search. Google never conducts searches like this for business purposes and any attempt to equate geofence warrants with Google advertising is unsupported by the facts. Google searched the accounts of tens of millions of people only because they received a warrant commanding it.

It is immaterial that Google could have structured user data to make it easier for the government to search, as the government suggests. This argument also ignores that there is at least one good reason why Google chose to organize the Sensorvault database by user account: because the data belongs to the users who created it. *See* ECF No. 59-1 at 8. Any Location History data that exists, exists only in individual accounts—it is generated by individuals; it belongs to those individuals; it is intended to be private; and so, it makes sense to store it in individual user accounts. As a result, any attempt to identify individuals in any area will necessarily entail the search of tens of millions of individual accounts.

Second, the government minimizes *United States v. Carpenter* and seeks to narrow its holding into insignificance. Instead, it relies on *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), two relics of a bygone era that the Court declined to extend in *Carpenter*. The so-called "third-party" doctrine is simply not on solid footing when it comes to digital searches and seizures, and the government's attempts to liken a geofence warrant to an "invited informant" are similarly out of touch and unpersuasive. The existence of a service agreement does not end the Fourth Amendment inquiry. On the contrary, Timothy Carpenter had an agreement with his cell phone service provider, yet the Supreme Court looked beyond that, considering context, common sense, and the sensitivity of the data, to hold that the sharing of cell phone location data was not truly "voluntary." Here, as Mr. Chatrie has demonstrated, the process of enabling Location History was also not "voluntary" in any meaningful sense.

Location History data is also far more precise than the cell tower data at issue in *Carpenter*. This precision matters because it means that Location History data is more *potent* than CSLI. A little goes a long way; it can reveal the same kind of private information with much fewer data points. A single data point from CSLI may only be capable of revealing which neighborhood or

zip code a device is in. By contrast, a single Location History data point may have GPS-level accuracy, pinpointing a device's location inside of a house or church. That is why defense expert Spencer McInvaille was able to determine the likely identities of at least three other individuals based on the supposedly "anonymized" data provided by Google during steps one and two. That is also why the government now proposes to sever the warrant; they know that even a little bit of "anonymized" data can reveal a wealth of personal information.

A geofence warrant is a digital dragnet. No matter how the government tries to dress it up or break it down, its defining features are overbreadth and lack of particularity. That is precisely why the government sought one here – they had no suspects, and they hoped a geofence search might generate one. Yet the government asks this Court to ignore the dragnet and instead rule that no one, including Mr. Chatrie, has an expectation of privacy in their Location History data. Under the government's logic, there would be no privacy right in virtually any data that involves a third-party. These arguments must be rejected. Mr. Chatrie urges this Court to find that he had an expectation of privacy in his Location History data and suppress the fruits of this modern-day general warrant.

II. Mr. Chatrie Had a Reasonable Expectation of Privacy in His Location History Data

A. The Third-Party Doctrine Does Not Apply

The government contends that the "third-party doctrine" forecloses any expectation of privacy in Location History data, *see* ECF No. 207-2 at 12, but the Supreme Court has never sanctioned a warrantless search of an individual's cell phone location data, let alone the search of millions at once. *See* 138 S. Ct. at 2219 (Court has "shown special solicitude for location information in the third-party context"). Indeed, the Court in *Carpenter* declined to extend the third-party doctrine to similar data and instructed lower courts not to "mechanically" apply old

rules to new technologies. *Id.* Yet that is precisely what the government asks this Court to do: mechanically apply precedent from the 1960s and 70s to the technology of 2021.

The government therefore invites error by likening Location History to an "invited informant," *see* ECF No. 207-2 at 12 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)), as if Google were no different from the guy who Jimmy Hoffa conspired with in his hotel room. The Court found it dispositive that the informant was not only in the suite by invitation, but that "every conversation which he heard was either directed to him or knowingly carried on in his presence." *Hoffa*, 385 U.S. at 302. Location History, by contrast, runs imperceptibly in the background, constantly recording, even if a user is doing nothing on the device. *See* ECF No. 205 at 26.

The government also heavily relies on *Smith v. Maryland*, 442 U.S. 735 (1979). There, the Court found no expectation of privacy in the digits dialed from a landline telephone. 442 U.S. at 742. The Court found it highly significant that callers were actively aware that they were interacting with the phone company when they placed a call, sometimes speaking with an operator, and receiving monthly bills with printouts showing the information collected. *Id.* at 742-45. In this case, by contrast, a user may enable Location History once—perhaps without even realizing it—and have no awareness that it remains on, silently recording, indefinitely. *See* ECF No. 205 at 26. Thus, if a user enabled Location History through the Google Assistant setup process, and then never used Google Assistant once, Location History would still be on and logging data every two or six minutes. *Id.* at 14, 26. Such a user would not know Location History is enabled, let alone how much data is being collected or how to manage it. Appearing to recognize that this was a problematic practice, Google eventually began sending out monthly emails to users who had enabled Location History, but Google has no record of sending such reminders to Mr. Chatrie and concedes that it may not have done so here. *See* ECF No. 205 at 30-31. Moreover, Google does

not bill users for Location History and Google does not compile Location History information for business purposes, unlike the digits dialed in *Smith*. *See* ECF No. 59-1 at 22. Consequently, Location History is not a "business record;" it is user data—content—that belongs to the individuals who created it. *See id.* at 8.

The government's reliance on *Miller* is likewise misplaced. In *Miller*, the Court found no expectation of privacy in checks, deposit slips, and statements because they were "*negotiable instruments*" intended for use in commercial transactions. 425 U.S. at 438 (emphasis added). The Court distinguished them from otherwise "confidential communications." *Id.* Location History data, by contrast, is considered "content" under the Stored Communications Act, *see* 18 U.S.C. § 2703(a) & (b), and Google treats it accordingly. *See* ECF No. 59-1 at 4. And in any event, Location History data is not a "negotiable instrument." No one gets paid in Location History. Rather, Location History is private data belonging to individual users that Google does not provide to advertisers. *See* ECF No. 205 at 9, 35; Tr. at 197 (regardless of the type of advertising, Google "never share[s] anyone's location history with a third party."); *see also Carpenter*, 138 S. Ct. at 2212 (wireless carriers "often sell aggregated location records to data brokers, without individual identifying information").

In sum, Location History is not an "invited informant." It is not a "business record." And it is not a "negotiable instrument." It is, however, significantly more revealing than the bank records in *Miller* or the telephone numbers in *Smith*. *See Carpenter*, 138 S. Ct. at 2217 ("After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."). And it is almost certainly different than whatever Lord Bacon had in mind when declaring that "all subjects … owe to the King tribute and service." ECF No. 207-2 at 13. Rather, Location History data is most like the cell site location information ("CSLI") at issue in *Carpenter*, in which the Supreme Court found the third-party doctrine inapplicable.

B. Mr. Chatrie Did Not "Voluntarily" Convey His Location Information to Google

One reason the *Carpenter* Court did not extend the third-party doctrine to CSLI was that people do not "voluntarily" convey sensitive data to the cell phone service provider in any "meaningful sense." 138 S. Ct. at 2220. Of course, cell phone users sign contracts with cell phone services providers, but the Supreme Court has never allowed such agreements to determine the contours of the Fourth Amendment. *See Smith*, 442 U.S. at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment"). Indeed, the *Carpenter* majority never mentioned the contract or terms of service.[1] Instead, the Court looked to the realities of the relationship between cell phone users and cell phone companies.

Here, the government invites this Court to simply "infer" that Google users intend to enable Location History and disclose dossiers of their every move because "Google provides services that are helpful to the user, like mapping or finding a phone," as opposed to "mere storage." ECF No. 207-2 at 14. Yet the cell phone company in *Carpenter* provided a helpful service as well. It transmitted phone calls and text messages directly to a user's mobile device, which of course required keeping track of where it was at all times. People were aware of this fact, the Court presumed. *See* 138 S. Ct. at 2211-12. Moreover, the records were "generated for commercial purposes," *id.* at 2217, and often sold in aggregate to data brokers for advertising purposes. *Id.* at 2212. Nonetheless, the Court looked to the realities of the digital age and saw that the "voluntary exposure" rationale underlying the third-party doctrine did not "hold up when it comes to CSLI" for two reasons. *Id.* at 2220.

[1] Nevertheless, it is worth reiterating that the Privacy Policies then in effect provided scant information about Location History, mentioning it just twice in two sentences. One described it only as a way to "save and manage location information in your account," while the other said "you can turn on Location History if you want traffic predictions for your daily commute." ECF No. 205 at 26-27 (quoting Def. Ex. 43 at 7-8).

First, "cell phones **and the services they provide** are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* at 2220 (quoting *Riley*, 573 U.S. at 385) (emphasis added). There can be no serious dispute that this remains true today, although the government appears to maintain otherwise. *See* ECF No. 207-2 at 24. Their argument seems to be that some features, like Location History and "mapping," are not so indispensable. But *Carpenter* did not intend to limit Fourth Amendment protections to devices that are only capable of making calls and text messages. Instead, *Carpenter* rested on *Riley*, where the Court based its decision on the fact that modern smartphones serve many critical functions beyond making calls. *See Riley*, 573 U.S. at 393. They "are in fact minicomputers that also have the capacity to be used as a telephone." *Id.* And importantly, they "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, **maps**, or newspapers." *Id.* (emphasis added). For most users, these functions are likely to be just as essential as owning a phone in the first place. Indeed, it is difficult to imagine a consumer who would purchase a device now that was incapable of mapping or location services.

Second, the *Carpenter* Court found it significant that cell phones generate CSLI "by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Id.* at 2220. Location History operates the same way once enabled, requiring no further action or interaction with the service as it quietly and constantly logs the phone's location data. As with CSLI, "[v]irtually any activity on the phone"—or no activity at all—generates Location History data, even if the user is asleep. *See* ECF No. 205 at 26; Tr. at 122 ("[T]here were no periods of data not being collected.").

The wrinkle in this case is that Location History is not absolutely required to use features like Google Maps or Google Assistant, for example. And it is technically possible to disable

Location History without disconnecting the device from the cellular network. *Cf. Carpenter*, 138 S. Ct. at 2220. At the same time, however, Google failed to inform users of these options, did not describe the full functioning of Location History, and employed a maze of location settings that made it difficult for ordinary people to understand, let alone control, the location information transmitted to Google. *See* ECF No. 205 at 23-29.

Google used an "opt-in" process that was uninformative at best, and deceptive at worst, nudging users at every turn to enable it without fully realizing what was happening. *See* ECF No. 205 at 29-31. This much is apparent from the high-profile "feedback" Google received and acknowledged from the likes of the United States Senate, the *New York Times*, and the *Associated Press*, not to mention a civil lawsuit led by the Attorney General of Arizona. *See* ECF No. 205 at 29-30. It is also apparent from Google's reforms in response to these criticisms, all of which either came too late to help Mr. Chatrie, or else didn't come at all. *See id.* at 30-31. Furthermore, it is far from clear, based on either of the two possible "consent flows" presented to Mr. Chatrie,[2] that a reasonable user would understand what Location History is, based on the partial sentence provided in the so-called "descriptive text." *See id.* at 11-12. Rather, it would be reasonable to believe that such data would be saved locally on the device itself and not with Google. *See id.* at 24. Users are neither required nor prompted to view additional "copy text" hidden behind an "expansion arrow," and they can enable Location History without ever seeing this information, which is also unilluminating. *See id.* at 13, 25.

As for disabling Location History, there is no way to turn it "off"—only to "pause" it. And even attempting to "pause" it results in an immediate, ominous pop-up warning advising users that

[2] The government maintains that there is only one possible "consent flow" in this case, *see* ECF 207-2 at 16-17, but Google testified that it could not be sure which language Mr. Chatrie would have seen (i.e., the "saves where you go" or "creates a private map" language) because it did not record the "UI" (user interface) on Mr. Chatrie's phone. *See* Tr. at 298; *see also* Def. Ex. 7 at 1-3; ECF No. 205 at 11.

doing so will result in unspecified "limited functionality" on the device. *See* ECF No. 205 at 27-28. Likewise, deleting all Location History records does not stop future collection, *see id.* at 15, and deleting the app used to enable Location History continues to allow collection. *Id.* at 14, 27. Even Google engineers found Google's location controls confusing, *see id.* at 29-30, with one employee emailing a company-wide listserv to ask: "which one of these options (some? all? none?) enter me into the wrongful-arrest lottery;" another wrote, "Add me to the list of Googlers who didn't understand how this worked." *Id.* at 30. Most recently, newly disclosed Google emails demonstrated that Google executives viewed it as a "problem" when users took advantage of easy-to-find privacy settings and then sought to obscure them in the settings menu.[3] This may well explain why Location History has been enabled by "numerous tens of millions" of Google users. It also accounts for any technical differences between Location History and CSLI when assessing whether the data is truly "shared" in a "meaningful sense." *See Carpenter*, 138 S. Ct. at 2220.

At the same time, there may be some users who affirmatively wish to keep a timeline of where they have been. And in such cases, individuals would still enjoy an expectation of privacy in their Location History data because it is their private property—data they create and save about their travels. *See* ECF No. 205 at 31-32. And because Location History tracks users all the time, it necessarily records when they are inside homes, churches, and similarly private locations, *i.e.*, constitutionally-protected spaces. Consequently, any trespass on the privacy of this digital property, especially when it reveals who or what is in a protected space, would trigger Fourth Amendment protections as well. *See* ECF No. 205 at 31-32.

[3] *See* Tyler Sonnemaker, *'Apple is eating our lunch': Google employees admit in lawsuit that the company made it nearly impossible for users to keep their location private*, Business Insider (May 28, 2021), *available at* https://www.businessinsider.com/unredacted-google-lawsuit-docs-detail-efforts-to-collect-user-location-2021-5.

The government dismisses this property-based argument as an invention of Justice Gorsuch's dissent in *Carpenter*. *See* ECF No. 207-2 at 27; ECF No. 41 at 12. But, as Mr. Chatrie has previously explained, *see* ECF No. 48 at 8-10, 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) ("[A]s we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."); *Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("[W]ell into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass."); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Justice Gorsuch was merely recognizing that such an approach would have been an appropriate way to resolve *Carpenter*, had the defendant raised the argument. Mr. Carpenter did not, but Mr. Chatrie has done so consistently and adopts those arguments again. *See* ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21; ECF No. 205 at 32.

C. Location History Data Is Highly Sensitive and Can Be as Precise as GPS

In holding that the third-party doctrine does not apply to CSLI, the *Carpenter* Court considered not just whether people "voluntarily" share their CSLI with service providers, but also whether CSLI was different from the bank records and phone numbers in *Smith* and *Miller*. As the Court explained: "*Smith* and *Miller,* after all, did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate 'expectation of privacy' concerning their contents.'" *Carpenter*, 138 S. Ct. at 2219. And in *Carpenter*, the Court recognized that there "is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* Unlike typical business records, CSLI "provides an intimate window into a person's life, revealing not only his particular

movements, but through them his 'familial, political, professional, religious, and sexual associations." *Id.* at 2217. Consequently, the Court determined that cell phone location records "hold for many Americans the 'privacies of life.'" *Id.* at 2217.

Location History data, no less than CSLI, provides a window into the same "privacies of life." *See* ECF No. 205 at 21-23. The government claims, however, that the data in this case was "not particularity sensitive" because "[n]either presence at a bank nor movements along public roads are particularly sensitive information." ECF No. 207-2 at 25. The government is wrong on three counts. First, the 150-meter geofence fully encompassed the Journey Christian Church, which is where Google placed Mr. Chatrie's phone most of the time. Only two of the data points from step one indicate that Mr. Chatrie was inside the bank. All the other points show him either inside the church or parked just outside of it. *See* Gov. Ex. 1 at 24. Second, because the effective range of the geofence was 387 meters, not 150 meters, the initial search encompassed not just the bank and the church, but all the private residences and businesses nearby, including a hotel. *See* ECF No. 205 at 17-18; Gov. Ex. 1 at 20. Many of these are constitutionally-protected spaces where Fourth Amendment protections are at their greatest. *See, e.g., United States v. Karo*, 468 U.S. 705, 714-15 (1984) ("Searches and seizures inside a home without a warrant are presumptively unreasonable."); *Stoner v. California*, 376 U.S. 483, 486 (1964) (requiring a warrant to search a hotel room). Additionally, the step-two data was not limited by any geofence and did in fact show people in their homes and apartments, in addition to tracking one person to a hospital. *See* ECF No. 205 at 22. Thus, as with CSLI, this kind of information "provides an intimate window into a person's life," revealing not only one's movements, but the "privacies of life" that the Court has sought to secure against "arbitrary power." *Carpenter*, 138 S. Ct. at 2214, 2217.

Third, it does not matter what data the government seized. It had no way of knowing, *ex ante*, what the geofence search would show. They cannot now justify that search based on the data they ultimately seized. But more importantly, it is a fiction that the search has a geographic limit to begin with. As Mr. Chatrie is now aware, a geofence search does not just entail searching the records of a few people in one place; it entails searching *all* Location History users in *any* place, regardless of how investigators draw the circle. *See* ECF No. 205 at 16, 33. Thus, any suggestion that a geofence search does not involve sensitive information misapprehends how it works. The government would have this Court believe that a geofence search is a garden-variety request for a few simple business records. But as in *Carpenter*, this "fails to contend with the seismic shifts in digital technology" that made the search possible in the first place. 138 S. Ct. at 2219. Consequently, the government "is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information." *Id.*

The government's remaining objection is that this case involves two hours of Location History instead of seven days of CSLI. *See* ECF No. 207-2 at 22. But two hours of Location History reveals the "privacies of life," especially when accounting for its greater precision and frequency of collection. Location History is at least as precise as CSLI, but it can also be as accurate as GPS. *See* ECF No. 205 at 20. That is because Google uses multiple data sources to estimate a user's location, including CSLI and GPS, as well as Wi-Fi and Bluetooth. *Id.* at 5. Thus, the precision varies from point to point, depending on the available inputs. *Id.* At the same time, it can do things that even GPS cannot do, like determine a user's elevation and identify the specific floor of the building they are on. Tr. at 372-73. Google also logs Location History data every two to six minutes, regardless of whether the phone is in use. *See* ECF No. 205 at 26.

By contrast, the precision of CSLI "depends on the geographic area covered by the cell site." *Carpenter*, 138 S. Ct. at 2211. This may be sufficient to place a person "within a wedge-shaped sector ranging from one-eighth to four square miles," for example. *Id.* at 2218. Or as the government demonstrated in this case, the coverage area for the three cell sites closest to the bank measures approximately 7 or 8 kilometers by 10 kilometers. Tr. at 528-29. As a result, a single CSLI data point could be used to determine which neighborhood or zip code someone was in, but it would not be accurate enough to identify the block and building. Moreover, even though cell phones 'ping' nearby cell sites several times a minute, service providers only log when the phone makes a connection, by placing a phone call or receiving a text message, for example. *See Carpenter*, 138 S. Ct. at 2211.

These differences between Location History and CSLI are significant because they affect how much data is needed to infer where someone was and what they were doing. While *Carpenter* anticipated that the precision of CSLI would improve, the Court was also faced with the fact that it was necessary to stitch together some minimum amount of CSLI to reveal the "privacies of life." The Court settled on seven days, but this was not a magic number; it was simply the number of days in the record for the shortest court order at issue. *See* 138 S. Ct. at 2266-67 (Gorsuch, J., dissenting). And in reality, that order only produced two days of CSLI. *Id.* at 2212. Moreover, *Carpenter* explicitly declined to say "whether there is any sufficiently limited period of time for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 2217 n.3.

Location History's greater precision and frequency of collection means that less time is needed to reveal the "privacies of life." It might take days of CSLI to piece together a mosaic with enough detail to be so revealing, but it takes just a little Location History to achieve the same

result. In this case, two hours was more than sufficient to identify users in sensitive and constitutionally-protected areas, including Mr. Chatrie in the church. And as Mr. Chatrie explains, the Supreme Court has repeatedly found such short-term searches to run afoul of the Fourth Amendment. *See* ECF No. 104 at 11; ECF No. 205 at 21-22 (citing *Karo*, 468 U.S. at 716, and *Kyllo*, 533 U.S. at 37). In short, *Carpenter* supports finding that Mr. Chatrie had a reasonable expectation of privacy in his Location History data.

III. The Warrant Was Overbroad

The government argues that the geofence warrant was supported by probable cause because "there was a fair probability that Google possessed evidence related to the robbery." ECF No. 207-2 at 29. And the government repeatedly refers to Google as a "witness" to the robbery. *Id.* at 1, 13. But Google neither witnessed the robbery nor independently possessed any evidence of it. Rather, people witnessed the robbery and some of those people possessed relevant Location History data in their Google accounts. The government, however, did not establish probable cause to search a single person's Google account. And they certainly did not establish probable cause to search "numerous tens of millions" of accounts.

Instead, the government engages in a Fourth Amendment slight of hand, substituting Google for the individual users they seek to search. With this trick complete, it might appear sufficient to simply recite the facts of the case, note the ubiquity of cell phones, and cite Google's popularity to establish probable cause. *See* ECF No. 207-2 at 32. But once again, Google is no "witness." Google does not own or control Location History data; users do. Google does not generate or keep Location History data; users do. It belongs to individuals, "numerous tens of millions" of them, and a geofence warrant searches every one of their accounts.[4]

[4] The government maintains that it "need not identify specific suspects," only establish that "evidence will be found in the place to be searched," ECF No. 207-2 at 32, citing *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). But the

Because the government did not establish probable cause to search any of these accounts, they now seek to wash their hands of the massive dragnet they cast. The government does not once mention the "numerous tens of millions" of users it searched. Instead, they describe step one as "filtering" data and attribute the action to Google as if such novel searches were a routine business practice. ECF No. 207-2 at 26, 36, 46. Contrary to the government's claims, however, Google does *not* use Location History for purposes of "radius targeting." *See* ECF No. 205 at 8-9. And regardless of the advertising type, Google "never share[s] anyone's location history with a third party." *See* Tr. 197; ECF. No. 205 at 9.

The government also lays any fault for the scope of the search at Google's feet, calling it "a result of Google's internal data storage practices." *Id.* at 37. But this was no garden-variety warrant. Instead of requesting data from specific users or accounts, which Google can identify and retrieve using unique account identifiers, the government required Google to search every Location History account for relevant data. Or in other words, the government reversed the normal warrant process, searching millions before identifying any suspects or specific accounts. Once again, this is not "equivalent to radius targeting" and is not something Google ever does for purposes of "selling a product," ECF No. 207-2 at 36. It was, plain and simple, an epic dragnet compelled by the government. Location History was not designed for such purposes, *see* ECF 205 at 20, and it does not make a difference that it could have been. The government is responsible for the warrants they execute. They cannot force Google to conduct a dragnet and then disavow the consequences. The fact remains that the government did not establish probable cause to search any of the millions of accounts they Google-searched, rendering the warrant profoundly overbroad.

---

search at issue in *Zurcher* involved photographs of a demonstration taken by a newspaper employee. The newspaper owned those photographs, the photographer was a true witness to the events, and the newspaper office did not also house the private photographs taken by millions of other people. *See Zurcher*, 436 U.S. at 551.

IV. The Warrant Lacked Particularity

The government points to the geofence process as a means of redeeming an otherwise overbroad and unparticularized warrant. It says that the three-step process saves the warrant from unconstitutionality because the object of the search was clear and it was Google who "filtered" (searched) through records belonging to tens of millions of people. Yet the data to be searched and seized was the subject of significant back-and-forth between Google and the government, none of which involved a judge.

First, the search procedure was the product of repeated "engagement" between Google and the Justice Department. Tr. at 476. Google's counsel engaged with the Computer Crimes and Intellectual Property Section to discuss "certain procedures that may be relevant for the way that … Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request." Tr. at 456-57; *see also* ECF 205 at 3-4. It rings hollow, therefore, to suggest that the government was unaware of how Google would interpret the warrant, how many people would be searched in step one, or that the method used would produce a high number of false positives. The affidavit contained none of this information, however, leaving it to the government and Google to follow the procedure they created behind closed doors. Such an understanding is also evident from the plug-and-play nature of the "go by" warrant that originated with CCIPS. *See* ECF No. 205 at 4.

Second, the warrant explicitly empowered the government to determine which users to search further in steps two and three. But the particularity requirement was designed to prevent that kind of officer discretion, as two federal courts in Illinois recently determined. *See* ECF No. 205 at 38-39. In fact, there were multiple emails and phone calls between the government and Google during step two because Google did not believe it was reasonable, as the government

requested, to provide additional Location History data for all 19 users identified in step one. *See id.* at 18-19, 39. The government responds, incredibly, that they had probable cause to seize stage two *and* stage three data for all 19 of these users, meaning two hours of Location History as well as full subscriber information for each account. *See* ECF No. 207-2 at 38-39. But their reliance on the "Playpen" cases is misplaced, *see* ECF 48 at 13-14, and Mr. Chatrie maintains that the government had no probable cause for any account. Furthermore, to read the warrant in this manner would make the entire three-step process superfluous, including the requirement that the initial two rounds of data be produced in "anonymized" form. It also guts the government's argument that this process has any constitutional significance. The warrant therefore lacked particularity at each step of the way in violation of the Fourth Amendment.

V. The Good Faith Exception Does Not Apply

The government's construction of *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) is unsupportable. There, the government received a tip about the location of computer servers hosting a message board called Playpen that allowed visitors to upload and download child pornography. *Id.* at 688. The front page of the message board displayed "two partially clothed, prepubescent girls with their legs spread apart" and was "suggestive enough that Playpen's content would be apparent to any visitor of the welcome page." *Id.* Visitors then had to enter a username and passcode to access the message board. *Id.* Playpen had about 158,000 members. *Id.* Following the tip, the government seized the Playpen servers.

Once the government seized the servers, it tried to obtain identifying information for Playpen's members, but could not because the members accessed the Playpen servers through a browser called Tor designed to conceal a user's location and activity. *Id.* To get around Tor's protections, the FBI used a digital tool that infected the Playpen servers. *Id.* Once an individual

accessed the infected Playpen server, the infected server sent instructions to the Playpen user's computer that allowed the FBI to remotely access information about the user's location and other identifying information. *Id.* at 688-89. The FBI sought a warrant allowing the FBI to install the digital tool on the Playpen servers for thirty days to identify Playpen members who entered a username and passcode within that thirty days. *Id.* at 689. The warrant accurately described the digital tool used and the scope of the intended search. *Id.* at 690.

At the time of the Playpen investigation, magistrate courts differed as to whether Federal Rule of Criminal Procedure 41 allowed a magistrate to issue a search warrant for searches that happened outside of the magistrate's district. *Id.* at 689. Concerned that its use of digital investigative tools exceeded the scope of the jurisdiction of the magistrate who authorized the Playpen search warrant, the FBI officers seeking the warrant discussed concerns about the legality of the Playpen warrant with attorneys within the Department of Justice and the FBI. *Id.* A federal magistrate in this district ultimately authorized the Playpen warrant, which allowed the FBI to use the digital tool to infect the Playpen servers and access identifying information about Playpen's members for thirty days. *Id.* Mr. McLamb was a Playpen member who accessed the Playpen servers within those thirty days. *Id.*

Mr. McLamb challenged the validity of the warrant and argued that *Leon*'s good faith exception to the Fourth Amendment did not apply. The Fourth Circuit, however, applied the good faith exception using the traditional *Leon* analysis. The court observed that there was "no indication" that the magistrate acted as a rubber stamp or that the affidavit in support of the warrant lacked a substantial basis to determine probable cause. *McLamb*, 880 F.3d at 690. It is critical to view those findings in the context of the facts of *McLamb*. First, the warrant confined the search only to members of the Playpen message board who accessed the message board within a thirty-

day timeframe. The welcome page to the message board plainly indicated to all members that entering the site provided access to child pornography, meaning that all members who accessed the site were inherently suspected of engaging in criminal activity. And second, the warrant did not give the FBI liberal discretion in executing the warrant. Those facts clearly separate the Playpen warrant from the geofence warrant in this case.

As to the first point, the warrant in this case authorized a search that is unparalleled in its overbreadth, requiring Google to search the content of accounts belonging to numerous tens of millions of people. All but a few of those individuals inherently are unconnected to the investigation in this case. All but one[5] of those individuals inherently are not suspects in this case. No search—digital or otherwise—can comply with the Fourth Amendment when it authorizes a global hunt through numerous tens of millions of innocent individuals' sensitive data.

As to the second point, the warrant in this case left immense discretion to Google and the government to execute the search. *See supra* at 16-17. This discretion was baked into the warrant, something that has troubled other courts evaluating similar geofence applications. *See, e.g.*, *Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 746 (N.D. Ill. 2020) (denying geofence warrant application, even after amendment, and observing that, unlike geofence warrant, "there was probable cause to believe [in *McLamb*] that anyone reaching the dark website was involved in possessing or trading child pornography, so that agents' discretion was in fact limited to seizing information about individuals as to whom probable cause was established"). The evidence before this Court paints the clearest picture yet as to just how much discretion the

[5] The government's assertions that a co-defendant could have been involved in the case potentially could have been a valid concern in the immediate aftermath of the robbery. But, once the police interviewed witnesses and watched the camera footage from the bank and the church—which the police did long before seeking the geofence warrant in this case, *see* Tr. at 623-25, there was no evidence to support a theory that the bank robber had co-defendants present within the geofence.

warrant left to Google and the government, which alone should preclude finding good faith.

The government very much wants to interpret *McLamb* as creating a new rule that cloaks police officers with good faith if they simply consult with an attorney before submitting a warrant. *See* ECF No. 207-2 at 41-43. *McLamb* adhered to the "traditional" *Leon* good-faith analysis. In discussing the question of the magistrate's jurisdiction to issue a warrant for a search that would inevitably search computers outside of the magistrate's district, the Fourth Circuit observed that one would expect an officer to have consulted with attorneys before seeking a search warrant that used "cutting edge investigative techniques." *McLamb*, 880 F.3d at 690-91. But *McLamb* in no way gave a "good faith" pass to police officers who consult with attorneys before submitting a warrant. Such a rule would render the qualifications in *Leon* inapplicable in every federal case, as federal prosecutors routinely review and edit federal search warrant applications. And such a rule would also do nothing to check the government overreach apparent in this case. The law enforcement community worked hand in hand with Google to develop the discretionary process set forth in the geofence warrant in this case, *see* Tr. at 455-57, 476, and further has no qualms about the unprecedented scope of the search in this case. Thus, it is up to the courts to properly apply the Fourth Amendment in this case and sanction the government overreach in this case through suppression.

VI. Conclusion

The geofence warrant in this case was devoid of probable cause and particularity, casting a digital dragnet that searched tens of millions of people. In effect, it was a general warrant, so obviously deficient that this Court should find it void and suppress all 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

/s/
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org