UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID CHARLES RHINE, Defendant.	Criminal No. 21-CR-687 (RC) MOTION TO SUPPRESS EVIDENCE FLOWING FROM THE GEOFENCE WARRANT

David Charles Rhine, though counsel, moves this Court to suppress Google Location History evidence, as well as the fruits of that 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 thousands of people. Mr. Rhine had a Fourth Amendment interest in his Location History data, and the warrant was overbroad and lacking particularity under the Fourth Amendment.

I. STATEMENT OF FACTS

On January 6, 2021, an estimated tens of thousands of people attended a rally on the National Mall near the White House where then-President Donald Trump spoke.[1] An estimated several to ten thousand people proceeded to protest at the Capitol Building.[2] At the same time, members of Congress and their staff were working inside

[1] Jie Jenny Zou & Erin B. Logan, *Key Facts to Know About the Jan. 6 Insurrection*, L.A. Times, Jan. 5, 2022, https://www.latimes.com/politics/story/2022-01-05/by-the-numbers-jan-6-anniversary.

[2] *See* The Conversation, Interview with Professor Steven Doig: It Is Difficult, if not Impossible to Estimate the Size of the Crowd that Stormed Capitol Hill, Jan. 8, 2021, https://theconversation.com/it-is-difficult-if-not-impossible-to-estimate-the-size-of-the-crowd-that-stormed-capitol-hill-152889.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the Capitol Building to certify the Electoral College vote count for the 2020 presidential election. Capitol Police Officers were present at the Capitol Building and its vicinity for security. At about 2:00 p.m., some people from the protest crowd broke through barriers to enter the Capitol Building, committing various crimes in the process. Also in the crowd were peaceful protestors, observers, and reporters. *See* Dkt. No. 1.

Capitol Police began evacuating congressional staff around 1:30 p.m., and Members of Congress were evacuated around 2:20 p.m., suspending their proceedings. Dkt. No. 1 at 1; Ex. A (Geofence Warrant Step 1) at 15-16. Congress resumed proceedings around 8:00 p.m. *Id*. The Capitol Building itself covers 175,170 square feet of land, approximately 4 acres. Ex A at 13.

Just a week later, the government sought and was granted a "geofence" warrant for data held by Google. In essence, the government compelled google to search *all* accounts with location data for data that fell within a perimeter drawn by the government. The geofence warrant entailed multiple steps, described below. Notably, in its warrant application, the government did not specify whether the perimeter of the geofence area (for this case, the area immediately surrounding and including the Capitol Building) was *visibly* restricted for the full relevant time period, but rather included only a general description of how the Capitol Building may be restricted. *See* Ex. A at 14. Additionally, the government's application for the geofence warrant relied on assumptions to equate presence at the Capitol with criminal activity, hypothesizing, "because of the pandemic, the security surrounding the Capitol in preparation for the Inauguration, the security surrounding the Capitol for the protests of the Certification, and the limited scope of the geographic area covered by this warrant, there will probably be no tourists or bystanders to be found in any of this data." *Id*. at 25.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

As detailed below, this geofence warrant led the government to obtain not only Mr. Rhine's recorded location history, but also his personal subscriber information. The warrant yielded location history information for thousands of people.

A. Google maintains location history for millions of users—the data is not especially precise and Google takes efforts to maintain the privacy of its users' data.

Location History is a Google feature that logs device location data, showing where a user has been with that device. *See* Ex. C (Google Amicus) at 5. When Google saves this data, it associates it with unique user accounts it keeps in the "Sensorvault." Ex. D (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. D 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. E (*Chatrie* Tr.) at 436–37, 513. Approximately one-third of all active Google users have Location History enabled on their accounts. Ex. D. at 4; Ex. E at 205. As of 2019, Google was unable or unwilling to estimate the total number, 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. D. at 2, which Google describes as a "digital journal" of a user's locations and travels. Ex. C 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

information, preventing businesses from being able to track individuals. *See* Ex. E 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. E at 212. It is not hard data, but is instead Google's best guess at device location based on available information. *See* Ex. C 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. E at 212, 530–31.

Importantly, Google is equally confident that a device could be anywhere within the Display Radius, i.e., the shaded circle. Ex. E 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." *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 360 (N.D. Ill. 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Significantly, there is only an "estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot [the display radius]." Ex. D at 8-9. To maintain 68 percent 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, Android, https://support.google.com/maps/answer/2839911 (last visited Oct. 13, 2022). 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. E at 213, 530-31. There is always a 32 percent 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 percent is the industry standard, and as Google explains it is "an approximation sufficient for its intended product uses," namely Timeline and advertising. *See* Ex. E at 581. Because it was not intended to solve crimes, Google warns that its use in geofence warrants risks generating "false positives." Ex. C 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. E 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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.

B. The geofence warrant application requested, and the warrant authorized, a three-step process for searching and seizing users' Location History data.

1. Step 1

The geofence warrant requested and authorized here collected an alarming breadth of personal data. In Step 1, the warrant directed Google to use its location data to "identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the TARGET LOCATION" during a four-and-a-half hour period, from 2:00 p.m. until 6:30 p.m. Ex. A at 6. The target location—the geofence—included the Capitol Building and the area immediately surrounding it, *id*. at 5, which covers approximately 4 acres of land, *id*. at 13. Indeed, the warrant acknowledges that "[t]o identify this data, Google runs a computation against all stored Location History coordinates for ***all Google account holders*** to determine which records match the parameters specified by the warrant." Ex. A at 26 (emphasis added). Though not spelled out with clarity in the warrant itself, the warrant ordered that the list provided in step 1 not include subscriber information, but that such information may be ordered at a later step. *See id*. at 6; *see also id*. at 25 ("This process will initially collect a limited data set that includes only anonymous account identifiers, dates, times, and locations.").

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. D at 4. This figure was likely

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

over 500 million.[3] 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. C 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.

Google ultimately identified 5,653 unique Device IDs that "were or could have been" within the geofence, responsive to the first step of the warrant. Ex. B (step 2 warrant and application) at 6. However, Google ***additionally*** searched location history data that Google preserved the evening of January 6. When searching this data, as opposed to the current data for active users at the time of the search, Google produced a list of 5,716 devices that were or could have been within the geofence during the relevant time period. *Id*. Google ***additionally*** searched location history data that Google preserved on January 7. When searching this data, Google produced a list of 5,721 devices that were or could have been within the geofence during the relevant time period. *Id*. The three lists combined yielded a total of 5,723 unique devices that Google estimated were or could have been in the geofence during the four-and-a-half hour period requested. *Id*. at 7.

These lists that Google provided to the government assigned a device identifier to each device that they kept consistent across all three searches and lists so that "a device that appears in the Geofence at noon, would have the same identifier if it also

[3] 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

appeared in the Geofence at 2:00 p.m." *Id.* at 6. And the lists provided by Google were merely estimates of each device's location:

> Because the location data is an estimate, Google's data also included a margin of error described as a circle around the device location with a certain radius. For example, a device might have a location of 38.89090, -77.00958 with a margin of error radius of 5 meters, meaning that the device could be up to five meters away from the Google location. Google has set a goal that the radius accurately capture at least 68% of its users locations. That means that there is up to a 32% chance that the user in any of this data is actually not within the radius surrounding the estimated location and could be somewhere else.

Id. at 7. Defense counsel has not been provided the step 1 geofence return. However, past cases affirm that the display radius (the circle in which Google estimates with 68 percent certainty contains the location of the device) can range up to 387 meters. *See United States v. Chatrie*, No. 3:19CR130, 2022 WL 628905, at *14 (E.D. Va. Mar. 3, 2022). Indeed, even for the geofence warrant return as to Mr. Rhine, only a single data point had a confidence radius of less than 100 feet. *See* Ex. H (geofence warrant return as to Mr. Rhine, Map). Even for that data point, Google was only 68 percent confident that the device in question was within the display radius, which, for that data point (with a display radius under 100 feet) extended outside the Capitol Building. *See id.*

2. Step 2

In this case, the second step of the geofence warrant was also done in bulk, given the lack of specificity as to the people sought. In the initial warrant, the Court ordered Google to make additional lists to eliminate *some* people who were presumptively within the geofence and committed no crimes. First, the warrant ordered Google to make a list of devices within the geofence from 12:00 p.m. to 12:15 p.m. on January 6. And second, the warrant ordered Google to make a list of devices within the geofence from 9:00 p.m. to 9:15 p.m. Ex. A at 6. For these lists too, Google would have to search

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

all users and collect additional data points at times outside the time when the government suspected crimes were committed within the geofence.

Google provided these lists to the government in addition to the lists detailed above. Google identified 176 devices that were or could have been within the geofence between 12:00 p.m. and 12:15 p.m., and 159 devices that were or could have been within the geofence between 9:00 p.m. and 9:15 p.m. Ex. B at 6. The government ultimately subtracted these devices from those that they deemed suspect. *Id*. at 7. However, this still left 5,518 unique devices under the government's suspicion. *See id*. The original warrant contemplated the removal of devices that were present at the window before and after the primary geofence time because the government asserted that the early and late windows were times when no suspects were in the Capitol Building, but legislators and staff were lawfully present. Ex. A at 27. However, the original warrant also indicated that "The government [would] review these lists in order to identify information, if any, that is not evidence of crime (for example, information pertaining to devices moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case)." Ex. A at 6.

Aside from comparing the primary list with the lists for the early and late windows, the government appeared to do no culling of the device list based on movement. Rather, the government used ***other*** criteria to decide which devices to target for a request for subscriber information.

3. Step 3

In step 3, as relevant to this case,[4] the government sought subscriber information—meaning the phone number, google account, or other identifying information associated with the device—for two different categories of people. First,

[4] Discovery indicates that the government later sought substantially more data from geofences in areas next to, but wholly outside of, the Capitol Building. However, Mr. Rhine addresses here the warrants and searches most relevant to his case.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the government sought subscriber information for any device for which there was a single data point that had a display ratio entirely within the geofence. Ex. B at 7. In other words, the government sought identifying information for any device for which Google was 68 percent confident the device was somewhere within the geofence at a single moment during the four-and-a-half hour geofence period. Again, the government equated presence to criminality. The government sought and the warrant ordered Google to provide identifying information on 1,498 devices (and likely people) based on this theory. *See id*.

Second, the government sought identifying subscriber information for any device where location history appeared to have been deleted between January 6 or 7 and January 13, and had at least one data point where even part of the display radius was within the geofence. *See* Ex. B at 7–8. The government agent asserted that such devices likely had evidence of criminality because: "Based on my knowledge, training, and experience, I know that criminals will delete their Google accounts and/or their Google location data after they commit criminal acts to protect themselves from law enforcement." *Id*. at 8. The warrant made no mention of news reports published in January 2021 about WhatsApp sharing data widely that caused many users to reconsider their privacy settings for their digital accounts.[5] Nor was there any mention of the news of the United Kingdom's investigation into Google's changes to its program to replace third-party cookies with its own in-house tracking of users' internet activities.[6] The theory that potentially changed privacy settings or a deleted account

[5] *See, e.g.*, Lily Hay Newman, *WhatsApp Has Shared Your Data with Facebook for Years, Actually*, Wired, Jan. 8, 2021, https://www.wired.com/story/whatsapp-facebook-data-share-notification/; Clare Duffy, *Why Messaging App Signal Is Surging in Popularity Right Now*, CNN Business, Jan. 13, 2021, https://www.cnn.com/2021/01/12/tech/signal-growth-whatsapp-confusion/index.html.

[6] *See, e.g.*, Leo Kelion, *Google Chrome Browser Privacy Plan Investigated in UK*, BBC, Jan. 8, 2021, https://www.bbc.com/news/technology-55219750; Sam Shead, *Google Chrome Changes to Be Investigated by UK Competition Regulator*, CNBC, Jan.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

was indicative of criminality led the government to request identifying information for 37 additional devices (and likely people). Ex. B at 8.

The Court granted the government's warrant request for subscriber information for the over 1,500 devices (and likely people) that met one of these two criteria. *See* Ex. B. And thus, the government obtained Mr. Rhine's Google account identifying information. *See* Exs. G, H, L.

C. The government used the evidence obtained from the geofence warrant to obtain further search warrants regarding Mr. Rhine, and ultimately to seize and search his phone.

On November 5, 2021, the government sought a search warrant for Mr. Rhine, including at his home, and any phone or other digital devices found with him. *See* Ex. M (Rhine Warrant Application); Ex. N (Rhine Warrant).[7] The government ultimately seized Mr. Rhine's cell phone and did a digital extraction. *See* Ex. Q (Rhine Warrant Return).

The warrant application was based on an amalgam of evidence. The government recited second-hand tips, where individuals claimed they had heard some unnamed person say that they heard Mr. Rhine's wife say that he had been at the Capitol on January 6. *See* Ex. M at 12. Notably, the warrant application summarized the primary tipster's report as:

> Information provided by TIPSTER 1 included that on January 6, 2021, Rhine's wife made a post to Facebook that Rhine had entered the Capitol building during the protest. After seeing the post, TIPSTER 1 confronted Rhine about being in the Capitol building and told him he needed to make a report about his part in the entering of the Capitol. According to

8, 2021, https://www.cnbc.com/2021/01/08/google-chrome-changes-to-be-investigated-by-britains-cma-.html.

[7] The government also obtained a warrant to search Mr. Rhine's home based on substantially the same facts. However, no evidence was seized as a result of that search, so it is not attached to this motion.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

> TIPSTER 1 in this tip, Rhine did not deny entering the Capitol building and said the Capitol police moved the barriers to let him into the building.

Ex. M at 12. However, an interview with the tipster as well as text messages of the "confrontation" provided to law enforcement later revealed that (1) the tipster ***never actually saw*** the alleged Facebook post by Mr. Rhine's wife and (2) ***neither Mr. Rhine nor his wife ever claimed he entered the Capitol Building*** during the text "confrontation." See Ex. M at 13–14.

Following receipt of these tips, the government combed video evidence from January 6th to try to identify Mr. Rhine in the footage. Investigators were not able to identify him in the footage. *See* Ex. O (Review of Triage Toolkit Videos). The government looked for other evidence.

The government queried the phone number associated with Mr. Rhine in its previous searches. First, the warrant noted: "on January 6, 2021, in and around the time of the incident, the cell phone associated with . . . RHINE, was identified as having used a cell site consistent with providing service to a geographic area that included the interior of the U.S. Capitol building." Ex. M at 12. Again, this evidence did not narrow the evidence of Mr. Rhine (or really his cell phone's) whereabouts to the suspected crimes.[8]

However, when the government searched Mr. Rhine's number amid the data obtained by the geofence warrant, it was able to determine his estimated path of travel, and the timing of his movements. *See* Ex. M at 13; Ex. G; Ex. H. This narrowed timeline and location information allowed the government to narrow in on particular portions of surveillance video in search of a person who *may* be Mr. Rhine. On this second review, the government followed a timeline for possible identifications of Mr.

[8] Mr. Rhine contends that the warrant and search that yielded this information was also constitutionally suspect. However, if the Court grants Mr. Rhine's motion here, the legality of that search is moot. Mr. Rhine may seek leave to raise arguments related to this search, depending on the Court's ruling on this motion.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Rhine. *See* Ex. P. The government showed various screen shots of the possible Mr. Rhine to one of the tipsters. The tipster did not identify Mr. Rhine on most of the screen shots, but told the government he did identify him in one. Ex. M at 14–15. The government relied on this single identification, along with the timeline obtained from the geofence data, to proffer a timeline of Mr. Rhine's movements in its warrant application. *See id*. at 16–23.

The Court granted the request for the search warrants pertaining to Mr. Rhine based on this affidavit. Ex. N. And, in executing this warrant, the government seized and searched Mr. Rhine's cell phone. Ex. Q.

II. ARGUMENT

The geofence warrant was an unconstitutional search that intruded upon Mr. Rhine's reasonable expectation of privacy in his Google data. This was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. As a result, this Court should suppress the results of the geofence warrant, including all of the fruits thereof.

A. Mr. Rhine had a reasonable expectation of privacy in his location history data.

Mr. Rhine 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 Cell Site Location Information (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 can identify individuals in private spaces, or engaged in personal and protected activities (such as exercising their rights under the First Amendment). And as

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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).

1. Location History is at least as precise as CSLI, may have 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. C 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. D at 4. Google indicates that Location History derived from Wi-Fi or GPS 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 typically 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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 thoroughfares 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*,

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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.

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 Id.* 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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 buildings. 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. Rhine had a reasonable expectation of privacy in his data.

2. 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 Carpenter,* 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. Rhine even realizing it—meaning he

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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. C 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. Rhine 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. Rhine does not yet have information about when Location History was enabled on his account or how. Nonetheless, Mr. Rhine 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 (Google summaries of Location History function) at 4. A later version said that Location History "Saves where you go with your devices." Ex. J (Norwegian Consumer Council Report on Google Location Tracking) 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

saved data would be saved only on their device, not with Google. Ex. E 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/ (last visited Oct. 13, 2022) (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. E at 110, 330.[9]

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. Rhine could have enabled Location History by accident well before January 2021. 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

[9] 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 id*. 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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 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.

B. Mr. Rhine had a property interest in his Location History data.

Mr. Rhine 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. Rhine's 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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*. at 414 ("*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 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. Rhine's location information belongs to Mr. Rhine. 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 consistently refers to user data as "your data" and as "your information," which could be managed, exported, and even deleted from Google's servers at "your" request. *See* Google, Privacy and Terms, https://policies.google.com/privacy?hl=en-US (last visited Oct. 13, 2022). 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

records after death, or in the alternative, whether Google should delete the data. *See* Ex. F (Google disclaimer regarding privacy of a deceased user's account).

These are not "business records." Businesses do not let customers export or delete the company's records at will. Mr. Rhine merely entrusted his information to Google. The data is heritable, alienable, and exclusive—classic attributes of property. In short, it is Mr. Rhine's (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. Rhine, 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, organizations, or individuals outside of Google," subject to a short list of explicit exceptions.[10] In other words, Mr. Rhine 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

[10] 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

converted this interest and thus committed a search and seizure under the Fourth Amendment, frustrating Mr. Rhine's right to exclusivity and control over his Location History data.

C. The Warrant Was Overbroad

The geofence warrant here entailed multiple massive searches of all Google users who had Location History enabled on their devices. Step 1 was a true 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. Google and the government also exceeded the scope of the Step 1 warrant. At Steps 2 and 3, the warrant remained overbroad, as it authorized further intrusive searches (of subscriber information) of thousands of devices which certainly included people involved in no criminal activity.

1. The Step 1 search was overbroad.

Probable cause requires "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates* 462 U.S. 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). Thus, a warrant is overbroad if it authorizes a search that is broader than the items/people for which the affidavit establishes probable cause. Here, the government did not have probable cause to search millions of Google accounts. While there was evidence indicating crimes were committed by some people, the warrant application did not set forth evidence that ***everyone*** present at or near the Capitol Building was guilty of a crime, nor that everyone with a Google account was.[11] Indeed, it is difficult to

[11] Notably, the relevant trespass statute requires entering or remaining "without lawful authority" into a "posted, cordoned off, or otherwise restricted area[,]" among other elements. 18 U.S.C. § 1752(a)(1), (c)(1). As detailed above, the warrant application

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

imagine that any amount of probable cause could justify a search of "numerous tens of millions" of private accounts multiple times. But in this case, the government had none.

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* Fuentes Opinion at 754. As here, Judge Fuentes found that the 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*.

From the outset, the government enlisted Google to search untold millions of unknown accounts in a massive fishing expedition. 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 ultimately snared about 1,500 Device IDs, the data for which the FBI then seized—all without probable cause to search or seize data in question. The Court should find that even step 1 was fatally overbroad from the beginning.

---

does not detail what restrictions were in place on January 6 (as opposed to generally), and the affidavit acknowledges that many people were present with lawful authority.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

2. Steps 2 and 3 were also overbroad.

Steps 2 and 3 fare no better. Following Step 1, the government still lacked probable cause to search or seize the Location History from a single account. In Step 2, the government also overstepped the bounds of the warrant itself by seizing data from *additional* searches that Google did of data it preserved at strategic times, without the apparent consent of its users. Indeed, Google's own policies for Location History convey to users that if they choose to delete Location History, that data is indeed gone (not preserved by Google). *See* Google Account Help, Manage Your Location History, https://support.google.com/accounts/answer/3118687?hl=en&visit_id=638016383612608202-3452514201&p=privpol_lochistory&rd=1#zippy=%2Cuse-a-web-browser (last visited Oct. 17, 2022).

In Step 2, the government seized data outside of the window of time in which it suspected crimes were committed. It seized location data for a window of time well before and well after the geofence time limit. These seizures were intended to identify those people presumptively lawfully within the geofence. However these people—suspected of no crime—***also and specifically*** had their private Location History data searched at Step 2. One of these control windows was at 9:00 p.m. This is a time when people can be expected to be at their home, hotel room, or otherwise enjoying personal time (for example, at a bar or social location, at an AA meeting, etc.). Not only did this search invade sensitive and private information, but it easily indicated the identities of the device IDs provided by google.

Indeed, discovering the likely identities or affiliations of the device IDs was the precise purpose for the control window searches of Location History data at 12:00 p.m. and 9:00 p.m. *See* Ex. A at 27. These searches were intended to identify people who were *likely* members of Congress or congressional staff. *See id.*; Ex. B at 7. Even the "anonymized" data provided at Step 2 would easily be expected to disclose a person's

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

residence, given the hour of the search. This is not only sensitive information, but also identifying information. And by the terms of its own warrant applications, the government did not have probable cause to believe that every device searched at this point belonged to someone who had committed a crime.

Step 3 allowed the government to seize additional identifying information about over 1,500 device IDs that the government 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. The government made no meaningful showing of probable cause in its follow up warrant affidavit. *See* Ex. B. Indeed, the government has previously argued that initial geofence warrants allow them to seize Step 2 and Step 3 data for all devices from Step 1. *See United States v. Chatrie*, 3:19-cr-130, ECF No. 207-2 at 38-39 (E.D. Va.). The government narrowed its list only to devices that Google believed were 68 percent likely to have been within the geofence for a moment during a four-and-a-half hour period. The government also sought information on any device that *might* have been within the geofence and appeared to have deleted its Location History function or Google account. *See generally* Ex. B. The government did nothing to control for lawful, peaceful protestors, reporters, law enforcement, paramedics, or observers amongst these devices. The assertion that *many* of the devices may belong to people who engaged in criminal conduct is not sufficient to justify the additional search of the subscriber information for *all* of these devices.

D. 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

"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). 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.

1. The warrants 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 and increasingly common form of legal process that is not tied to any known person, user, or account." Ex. C at 11. Here, the warrant did not identify Mr. Rhine. Nor did it identify the thousands of other individuals whose personal information was searched and turned over to the government. 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.

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 (multiple times). It also left it to Google and the government to determine whether devices were "within" the geofence.

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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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:

> a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person. . . . Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.

Ybarra, 444 U.S. at 91. Here, the government has acknowledged that not *every person* present within the geofence was likely involved in criminal conduct. Yet it's supposed narrowing efforts are both unduly intrusive, and only *potentially* exclude from yet further searches a small set of government workers present on January 6.

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 (2006) (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).

The warrant here contained no particularized description of the accounts to be searched and seized. There was no basis to conclude that all of the thousands of people *possibly* present within the geofence had committed crimes. 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.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

2. The warrants did not adequately identify the data to be seized.

Step 1 provided exceedingly broad criteria for the data to be seized (discussed above). And Step 2 and Step 3 failed to provide clear instructions on what further could be seized. The warrant left it up to Google and the government (largely the government) to decide which users would have their subscriber information handed over to the government—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"). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search," the Supreme Court has said, "the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

Step 1 returned devices for which any part of the display radius was within the geofence during the four-and-a-half hour period. Given the potential size of the display radii, this easily may have picked up devices that were hundreds of yards away from the Capitol Building. And even then, or for devices that more squarely appeared within the geofence, Google's display radii only represent their *hope and estimate* that a device is within the display radius 68 percent of the time. So even a device that Location History most strongly suggested was within the geofence had a 32 percent chance of actually being located elsewhere. 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. C at 20 n.12.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

And at Steps 2 and 3, the only clear criteria approved by the Court for narrowing devices for which subscriber information would be seized was to eliminate devices that also appeared within the geofence during one of the control periods. As discussed above, this only eliminated a small number of likely government employees. The government elected to use Google's display radii to narrow some devices.

Yet even for devices that were only *possibly* within the geofence, the government also seized subscriber information if Google's searches of multiple datasets. In this respect, the government *exceeded* the bounds of the Search Warrant. These additional datasets were not Google's Location History—data it held as bailee of its users and subject to control by its users. Rather, this was data that Google strategically saved, apparently without its users consent, and then provided to the Government even when users had specifically asked their bailee to delete that data prior to this warrant. Indeed—this unwarranted search was used to find evidence beyond that which the warrant application asked for: namely, evidence of whether a user had deleted their Location History or Google Account. The government may claim that this was all within the bounds of the warrant. But such claim illustrates the warrant's fatal lack of particularity.

Even the government's "narrowed" warrant certainly left innocent people (and their devices) subject to further invasion of privacy. And these bases for narrowing depend on Google's calculations, the government's speculation, and prior searches in excess of the original warrant.

Courts have repeatedly held that the Court must be more involved in narrowing at steps 2 and 3, even in far narrower cases. 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*

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

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."). This is because "[t]he Fourth Amendment's particularity requirement has three components: a warrant 'must identify the specific offense' for which law enforcement has established probable cause; it must 'describe the place to be searched'; and it must "specify the 'items to be seized by their relation to designated crimes.'" *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523, 528 (D.D.C. 2018) (quoting *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013)).

Unlike in some prior cases, in this case, court intervention was required before Google revealed subscriber information. However, as detailed above, the court accepted a very simplistic narrowing procedure by the government that was unlikely to remove innocent devices from the list subject to further invasion of privacy, and that depended in part on a search in excess of the original warrant.

Additionally, the items to be seized at Step 3 lack particularity, and include, for example: "Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or ***unknowingly***) the commission of the criminal activity under investigation; or (ii) communicated with any PROVIDER account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;" "Information that constitutes evidence indicating state of mind (e.g., intent, absence of mistake)[;]" and "Information that constitutes evidence of any conspiracy, planning, or preparation to commit those offenses[.]" Ex. A at 8–9. Some requested information is ***not*** evidence of a crime, let alone a particular crime, and the affidavit did not provide a basis to believe that evidence of conspiracy would be found in Google accounts. The breadth and vagaries

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

of the items to be seized was an invitation to do a general search of the private papers—Google account—of anyone who may have been in or near the geofence.

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 the government and/or Google to determine whose and what data was subject to seizure. But the Fourth Amendment cannot sustain such a warrant because it lacks particularity.

E. The geofence data itself as well as its fruits—including evidence obtained by the search warrant for Mr. Rhine's home, property, and phone—must be suppressed.

The fruits of a Fourth Amendment violation are not admissible at trial. *See Wong Sun v. United States*, 371 U.S. 471, 484–88 (1963). The exclusionary rule prohibits the government from introducing in its case in chief evidence obtained in violation of the Fourth Amendment. *See, e.g.*, *Mapp v. Ohio*, 367 U.S. 643, 655 (1961); *Weeks v. United States*, 232 U.S. 383, 398 (1914). Evidentiary exclusion "compel[s] respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard" the Fourth Amendment's commands. *Elkins v. United States*, 364 U.S. 206, 217, 80 S. Ct. 1437, 4 L.Ed.2d 1669 (1960). Thus, evidence resulting from a Fourth Amendment violation should be excluded unless the causal connection is "too attenuated to justify exclusion[.]" *Hudson v. Michigan*, 547 U.S. 586, 592 (2006) (citing *United States v. Ceccolini*, 435 U.S. 268, 274 (1978)).

When excising the geofence evidence from the warrant application to search Mr. Rhine, his home, and his personal digital devices, the affidavit fails to establish

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

probable cause to justify the warrant. The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause." U.S. CONST. amend. IV. To comply with that prescription, the affidavit in support of a request for a warrant must provide a "substantial basis for concluding that probable cause existed." *United States v. Warren*, 42 F.3d 647, 652 (D.C.Cir.1994) (quoting *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983)). The task of a judge reviewing an affidavit for probable cause "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238.

In reviewing a warrant application, the Court must consider the totality of the circumstances. Ultimately the Magistrate Judge (or other Court) must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238.

Here, without the geofence evidence, the affidavit lacked evidence that Mr. Rhine committed any crime. The affidavit contained tips by two people with no tested history of providing information to the government. Neither of these tipsters had direct knowledge of Mr. Rhine's whereabouts or actions on January 6, 2022. Indeed, neither had even meaningful *second-hand* information. Rather, one tipster claimed to hear only third- or fourth-hand information that they had heard from other people that they had heard from Mr. Rhine's wife that he had been at the Capitol Building and gone inside on January 6, 2021. The lack of information about the tipster, and the third- to fourth-hand basis for this tipster's claimed knowledge provide little indicia of reliability.

The other tipster demonstrated his unreliability by initially over-reporting the basis for his knowledge, reporting initially that Mr. Rhine *had* entered the building and

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

his wife had claimed as much in a Facebook post, and that Mr. Rhine told the tipster, upon being confronted, that police moved barriers to let *him* enter the building. Ex. M at 12. However, when law enforcement went to interview this tipster, he clarified that he never actually saw the alleged Facebook post by Mr. Rhine's wife. And review of Mr. Rhine's actual conversation with the tipster revealed that, in fact, he told the tipster that he saw Capitol Police remove barriers to let "people" in. Ex. M at 13–14. Thus, this tipster, contrary to his claim, had at best second-hand information suggesting Mr. Rhine entered the Capitol Building. And this tipster already demonstrated his inclination to overstate evidence. Again, this tip has minimal indicia of reliability.

Furthermore, the statement regarding the CSLI ("tower dump") obtained from Verizon only indicated that Mr. Rhine's cell phone contacted a "cell site consistent with providing service to a geographic area that included the interior of the U.S. Capitol building." Ex. M at 12. This is an exceedingly vague piece of evidence that does little more than place Mr. Rhine in the general vicinity of the Capitol Building.[12]

Without the geofence evidence, the affidavit at best indicated that Mr. Rhine was in Washington, D.C., in the vicinity of the Capitol Building. Notably, when investigators searched for Mr. Rhine based on the tips alone, they could not locate him in the security footage at the Capitol. *See* Ex. O. Only after establishing more precise estimated locations and a timeline based on the geofence data, did the government investigator identify a person who *could* be Mr. Rhine. And only upon showing these to the tipster who had already exaggerated the strength of his evidence, did that tipster identify one (though not all) of the security footage screenshots provided by the government. *See* Ex. M, P.

[12] To the extent the Court may find to the contrary, Mr. Rhine would seek leave to challenge the warrants used to obtain this data. These were also general warrants, similar in many ways to the flawed geofence warrant challenged here. But if the Court grants the instant motion, a further challenge to the tower dump warrants may be moot.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Without the geofence evidence, and the unreliable identification obtained as a result of that evidence, the warrant affidavit did not establish a "fair probability" that Mr. Rhine entered the Capitol building or committed any crime. *See Gates*, 462 U.S. at 238. Absent the geofence evidence and derivative ID and video screen shots, the warrant affidavit also failed to establish probable cause that a search of Mr. Rhine, his home, and his digital device(s) would yield evidence of a crime.

III. CONCLUSION

The Court should suppress all evidence obtained from the geofence warrant. This includes the Location History data itself, subscriber information, evidence obtained with that subscriber information, and evidence obtained from the Search Warrant for Mr. Rhine, his home, and his digital device(s).

DATED this 17th day of October 2022.

Respectfully submitted,

s/ Rebecca Fish
Assistant Federal Public Defender
Attorney for David Charles Rhine

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

TABLE OF CONTENTS
FOR EXHIBITS

EXH. #	DESCRIPTION
A	***SEALED*** Geofence Warrant - Step 1; Filed: 01/13/21
B	***SEALED*** Geofence Warrant and Application – Step 2 and 3; Filed 01/18/21
C	Google Amicus Curiae Re: Geofence General Warrant *United States v. Chatrie*, 3:19-cr-00130-MHL, dkt. 73; Filed 12/23/19
D	Marlo McGriff Declaration – Google Location History Product Manager *United States v. Chatrie*, 3:19-cr-00130-MHL, dkt. 96-1; Filed 03/11/20
E	*Chatrie* Suppression Hearing Transcripts, March 4-5, 2021, *United States v. Chatrie*, 3:19-cr-00130-MHL, dkt. 201-202; Filed 03/29/21
F	Google disclaimer regarding privacy of a deceased user's account
G	***SEALED*** Geofence Warrant Return Location History as to Mr. Rhine
H	***SEALED*** Geofence Warrant Return Map as to Mr. Rhine
I	Google, Android and Location Tracking History Summaries
J	Norwegian Consumer Council Report on Google Location Tracking, "Every Step You Take-How deceptive design lets Google track users 24/7"
K	"Unique in the Crowd: The privacy bounds of human mobility," Scientific Reports, Published March 25, 2013.
L	***SEALED*** Geofence Follow-Up Warrant Application for Further Subscriber Information; Filed 03/26/21
M	***SEALED*** Rhine Search Warrant Application; Filed 11/05/21
N	***SEALED*** Rhine Issued Search Warrant; Issued 11/05/21
O	***SEALED*** Review of Triage Toolkit Videos Report; Dated 06/23/21
P	***SEALED*** Review of Videos Report; Dated 07/27/21
Q	***SEALED*** Warrant Return for Rhine Warrant; Executed: 11/09/21

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710