[redacted]

IN THE UNITED STATES DISTRICT COURT
[redacted]

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal Number:** [redacted]
	)	
[redacted]	)	
Defendant.	)	

MOTION TO SUPPRESS EVIDENCE FROM A GEOFENCE WARRANT

[redacted] though undersigned counsel, moves this Court to suppress Google Location History evidence obtained by a modern-day general warrant, in violation of the Fourth Amendment. The "geofence warrant" searched and seized Google "Location History" data belonging to an unknown number of people after a robbery of [redacted]' Bank in [redacted] Mr. [redacted] had a Fourth Amendment interest in his Location History data, and the warrant was overbroad and lacking particularity under the Fourth Amendment. The FBI seized data beyond the warrant's scope. The application was based on false statements, omitted material facts, and was facially invalid. The good faith doctrine is thus inapplicable, and consequently, the warrant and its fruits should be suppressed.

FACTS

Someone robbed the [redacted]' Bank at [redacted] in [redacted], [redacted] around [redacted] 2018. Surveillance video from a nearby pizza place appeared to show a dye pack exploding in the parking lot and police recovered a dye stained $50 bill from the area. In the videos, police also identified a silver Ford Focus with the same individual and no visible passengers driving away from the bank. The next morning, at around 8:30am, a witness found a $50 bill with red dye [redacted], approximately 0.7 miles from the bank.

Police investigated several leads of suspects other than Mr. [redacted] but made no arrests. Instead, the FBI applied for, and received, a novel geofence warrant for the search and seizure of Google "location history" data from an unspecified number of unknown Google users. *See* Ex. A

[redacted]

(Search Warrant & Application) at 3. The warrant application describes generally that Google collects location data from some users, *id.* at 11; described the bank robbery in one paragraph, *id.* at 12, and asserted that criminals generally use phones to coordinate crimes and take pictures of evidence or contraband, *id.* at 12-13. The application did not refer to any other possible suspects. It provided no evidence that the bank robber in this case had a cell phone. It provided no evidence that the robber had a Google account, let alone one linked to a cell phone. It did not offer any facts to indicate that such a phone would have had Google Location History enabled. And it did not allege any that the robber had such a phone with him at the time of the robbery.

I. Location History

Location History is a Google feature that logs device location data, showing where a user has been with that device. *See* Ex. B (Google Amicus) at 5. When Google saves this data, it associates it with unique user accounts it keeps in the "Sensorvault." Ex. C (McGriff Decl.) at 3. If a user has the Google Location History enabled, then Google estimates the user's device location using GPS data, the signal strength of nearby Wi-Fi networks, Bluetooth beacons, and cell phone towers. Ex. C at 4. Location History is not an "app"; it is a setting on the Google account associated with a device, and it is currently an "opt-in" feature. Once enabled, it records that device's location as often as every two minutes, regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. *See* Ex. D (*Chatrie* Tr.) at 436–37, 513. Approximately one-third of all active Google users have Location History enabled on their accounts. Ex. C. at 4; Ex. D at 205. Google has been unable or unwilling to say exactly how many users this was in 2019, but Google acknowledges that it was at least "numerous tens of millions" of people. *Id.*

Google saves Location History data in each user's "Timeline," Ex. C. at 2, which Google describes as a "digital journal" of a user's locations and travels. Ex. B at 16. Google considers this information to be communications "content" for purposes of the Stored Communications Act, 18

U.S.C. § 2703, requiring the government to obtain a warrant to access it. *See id.* Google also uses Location History data to target advertising based on a user's location, although it obscures individual device information, preventing businesses from being able to track individuals. *See* Ex. D at 197.

Neither the Timeline feature nor the advertising relies on a high degree of accuracy. Rather, Location History is merely Google's ***estimation*** of where a device is. Ex. D at 212. It is not hard data, but is instead Google's best guess at device location based on available information. *See* Ex. B at 10–11 n.7 ("In that respect, LH differs from CSLI [Cell Site Location Information], which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points …"). As Google puts it, Location History is a "probabilistic estimate," and each data point has its own "margin of error." *Id.* Thus, when Google reports a set of estimated latitude/longitude coordinates in Location History, it also reports a "confidence interval," or "Map Display Radius," to indicate Google's confidence in its estimation. Ex. D at 212, 530–31.

On a map, Google shows the coordinates as a small, solid "blue dot." And it shows the Display Radius as a larger "light blue circle" around the dot. *See* Google, *Find and Improve Your Location's Accuracy*, https://support.google.com/maps/answer/2839911 ("The blue dot shows you where you are on the map. When Google Maps isn't sure about your location, you'll see a light blue circle around the blue dot. You might be anywhere within the light blue circle."). *See* Figure 1.

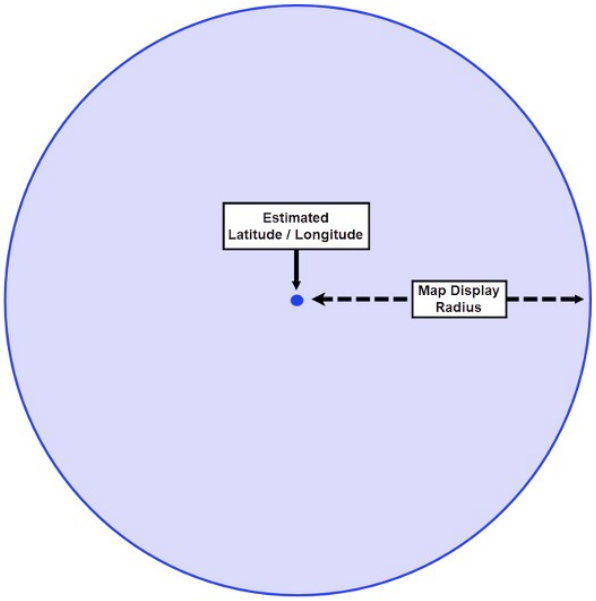

Figure 1

Importantly, Google is equally confident that a device could be anywhere within the Display Radius, *i.e.*, the shaded circle. Ex. D at 214. The estimated coordinates are simply the center point of that circle. It is equally likely that the device is at the center point as anywhere else in the shaded circle, even at the edge. Indeed, Google users may be familiar with this phenomenon, as "in the common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake." *In re Search Warrant Application for Geofence Location Data Stored at Google*, No. 20 M 525, 2020 WL 6343084 at *9 (N.D. Ill. Oct. 29, 2020). The Map Display Radius is not a fixed margin of error; it expands and contracts in accordance with Google's confidence in each location estimation.

Significantly, there is only an "estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot." Ex. C at 8-9. To maintain 68% confidence, Google adjusts the size of the Display Radius. As Google explains, "The smaller the circle, the more certain the app is about your location." Google, *Find and Improve your Location's Accuracy* at 1. By contrast, a large circle means that Google is less confident in a user's location, indicating that they could be anywhere within a much larger area, the product of a larger Display Radius. *See* Ex. D at 213, 530-31. There is always a 32% chance a device is outside of the Display Radius altogether. *See id.* at 213. Or in other words, the odds are almost 1-in-3 that the user's actual location lies beyond the shaded circle.

A confidence interval of 68% is the industry standard, and as Google explains it is "an

[redacted]

approximation sufficient for its intended product uses," namely Timeline and advertising. *See* Ex. D at 581; Ex. G ([redacted] Location History). Because it was not intended to solve crimes, Google warns that its use in geofence warrants risks generating "false positives." Ex. B at 20 n.12. According to Google, "the margin of error associated with LH data means that the government's effort to use this information for purposes for which the LH service was not designed creates a likelihood that the LH data will produce false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." *Id.*

Google is also clear that it does not use Location History to geotarget ads, and that it does not ever share Location History data with advertisers or other third parties. Ex. D at 198; 367-69. This is done for privacy purposes, so that advertisers do not get to see which devices were in the area. *Id.* at 197, 199. Likewise, advertisers cannot go back to Google and ask for more information about where certain devices were before or after they saw an ad or visited a store. *Id.* at 199. In fact, advertisers cannot get any identifiable information about individual Google users. *Id* . at 199.

1. The Geofence Warrant Application Requested, and the Warrant Authorized, A Three-Step Process for Searching and Seizing Users' Location History Data.

a. Step 1

In Step 1, the warrant directed Google to "query location history data" to identify devices in two locations: 1) the [redacted] Bank, and 2) a point on the [redacted] *Id.* at 3-4. The warrant then directed Google to produce "GPS, Wi-Fi or Bluetooth sourced location history data" from devices that "reported a location within" a 150-meter radius of those two points between 4:45 p.m. and 5:05 p.m. *Id.* at 3-5. It also stated that Google "shall" produce this data in "anonymized" form by specifying the "unique device ID" instead of "identifying information."[1] *Id.* at 5.

The two locations included over 20 private homes, a clubhouse, a grocery store, several

[1] As Mr. [redacted] explains below in Section V, the "unique device ID" is not actually "anonymous" data.

restaurants, a law firm, at least two other banks, a gas station, the entrance to a set of professional buildings, an acupuncture office, the parking lot of a daycare, and a mental health treatment provider that specializes in adults with intellectual disabilities. *See* Figure 2.

Location 1 **Location 2**

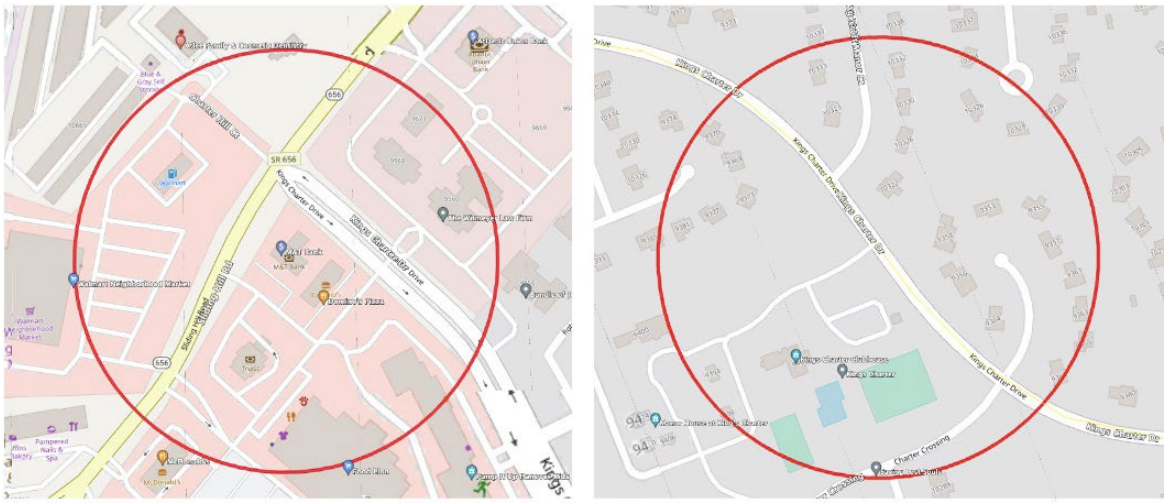

Figure 2

In order to conduct this initial "query," Google was required to search all Google users with Location History enabled, not just those in the area. Thus, Google had to search the "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)" who have Location History enabled. Ex. C at 4. This figure was likely over 500 million in 2019.[2] A geofence warrant requires searching the contents of *every one of these accounts* because there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." Ex. B at 12. Thus, to conduct a geofence search, Google had to "search across all [Location History] journal entries to identify users with potentially responsive data, and then run a computation against every set of coordinates to determine which (Location History] records match the time and space parameters in the warrant." *Id.* at 12-13.

In fact, the geofence warrant required Google to conduct ***two*** searches of "numerous tens

[2] Google said it had over 1.5 billion active users on October 26, 2018, a third of which is 500 million. *See* @gmail, Twitter (Oct. 26, 2018, 9:02), https://twitter.com/gmail/status/1055806807174725633.

of millions" of accounts—one for each location. As a result, to produce the requested records in Step 1, Google had to search the approximately 500 million Google accounts—twice. Discovery reports reveal that it took Google five months to conduct these searches and send the data to the FBI. Mr. [redacted] has requested all communications between Google and the government, which might shed light on the reason for this delay, but the government has yet to produce them.

Google ultimately identified 98 unique Device IDs at Location 1 and 17 unique IDs at Location 2 during the specified timeframe. Three of those IDs appeared at both locations, meaning that there was a total of 112 unique Device IDs identified in this warrant, associated with 111 accounts. The government seized the Step 1 data for these 112 IDs, which contained 352 distinct location points with Display Radii ranging from 3m to 1793m. Figure 3 illustrates these results.

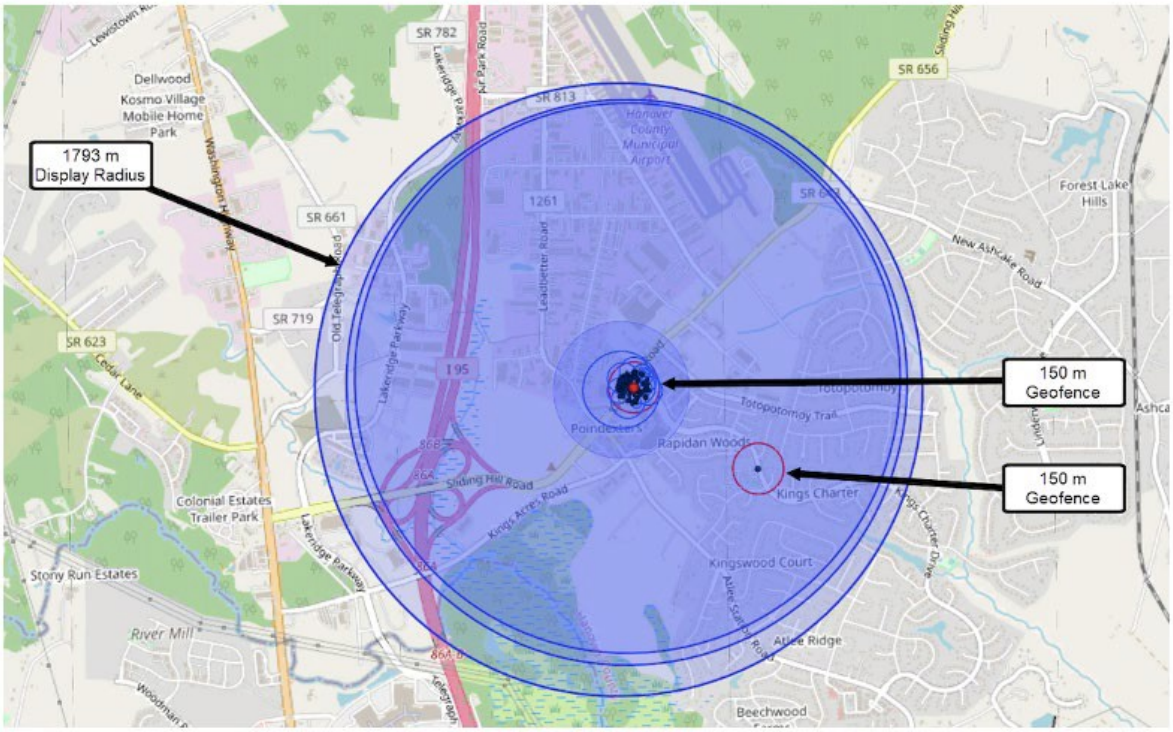

Figure 3

The light blue circles in Figure 3 represent the Display Radius data, meaning that the devices identified as being inside the red geofences were equally as likely (68%) to be anywhere inside the blue circles. They represent the effective range of the geofence data seized at Step 1, and they encompass

[redacted]

an area 71.4 times as large as the area of the two geofence locations put together. The effective range includes: churches; a preschool; pharmacies; a health clinic; a law office; a laser skin removal office; a municipal airport; dance studios; supermarkets; restaurants; construction and home improvement companies; auto repair shops; hundreds of individual homes; and, perhaps obviously, a handful of banks including the one involved here.

b. Step 2

In Step 2, the warrant authorized the government to obtain "additional location coordinates for the Time Period outside of the Target Location." Ex. A at 5. These "contextual location coordinates" sought to track devices outside the geofence described in Step 1, allowing the government to obtain additional location data on devices it deemed "relevant to the investigation." *Id.* at 5. The warrant contained no objective criteria to identify such devices. Instead, the warrant left it up to the FBI to determine whether the additional data to be seized was "relevant." *Id.* at 4.

Here, the FBI seized additional Location History data for six different Device IDs. Two of those six devices were in both locations at Step 1; the FBI did not seek additional information on the third ID. It remains unclear how or why the FBI selected the other four IDs for further scrutiny. It took Google about one month to produce the Step 2 data. The defense has requested, but has not yet received, in discovery copies of all communications between the FBI and Google regarding the warrant that will detail the back-and-forth between Google and the government in this case. Notably, the warrant kept the same "Time Period" in both Steps 1 and 2, limited to 20 minutes around the robbery (4:45 to 5:05 p.m.). But the FBI somehow seized data for all six IDs far beyond that 20-minute window, from 3:45 p.m. to 6:04 p.m.—almost two more hours.

c. Step 3

In Step 3, the government further culled the list and seized from Google the de-anonymized account information for four Device IDs, including the username and subscriber information,

associated email addresses and telephone numbers. *See* Ex. A at 5. Google provided a final file matching each Device ID with its "Gaia ID" as well as records reflecting the associated subscriber information. In this case, the four IDs turned out to be related to just three registered accounts: one for Mr. [redacted] one for another user, and two devices logged into a third Google account. Mr. [redacted] was the only ID in both locations to make it to Step 3. The FBI did not seek Step 3 data on two other IDs reported in both locations. The government has yet to disclose how it determined that those four IDs were relevant to its investigation. Again, the defense has requested, but has not yet received in discovery, copies of communications between the FBI and Google about the Stage 3 returns. Based on the data it obtained from the geofence warrant, the government obtained a warrant for Mr. [redacted] the Google account on [redacted] 2019.

ARGUMENT

The geofence warrant was an unconstitutional search that intruded upon Mr. [redacted] reasonable expectation of privacy in his Google data. For the reasons below, Mr. [redacted] maintains that the warrant was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. The good faith doctrine does not apply, and the warrant was so obviously deficient that it was *void ab initio*. As a result, this Court should suppress the results of the geofence warrant, including all of the fruits thereof.

I. Mr. [redacted] Had a Reasonable Expectation of Privacy in His Location History Data

Mr. [redacted] had a reasonable expectation of privacy in his Location History data following the Supreme Court's landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012), because, like CSLI and GPS data, Location History reveals the "privacies of life." *Carpenter*, 138 S. Ct. at 2214. Although this case involves a shorter duration of data, the precision and always-on nature of Location History makes it even more invasive, requiring less to achieve the same effect. Indeed, just a small amount of Location History

[redacted]

can identify individuals inside of their homes and other private spaces. And as a result, a geofence warrant almost always involves intrusion into these constitutionally protected areas, infringing on fundamental privacy interests recognized by the Court in *United States v. Karo*, 468 U.S. 705, 715-18 (1984), and *United States v. Kyllo*. 533 U.S. 27, 37 (2001).

A. Location History Is At Least As Precise as CSLI, Often Has GPS-Quality Accuracy, and Is Highly Intrusive

Location History data, even small quantities, can reveal the "privacies of life" because of its greater precision and frequency of collection. It is at least as precise as CSLI, but it can also be as accurate as GPS. *See* Ex. B at 10. 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, which vary in their accuracy. *Id.;* Ex. C at 4. In this case, all the estimated Location History points with known data sources derive from either Wi-Fi or GPS signals, which Google states are "capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." *Id.* Furthermore, Location History logs a device's location as often as every two minutes—regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. *Id.* at 436–37, 513.

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. 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. *Id.* 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, *id.* at 2218-19, the Court also faced technology that required stitching 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 timespan for the shortest court order in the record. *See id.* at 2266-67 (Gorsuch, J., dissenting). In fact, that order only produced *two* days of CSLI. *Id.* at 2212. *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. But short-term searches may still be capable of revealing the "privacies of life," *id.* at 2214, which was the main concern in both *Carpenter* and *Jones*.

Although *Jones* and *Carpenter* involved so-called "long-term" searches, what motivated the Court in each case was the risk of exposing information "the indisputably private nature of which takes little imagination to conjure: 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." *Jones,* 565 U.S. at 415 (Sotomayor, J., concurring) (internal quotation omitted); *accord Carpenter*, 138 S. Ct. at 2215. Thus, "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance . . . will require particular attention." *Jones*, 565 U.S. at 415. The same is true for the data here, given that "[a] cell phone faithfully follows its owner beyond public throughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.

Before *Jones* and *Carpenter*, the Court was concerned with short-term location tracking, especially when it reveals information about a private interior space. In *Karo*, using an electronic beeper to track an object inside a private residence was a search. 468 U.S. at 716. In *Kyllo*, using a thermal imaging device to peer through the walls of a private residence was a search despite taking "only a few minutes" and not showing people or activity inside. 533 U.S. at 30, 37.

Location History's greater precision and frequency of collection means that less time is needed

[redacted]

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 end. In this case, the data was more than sufficient to reveal individuals in private homes connected to their WIFI, at the address of a mental health treatment provider, an unrelated bank, and an office park that included a law firm, medical billing company, and acupuncture provider. Although Google initially "anonymized" this data, the FBI could have obtained the subscriber information at any time using a subpoena. *See Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 749 (N.D. Ill. 2020) ("Fuentes Opinion"). Others who have considered geofence warrants have also recognized the private nature of Location History data. *See* Fuentes Opinion, 481 F. Supp. 3d at 737 ("[T]here is much to suggest that *Carpenter*'s holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration."); *Matter of Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *5 n7 (N.D. Ill. July 8, 2020) ("Weisman Opinion") ("The government's inclusion of a large apartment complex in one of its geofences raises additional concerns … that it may obtain location information as to an individual who may be in the privacy of their own residence").

The *en banc* Fourth Circuit also recently confronted a similar retrospective location tracking scheme, and held that citizens whose locations were recorded had a reasonable expectation of privacy. *Leaders of a Beautiful Struggle v. Baltimore Police Dept.* involved a police-contracted surveillance program in which planes flew over Baltimore continuously, capturing high-resolution photographs that depicted over 32 square miles for 12 hours a day. 2 F.4th 330, 334 (4th Cir. 2021). The images were kept for 45 days. *Id.* During that time, when a crime occurred, police could review photographs from the area, and then, just as with a geofence warrant, track individuals and compile reports with images. *Id.* These "tracks" were "often shorter snippets of several hours or less." *Id.* at 342.

The Fourth Circuit held that "*Carpenter* applies squarely to this case" because the data allowed

police to "travel back in time" to observe a target's movements, as if they had "attached an ankle monitor" to every person in the city. *Id.* at 341. This "'retrospective quality of the data' enables police to 'retrace a person's whereabouts,' granting access to otherwise 'unknowable' information." *Id.* at 342. Google location history is far more intrusive than the pixilated surveillance photos in *Leaders*. In fact, Location History data is even more intrusive than aerial surveillance photos, because it records movements *inside* as well as outside, including in private homes. And Location History data can stretch back months or years, for as long as the service has been enabled. Thus, under *Leaders,* as well as *Carpenter*, *Jones*, *Karo*, and *Kyllo*, Mr. [redacted] had a reasonable expectation of privacy in his data.

B. The Third-Party Doctrine Does Not Apply

The so-called "third-party doctrine" does not foreclose finding an expectation of privacy in Location History data. 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 (noting that the Court has "shown special solicitude for location information in the third-party context"). Indeed, the *Carpenter* Court declined to extend the third-party doctrine to similar data and instructed lower courts not to "mechanically" apply old rules to new technologies. *Id.*

To begin with, Location History is not an "invited informant" as in *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). Likewise, Location History is not a "business record," as in *Smith v. Maryland*, 442 U.S. 735 (1979). And Location History is not a "negotiable instrument," as in *United States v. Miller*, 425 U.S. 435, 438 (1976). All of these "third-party doctrine" cases involved situations where individuals were actively aware that they were interacting with another person or business. Here, by contrast, Location History was likely enabled without Mr. [redacted] even realizing it—meaning he would have had no awareness that it was on, silently recording, every two minutes. He would not have known Location History was enabled, let alone how much data was being collected or how to manage it. There would have been no monthly bill to remind him, unlike the digits dialed in *Smith*. *See* Ex. B at

22. And there would have been no deposit slip or receipt from the bank. Rather, Location History data is most like the CSLI at issue in *Carpenter*, in which the Supreme Court found the third-party doctrine inapplicable.

Moreover, Mr. [redacted] did not "voluntarily" convey his Location History data to Google in a meaningful way. Although Location History must be enabled by the user, the process of doing so is unlikely to have been knowing or informed, but perfunctory at best and deceptive at worst. Mr. [redacted] does not yet have information about when Location History was enabled on his account or how. Nonetheless, Mr. [redacted] is aware that in the years preceding the warrant, it was possible to enable Location History in multiple ways, including during the initial setup of a cell phone or during the first use of certain Google applications or services. If enabled in this fashion, a user would have seen one line of text about Location History in a pop-up screen.

One iteration told users that it "Creates a private map of where you go with your signed in devices." Ex. I at 4. A later version said that Location History "Saves where you go with your devices." Ex. J at 19. This was the only text a user would have been required to read, and it was not only inadequate, but outright confusing. Additional information was available on another screen with "copy text," but users would have had to actively seek it out. Even then, what little else Google said about Location History did not adequately convey how it functioned.

First, it was not clear that location data would be saved by Google, as opposed to stored locally on the device. A user might reasonably infer that this "private map" or saved data would be saved only on their device, not with Google. Ex. D at 301, 346 (descriptive text does not make a "distinction" as to whether location information is saved on-device or on Google servers). In fact, that is how certain personalized features work on Apple Maps, available on Apple iPhones. *See* Apple, *Privacy*, https://www.apple.com/privacy/features/ (describing how certain personalized features on Apple Maps "are created using data on your device" to "help[] minimize the amount of data

sent to Apple servers"). Unless a user actively clicked the small "expansion arrow" on the other side of the screen from "Location History," there would be no indication that the data is saved in the cloud on Google's servers. *See* Ex. D at 110,330.[3]

Second, nothing explained that Location History will operate independently, regardless of whether the phone is in use. This is in stark contrast to the facts in *Smith v. Maryland*, where phone users often had to interact with telephone operators using switching equipment to make calls. *See* 442 U.S. at 742. Here, Mr. [redacted] could have enabled Location History by accident well before December 2018. Even if he never again engaged with Google's "location-based services," or any other Google service, Location History would track his location at all times, even while he slept.

Finally, Google's Privacy Policy or Terms of Service have little if any bearing on an individual's Fourth Amendment expectations of privacy. *See United States v. Irving*, 347 F. Supp. 3d 615, 621 (D. Kan. 2018) (rejecting government's argument that defendant had no expectation of privacy in his Facebook account information even though Facebook informed users that it collects user information). That is because Fourth Amendment rights do not rest on the terms of a contract. *See United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018) (recognizing that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement). As the Court said in *Smith*, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." 442 U.S. at 745. Otherwise, by "choosing" to

[3] Additional language may also appear at the bottom of the screen, away from the Location History "descriptive text," and in lighter font. There are two potential versions of this language, *see supra* at 11-12, but both state that this "data may be saved" and that "You can see your data, delete it and change your settings at account.google.com." *Id.* Neither version mentions Location History or location data, nor gives any indication of what it is, let alone that the phone will begin to transmit its location to Google every two minutes in perpetuity, or that this information may be available to the government.

[redacted]

live in the digital age and to participate in the digital world, an individual would be forfeiting any right to privacy in their effects. Such a state of affairs cannot stand when "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *United States v. Di Re,* 332 U.S. 581, 595 (1948)).

As in *Carpenter*, the question is not whether there was an agreement between an individual and a service provider. The question is whether, in a "meaningful sense," users "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements" to the government. *Carpenter*, 138 S. Ct. at 2220. And in the case of Location History, Google's pop-ups and terms of service do not suffice to extinguish users' privacy interest in their account data.

II. Mr. [redacted] Had a Property Interest in His Location History Data

Mr. [redacted] also had a property interest in his Location History data, the digital equivalent of his private "papers and effects." U.S. Const. Amend. IV. Google was a mere bailee of Mr. [redacted] data, and the government converted his property interest in his data through its search and seizure. Supreme Court jurisprudence has long adhered to—and continues to validate—a property-based understanding of the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2213-14 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *Jones*, 565 U.S. at 406-07 ("For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."); *id.* at414 ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.") (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 40 ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass"). Most recently, 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

[redacted]

Gorsuch drew a strong analogy between cell phone location data and mailed letters, which have had an established Fourth Amendment property interest for over a century, whether or not they are held by the post office. *Id.* at 2269. Just as Gmail messages belong to their senders and recipients (and not to Google), so too does Location History data belong to the users who generate them. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010); *see also* Michael J. O'Connor, *Digital Bailments*, 22 U. Pa. J. Const. L. 1271, 1309 (2020) ("Founding sentiment, courts, and scholars all agree: Yes, digital documents are indeed the same papers, even if they use new and unfamiliar ink.").

Mr. [redacted] location information belongs to Mr. [redacted] Google may be responsible for collecting and maintaining it, but Google also understands that it is private user data. For example, Google's privacy policy in effect at the time that Mr. [redacted] created his account consistently refers to user data as "your information," which could be managed, exported, and even deleted from Google's servers at "your" request. *See* Ex. E (May 2018 Google privacy policy). Google even recognizes that its users "expect Google to keep their information safe, even in the event of their death," allowing a user to specify who can have access to his or her records after death, or in the alternative whether Google should delete the data. *See* Ex. F.

These are not "business records." Businesses do not let customers export or delete the company's records at will. Mr. [redacted] merely entrusted his information to Google. The data is heritable, alienable, and exclusive—classic attributes of property. In short, it is Mr. [redacted] (and millions of other citizens') "papers" under the Fourth Amendment, held in trust by Google. 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. [redacted] to keep his data safe. While Google reserves the right to use the data for advertising or development purposes, it also promises not to disclose it to "companies,

[redacted]

organizations, or individuals outside of Google," subject to a short list of explicit exceptions.[4] In other words, Mr. [redacted] 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). The government converted this interest and thus committed a search and seizure under the Fourth Amendment, frustrating Mr. [redacted] right to exclusivity and control over his Location History data.

III. The Warrant Was Overbroad

The geofence warrant here entailed two massive searches of all Google users who had Location History enabled on their devices. Step 1 was an epic dragnet, conducted by Google at the government's direction. The FBI commandeered Google to search through millions of private accounts to determine if any of them contained data of interest. The warrant was therefore unconstitutionally overbroad, a modern-day general warrant. And as if that was not sufficient, the FBI somehow found a way to exceed its scope, seizing an additional two hours of Location History data in Step 2, for which it had no authorization whatsoever.

A. Step 1

Overbreadth concerns probable cause, which is defined as "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates* 462 U.S.

[4] One of these exceptions is "For legal reasons," but – like attorneys' records, the contents of a bank deposit box, or other bailments, 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, e.g.,* Jim Harper, *The Fourth Amendment and Data: Put Privacy Policies in the Trial Record*, The Champion, Jul. 2019, at 21.

213, 238 (1983). And it is axiomatic that a warrant may not authorize a search or seizure broader than the facts supporting its issuance. *See Veeder v. United States*, 252 F. 414, 418 (7th Cir. 1918). Here, however, the government did not have probable cause to search millions of Google accounts. It did not have probable cause to search 112 accounts, six accounts, or even one account. Indeed, it is difficult to imagine that any amount of probable cause could justify a search of "numerous tens of millions" twice over. But in this case, the government had none.

That is because probable cause requires a logical connection, or evidentiary "nexus" between the crime for which probable cause exists and the evidence to be seized, which the government did not demonstrate. *See United States v. Lyles*, 910 F.3d 787, 795 (4th Cir. 2018); *see also* LaFave, 2 Search and Seizure (6th Ed.), § 3.7(d). And according to the Fourth Circuit, this means a nexus between the alleged crime and any phone that is the subject of a warrant. In *Lyles*, for example, the government obtained a warrant to search a house for items including cell phones. 910 F.3d at 790-91. But the Fourth Circuit (Judge Wilkinson, writing for the Court), held the warrant invalid because:

> the warrant application lacked any nexus between cell phones and marijuana possession. There is insufficient reason to believe that any cell phone in the home, no matter who owns it, will reveal evidence pertinent to marijuana possession simply because three marijuana stems were found in a nearby trash bag. At some point an inference becomes, in Fourth Amendment terms, an improbable leap.

Id. at 795. As in *Lyles*, the warrant application here provided no case-specific facts that the robber had a cell phone, was a Google user, or had Location History enabled at the times in question. The affidavit did not allege, even inferentially, that the robber used or possessed a cell phone or acted in concert with anyone else. Ex. A at 12, ¶16. Instead, the application offers only generalizations that when people commit crimes "in concert," they use cell phones to coordinate; and that criminals often take pictures of contraband. Ex. A at 12-13, ¶18. Yet the robbery as alleged was not committed "in concert" with anyone else; the government has only ever alleged that one person was involved in the

robbery. Moreover, the government provides no reason to think that ***photos*** saved on a phone would have anything to do with Location History data stored in a Google account.

Broad conjecture does not amount to probable cause. Probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois* 444 U.S. 85, 91 (1979). For this reason, the D.C. Circuit struck down a warrant authorizing the search of all cell phones in a house, finding that the affidavit "conveyed no reason to think that [the suspect], in particular, owned a cell phone" and no "reason to believe that a phone may contain evidence of a crime." *United States v. Griffith* 867 F.3d 1265, 1272-74 (D.C. Cir. 2017). And in Illinois, Judge Fuentes denied a geofence application on similar grounds. *See In re Information Stored at Premises Controlled by Google* (N.D. Ill. 2020) 481 F. Supp. 3d 730, 754. As here, Judge Fuentes found that government's position "resembles an argument that probable cause exists because those users were found in the place . . . [where] the offense happened," an argument the Supreme Court rejected in *Ybarra. Id.*

Boilerplate assertion that criminals use phones to commit crimes "'cannot substitute for the lack of evidentiary nexus'" between the particular crime for which probable cause exists and the evidence sought. *United States v. Ramirez*, 180 F. Supp. 3d 491, 495 (W.D. Ky. 2016) (quoting *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir.1994)). An officer's training and experience is, of course, relevant to whether an affidavit establishes probable cause. But profile evidence must describe both the characteristics of the type of person that commits the asserted crime, and facts that fit the subject of the search into that profile. For example, this Court held that an officer's affidavit describing in detail the typical practices of drug dealers and alleging relevant facts (three phones in car where common cutting agent found) sufficed to establish a nexus between the phones and the crime. *United States v. Peterson*, 2019 WL 1793138, *12 (E.D. Va. 2019). By contrast, the affidavit here does not discuss the typical practices of bank robbers, or even robbers, or even robbery-related crimes. Instead, it generalizes to, quite literally, all crimes.

From the outset, the government enlisted Google to search untold *millions* of unknown accounts in the largest type of fishing expedition in Fourth Amendment history. The number of individuals affected by this case dwarfs the number of people searched in any other reported criminal opinion. The fact that Google produced records for 112 Device IDs in Step 1 does not diminish the scope of the initial search conducted at the government's behest. On the contrary, it illustrates just how broad the search really was.[5] Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the warrant forced Google to act as an adjunct detective, scouring the accounts of "numerous tens of millions" of users to generate a lead for the government. In short, Step 1 compelled a search of the intimate, private data belonging to millions, in a digital dragnet that snared 112 Device IDs, the data for which the FBI then seized—all without probable cause to search or seize data from a single account. Step 1 was a massive fishing expedition, fatally overbroad from the beginning.

B. Steps 2 & 3

Steps 2 and 3 fare no better. Following Step 1, the government still lacked probable cause to search or seize the Location from a single account (let alone two times "numerous tens of millions"). In Step 2, the government also overstepped the bounds of the warrant itself by seizing nearly 2 hours of additional Location History data for six Device IDs without authorization.

Step 2 allowed the government to seize Location History data beyond the geographic limits of the two 150-meter geofences. However, it only permitted the FBI to do so "for the Time Period" identified in Step 1, *i.e.*, the 20 minutes from 4:45pm to 5:05pm. Ex. A at 4 (". . . provide additional location coordinates for the Time Period that fall outside of the Target Location."). That is not what

[5] Assuming that Google had at least 1.5 billion active users in 2019, a third of which had Location History enabled (500 million) and whom the government searched twice (1 billion), then 112 responsive Device IDs represents a miniscule hit rate of 0.0000112%. In fact, it is even less considering that two Device IDs belonged to one account, meaning 111 accounts were responsive.

happened. Instead, the government seized the data for six Device IDs for a span of 2 hours and 19 minutes, from 3:45 p.m. until after 6:04 p.m., almost 2 hours more data than the warrant authorized. Figure 4 shows the first and last entries in the Step 2 data seized:

	A	B	C	D	E	F	G	H
1	Device ID	Date	Time (America/New_York -05:00)	Latitude	Longitude	Source	Maps Display Radius (m)	
2	[redacted]	[redacted]/2018	15:45:07 (-05:00)	[redacted]	[redacted]	GPS	3	
568	[redacted]	[redacted]/2018	18:01:27 (-05:00)	[redacted]	[redacted]	WIFI	30	

Figure 4

The Step 2 seizure was literally unwarranted and should be treated as such. The seizure of evidence not named in a warrant must be treated as a warrantless seizure. *See Horton v. California*, 496 U.S. 128 (1990) (analyzing warrant for robbery proceeds, seizure of firearms and other evidence of robbery as warrantless seizure under plain view exception). Mr. [redacted] had a Fourth Amendment interest in his Location History data, and no warrant exception applies. On the contrary, the government exhibited a "flagrant disregard" for the terms of the warrant. *United States v. Ruhe*, 191 F.3d 376, 383 (4th Cir. 1999). The timeframe was clear, and the government clearly disregarded it. Suppression of the entire warrant return and its fruits is therefore justified. *Ruhe*, 191 F.3d at 383-84.

Step 3 allowed the government to seize additional identifying information about four Device IDs that the FBI selected from the data it obtained in Steps 1 and 2. Once again, the warrant application did not demonstrate probable cause to search or seize this data. And the government cannot bootstrap its way to probable cause by relying on information it obtained unlawfully in Steps 1 and 2. In fact, Step 3 was a farce. The government could have obtained the subscriber information for any Device ID identified in Steps 1 and 2 simply by issuing a subpoena to Google. *See* Fuentes Opinion, 481 F. Supp. 3d at 749 (finding "no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities."). Indeed, the government has

previously argued that such warrants allow them to seize Step 2 and Step 3 data for *all* devices from Step 1. *See United States v. Chatrie*, 3:19cr130, ECF No. 207-2 at 38-39 (E.D. Va.). As a result, the entire 3-step process is superfluous, including the purported anonymization. All that remains is a search that was fundamentally and thoroughly overbroad, lacking in probable cause for the data it authorized the FBI to seize, and executed without regard for the minimal limitations it proffered.

IV. The Warrant Lacked Particularity

The Fourth Amendment's requirement that warrants "particularly describe[e] . . . the things to be seized," U.S. Const. Amend. IV, means that the description of "what is to be taken" can leave "nothing . . . to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford v. Texas*, 379 U.S. 476 (1965). The description must be provided or confirmed by a "detached" magistrate, "instead of being judged by the officer engaged in the often-competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 13-14 (1948). A magistrate issuing a warrant cannot "assign[] judicial functions to the executive branch." *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 176 (4th Cir. 2019). The warrant here violates the particularity requirement by delegating discretion at each step to Google and the FBI, not a judge, to answer basic critical questions.

A. Step 1

Step 1 fails the particularity requirement because it does not specify the accounts to be searched and the data to be seized. Instead, it concocted a three-step process to mask that is actually searching "numerous tens of millions" of accounts (twice). It also left it to Google and the government to determine whether devices were "within" the geofences.

i. The Warrant Did Not Adequately Identify the Accounts to Be Searched

Geofence warrants differ from other types of police requests. Typical requests compel Google to disclose information for a specific user, while "[g]eofence requests represent a new

[redacted]

and increasingly common form of legal process that is not tied to any known person, user, or account." Ex. B at 11. Here, the warrant did not identify Mr. [redacted] Nor did it identify any of the individuals whose personal information was searched and turned over to the FBI. Instead, the warrant operated in reverse: it required Google to search all accounts with Location History enabled—*i.e.*, "numerous tens of millions"—a portion of which was then seized.

To be sure, there are circumstances where the government need not identify the name of the individual whose information is to be searched and seized. But this is not one of them. So-called "John Doe" warrants—warrants that do not expressly identify the person to be searched or arrested—require something more. To comply with the Fourth Amendment, they must provide "a particularized description of the person to be arrested . . . on the face of the 'John Doe' warrant." *United States v. Jarvis*, 560 F.2d 494, 497 (2d Cir. 1977) (citing *West v. Cabell*, 153 U.S. 78, 86 (1894)).

"All persons" warrants, which aim to search and/or seize all individuals who happen to be at a location during a search—require much more: "probable cause to believe that ***all*** persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004). Here, the government has not alleged any good reason to suspect or believe that all persons present within the 150-meter radius was guilty of committing the robbery. As in *Owens*, such "all persons" language is insufficient if it is "based on nothing more than their proximity to a place where criminal activity *may or may not* have occurred." *See id.* at 276-77.

Finally, anticipatory warrants, which rely on a triggering condition not yet met at the warrant's issuance, require at least more than being in the wrong place at the wrong time. *See United States v. Grubbs*, 547 U.S. 90, 96-97 (holding anticipatory warrants must satisfy two prerequisites—1) "*if* the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place'"; and 2) "there is probable cause to believe the triggering condition *will occur*"—to meet the Fourth Amendment's probable cause requirement); *see*

[redacted]

also United States v. McLamb, 880 F.3d 685, 688 (4th Cir. 2018) (noting that in order to access a child pornography website running FBI malware, a user had to download special software and enter a 16-character URL consisting of random letters and numbers, as well as a username and password).

The warrant here contained no names, and it contained no particularized description of the accounts to be searched and seized. There was no basis to conclude that all 98 of the devices identified in Step 1 were involved in the bank robbery. There was no triggering condition to cabin officer discretion. The warrant simply failed to adequately identify any accounts and thus lacked the particularity required by the Fourth Amendment.

ii. The Warrant Did Not Adequately Identify the Data to Be Seized

Step 1 failed to provide clear instructions on what could be seized. The warrant left it up to Google and the government to decide which users would have their account information handed over to the FBI—the hallmark of an unparticularized warrant. *See Steagald v. United States*, 451 U.S. 204, 220 (1981); *Stanford v. Texas*, 379 U.S. 476, 482-83 (1965) (describing the "battle for individual liberty and privacy" as finally won when British courts stopped the "roving commissions" given authority "to search where they pleased"). Furthermore, in doing so, the warrant ensnared people who had nothing to do with the robbery.

Step 1 returned devices with Map Display Radii that far extended beyond the geofence, making it at least equally as likely that those devices were outside the geofence. *See* Figure 3. Moreover, because Google only aims to be 68% confident in the Map Display Radius, there was a 32% chance that those devices were even farther afield. This situation, as Google explains, "creates a likelihood [of] false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." Ex. B at 20 n.12.

Not only did the government not inform this Court of that likelihood, *see infra* Section V, it also exploited it to increase the amount of data seized. The warrant says Google shall produce

[redacted]

data for "each location point recorded within the Initial Search Parameters." Ex. A at 5. But it does not specify how to determine whether a device is "within" those parameters. Because Location History is only an estimation of where a device was, determining the devices "within" a geofence is much more complicated and open to interpretation than the warrant makes it appear. Determining who is "within" a geofence involves a choice, made without judicial oversight and approval, about whose data gets seized. The government was aware of this fact and stayed silent, leaving it up to Google and investigators to work out among themselves, without input from a judge.

As is apparent from Figure 3, there are very real and measurable consequences to the choice of how to count devices within the geofences here. Although the government may claim that the geofence boundaries limit their discretion, the reality is that Google and the government decided to read the warrant in way that produced data on devices that were as likely to be within 150 meters of the bank as they were to be a mile away. One device had a Display Radius of 1,793 meters (1.1 miles); another had 1,660 meters (1.03 miles); and a third had 1,616 meters (1 mile). *See* Ex. H (Step 1, Location 1 Data). Consequently, the effective range of the warrant was not 150 meters, but 1,793 meters, meaning that at least one device was 68% likely to have been anywhere within 1,793 meters, an area is 71.4 times larger than the two geofences combined.

B. Steps 2 & 3

Steps two and three of the warrant *explicitly* gave the FBI discretion to determine which Google users will be subject to further scrutiny. Step two said: "If additional information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location." Ex. A at 5. This means that the FBI was responsible for identifying what was "relevant" and what else to seize. Here, the FBI identified Mr. [redacted] data as "relevant," and without returning to the court for additional authorization.

[redacted]

And what's more, the FBI somehow obtained an additional two hours of his Location History data in the process, including similar data for five other devices.

In Step 3, the FBI had the opportunity to identify "relevant" accounts, for which Google was required to provide subscriber information, including the account holder's name, email address, and phone number. The warrant stated: "For those device IDs identified as relevant . . . law enforcement may request that Google Provide identifying information . . . for the Google Account associated with each identified device ID." *Id.* at 5. Once again, the warrant left it up to the FBI, not a judge, to determine whose data to seize. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See In re Information Stored at Premises Controlled by Google,* 481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); *In re Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020) ("[T]his multi-step process simply fails to curtail or define the agents' discretion in any meaningful way.").

The Fourth Amendment does not "countenance open-ended warrants, to be completed while a search is being conducted and items seized[.]" *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979). The Warrant Clause requires the determinations of probable cause and particularity be made *ex ante* by a "neutral and detached judicial officer," and not through "the hurried judgment of a law enforcement officer engaged in the often competitive enterprise of ferreting out crime." *Id.* at 326. In Steps 2 and 3, the warrant explicitly empowered officers to determine whose and what data was subject to seizure. But the Fourth Amendment cannot sustain such a warrant because it lacks particularity.

V. The Good Faith Exception Does Not Apply

The Fourth Amendment's most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is

based on "objectively reasonable law enforcement activity." But, *Leon* "good faith" offers no qualifications in four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted as a rubber stamp for the police, *id.* (citing *Gates*, 462 U.S. at 288); (3) where a warrant affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid, *id.* at 923.

The Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id.* at 917, 923. The *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. As set forth above, this geofence 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."). But, even if the Court determines that *Leon* applies here, three of the firm boundaries to the good faith rule that *Leon* recognized clearly apply.

First, the good faith exception should not apply because the geofence warrant was "so lacking in indicia of probable cause" to search for Mr. [redacted] data that it was entirely unreasonable for any objective officer—*i.e.*, one with even a rudimentary understanding of the Fourth Amendment's requirements—to rely on. *See Leon*, 468 U.S. at 923. Police must demonstrate a fair probability that the evidence the police seek will be where they are searching. *See United States v. Doyle*, 650 F.3d 460, 472 (2011) (rejecting good-faith exception where warrant application contained "remarkably scant evidence . . . to support a belief that [the defendant] *in fact* possessed child pornography"); *see also United States v. Church*, 2016 WL 6123235, at *6-7 (E.D. Va. Oct. 18, 2016) (observing that good-faith exception inappropriate where no evidence to connect suspect's house to the crime under

investigation); *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013). That did not happen here. Rather, the police obtained a warrant based on conjecture that Google had location data for a robbery suspect—a suspect the police had no evidence had a cell phone, let alone one with a Google account that had Location History enabled. Obtaining warrants based on conjecture is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

Second, the good faith exception should not apply because the geofence warrant was "facially deficient" and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. As set forth above, "it is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also United States v. Leary*, 846 F.2d 592, 607-09 (10th Cir. 1988) ("reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases).

Third, the warrant application is riddled with false and misleading statements and is severely compromised by material omissions that would have informed the reviewing judge about the effects of authorizing such a warrant. In *Franks*, the Supreme Court observed: "When the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a truthful showing." (original citation omitted). 438 U.S. at 164-65. Where a substantial preliminary showing demonstrates that an affiant made material, false statement with reckless disregard for the truth, the Court must determine whether to strike those portions of the application and if so, whether the remaining content establishes probable cause. *Id.* At 155-56. In considering the veracity of the affidavit in support of the search warrant, the Court must also consider omissions that the affiant made with reckless disregard for the truth. *See United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *United States v. Tate*, 524 F.3d 449, 455 (4th Cir. 2008).

[redacted]

Here, the application says nothing about the numerous tens of millions of accounts to be searched, that the effective radius of the geofence would extend well beyond the authorized 150 meters, that the geofence would capture devices outside of the geofence, or that the approximate device locations were only an estimated 68% accurate. The warrant also falsely claimed that the information returned would be anonymous. Ex. A at 4. While the identifying Device ID is a number rather than a name, it takes little effort to identify an individual person through just a few location points. *See* Ex. D at 62-70; Ex. K (finding in study of 1.5 million people that four location points were enough to identify 95% of individuals in the study). The Device ID also remains the same from warrant to warrant, meaning that the police know who that person is from warrant to warrant. Ex. D at 451-54. This level of omission and misinformation only underscores that the geofence warrant in this case was not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

The government cannot argue it did not understand how this warrant would work because the basic contours of a geofence warrant came from repeated discussions between Google and the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice in 2018. Ex. D at 456-57 ("CCIPS is an agency that . . . our counsel engages with to discuss sort of certain procedures that may be relevant for the way that . . . Google will need to handle these types of requests"); *id.* at 476 (noting repeated "engagement" between CCIPS and Google "help[ed] to socialize the concept of these types of warrants"); *id* at 552-53. The Justice Department even provided "go-by" language to local law enforcement agencies for use in plug-and-play geofence warrant applications. *Id.* at 552-553. For any of these reasons, the Court cannot find that the good-faith exception applies to evidence obtained from the geofence warrant and the fruits flowing therefrom.

CONCLUSION

Thus, Mr. [redacted] moves this Court to suppress the warrant returns as well as their fruits.

[redacted]

Respectfully Submitted,

[redacted]

By: /s/

Laura Koenig
Va. Bar No. 86840
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/

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
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