UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	
	:	**Case No. 1:22-cr-404 (JEB)**
ISREAL EASTERDAY,	:	
	:	
Defendant.	:	

UNITED STATES' SUPPLEMENT TO ITS OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS GOOGLE GEOFENCE DATA

As the Court requested, the United States respectfully provides the below supplemental factual background in support of its opposition to the defendant's motion to suppress "all information obtained by the government" from Google, Inc. ("Google") pursuant to two judicially authorized federal search warrants. ECF No. 45 ("Def.'s Mot.") at 3-4; *see also* Search Warrant, 1:21-sc-77, ECF No. 3 ("the Initial Google Geofence Warrant") and Search Warrant, 1:21-sc-1660, ECF No. 3 ("the Expanded Google Geofence Warrant") (collectively "the Google Geofence Warrants").

A. Results of the Initial Google Geofence Warrant

i. Obtaining the Initial Geofence Data

On January 6, 2021, government agents sent a preservation letter to Google directing it to maintain a copy of its data as it existed at that time. Government agents took this step because they knew, at the outset of their investigation into that day's riot at the U.S. Capitol building, that it was possible that Google users or employees might delete or alter data that would be relevant to the investigation.

On January 13, 2021, the government applied for – and Magistrate Judge Harvey issued – a geofence warrant directing Google to disclose certain Location History information for Google

accounts [1] that connected to Google's services from a specific geographic area, which corresponded approximately to the boundaries of the U.S. Capitol Building, during three specific time windows on January 6, 2021: 12:00-12:15 p.m. ("the Pre-Riot Control List"), 2:00-6:30 p.m. ("the Initial Riot List"), and 9:00-9:15 p.m. ("the Post-Riot Control List"). *See* 1:21-sc-77, ECF No. 3.[2] The warrant directed Google to disclose an anonymized list of such accounts. The warrant specified that the government would review the anonymized list and confirm that it fell within the scope of its January 6 investigation. Any information that was determined to fall outside the scope would be sealed and excluded from further review.

In response to the Initial Google Geofence Warrant, Google created three lists of anonymized accounts reporting Location History data within the geofence between 2:00 p.m. and 6:30 p.m. (*i.e.* three versions of the Initial Riot List). The first Initial Riot List was based on Google data as it existed on January 13, 2021, and contained 5,653 accounts. The second Initial Riot List was based on data as it existed in the evening of January 6, 2021, and contained 5,716 accounts. The third Initial Riot List was based on Google data as it existed in the morning of January 7, 2021, and contained 5,721 accounts. Users whose data appeared in the January 6 and/or January 7 lists, but not the January 13 list, were suspected of having deleted or hidden their data to avoid identification by law enforcement. There were 70 such unique accounts.

Meanwhile, Google identified 176 accounts that fit the criteria for the Pre-Riot Control List and 159 accounts that fit the criteria for the Post-Riot Control List. The Pre-Riot and Post-Riot

[1] This filing refers to "accounts," not "devices," because it is and was possible for a single device, such as a cellular telephone, to access or connect to multiple Google accounts and thus a single device could generate geofence "hits" for multiple Google accounts.

[2] The warrant and supporting affidavit remain sealed, so the government has not attached either to this filing.

Control Lists overlapped somewhat but not completely; between the two control lists, the government identified 215 accounts that appeared to have been in the Capitol lawfully.

ii. *Culling the Initial Geofence Data*

Aggregating the three lists provided by Google, the government identified 5,723 unique accounts that appeared to have registered within the Capitol building between 2:00 p.m. and 6:30 p.m. on January 6, 2021. To focus its investigation, the government reviewed the anonymized Initial Riot List and sought to eliminate accounts that appeared unlikely to belong to people who committed a crime.[3] The government narrowed and refined the pool of relevant devices in three principal steps.

[3] In Attachment B(I)(d) of the affidavit supporting the Initial Geofence Warrant, 21-sc-77, the government stated that it would review the data provided by Google "to identify information if any, that is not evidence of a crime (for example, information pertaining to devices moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case)." *Id.* (emphasis added). The Court in this case asked the government to explain what it meant by "moving through" or how the government determined that a device was "moving through" the Capitol building "in a manner inconsistent with the facts of the underlying case" when many rioters have been prosecuted for unlawfully entering—and moving through—the Capitol building.

Contrary to the Court's reasonable interpretation, this phrasing does not refer to people "moving through" the U.S. Capitol building by walking through it. Instead, it was aimed at describing the government's conservative approach to dealing with potential margin of error and accuracy issues with Google's data. For example, as Google has explained, even when Google's Location History includes a point and shows a margin of error radius, that radius reflects only a 68% likelihood that the corresponding account/device was located within the radius at the time. *See* Ex. A, McGriff Decl. ¶¶ 24-25; *see also* Declaration of Sarah Rodriguez, *Chatrie*, 2019 WL 8227162, para. 8, 14. Accordingly, the government did not rely on Location History data alone, but instead sought to corroborate it.

In reviewing the Location History data provided by Google in response to the Google Geofence Warrants, the government found that the data indicated some accounts/devices were located in places where surveillance video in fact revealed no one was located or could be located. For example, occasionally the Google Location History data showed that an account/device in an inaccessible place, so no person could have been there, or in a place that surveillance video or other evidence showed was empty at the time that the Google Location History showed an account/device there. In such situations, the agents reviewing the warrant returns considered the device to be "moving through" the Capitol building "in a manner inconsistent with the facts of the underlying case" and culled those accounts.

First, the government compared the Initial Riot List data with the Pre-Riot Control List data and Post-Riot Control List data, striking any accounts from the Initial Riot List that also appeared on one of the control lists. That process eliminated 215 unique accounts, leaving 5,508 unique accounts remaining.

Next, the government eliminated all accounts from the Initial Riot List that did not have at least one location data point where the margin-of-error radius was contained *entirely* within the Capitol's boundaries (*i.e.* the geofence). This process reduced the pool to 1,498 unique accounts. *Id.*

Finally, of the 70 accounts for which the user appeared to have deleted the Location History data between January 6/7 and January 13, the government found that 37 of those accounts had at least one data point that fell within the Geofence but for which some portion of the margin of error radius fell outside the Geofence. Even though those 37 devices did not qualify for inclusion under the government's second refinement step (described above), the government added those 37 accounts back because the suspected deletion of data served as an additional indicator of criminality.

In total, the government thus sought to unmask (*i.e.* de-anonymize) 1,535 unique accounts in response to the Initial Geofence Warrant and submitted an application for a Court Order to that effect pursuant to 18 U.S.C. § 2703(d). On January 18, 2021, Magistrate Judge Harvey issued the requested Order. *See* 21-sc-77, ECF No. 8.

B. Results of the Expanded Geofence Warrant

i. Obtaining the Expanded Geofence Data

On May 21, 2021, the government applied for – and Magistrate Judge Meriweather issued – an expanded geofence warrant directing Google to disclose certain Location History information

for accounts that connected to Google's services from a larger specific geographic area, which corresponded approximately to the boundaries of the restricted areas of the U.S. Capitol grounds, during a wider specific time window on January 6, 2021: 12:00-9:30 p.m. ("the Expanded Riot List"). *See* 1:21-sc-1660, ECF No. 3.[4] Just as before, the warrant directed Google to disclose an anonymized list of such accounts. The warrant specified that the government would review the anonymized list and confirm that it fell within the scope of its January 6 investigation. Any information that was determined to fall outside the scope would be sealed and excluded from further review. In response to the Expanded Geofence Warrant, Google produced a list of 12,370 unique accounts ("the Expanded Riot List").

Additionally, the government believed that it was unlikely that the 215 unique accounts identified via the Pre-Riot Control List and Post-Riot Control List reflected the total number of people who had been legitimately inside the U.S. Capitol building on January 6, 2021, between 2:00 p.m. and 6:30 p.m. while using Google services—such as Congresspeople, their staffs, and law enforcement officers. Accordingly, FBI agents contacted members of the Legislative Branch and relevant law enforcement agencies and asked them to provide the gmail account identifiers of anyone legitimately on Capitol grounds during the riot. As the request was voluntary, some offices and agencies complied while many did not.

ii. *Culling the Expanded Geofence Data*

In response to the Expanded Geofence Warrant, Google produced a list of 12,370 unique devices ("the Expanded Riot List"). The government did not seek to unmask all of these users, however. The government culled the Expanded Riot List according to the following criteria:

a. First, the government removed the 1,535 accounts it had unmasked as a result of the

[4] The warrant and supporting affidavit remain sealed, so the government has not attached either to this filing.

Initial Geofence Warrant and its associated unmasking Court Order, pursuant to 18 U.S.C. § 2703(d);

b. Second, the government removed all accounts known by law enforcement—either via the control lists or information voluntarily provided by the Legislative Branch or relevant law enforcement agencies—to have been legitimately on Capitol grounds during the riot.

c. Third, the government removed all accounts that registered a Location History point within the boundaries of the geofence (*i.e.* the restricted Capitol grounds) prior to 12:50 p.m. or after 6:10 p.m., as people in those groups were likely to have been legitimately on Capitol grounds during the riot.

d. Finally, out of the remaining pool of accounts, the government removed all accounts that did not register at least one Location History point where the margin for error was *fully* within the boundaries of the geofence (*i.e.* the restricted Capitol grounds).

After applying these limiting criteria, 7,806 accounts remained. The government sought—and Magistrate Judge Meriweather issued—a Court Order directing Google to unmask those 7,806 accounts. *See* 21-sc-1660, ECF No. 5.

C. Technological Questions

In addition to seeking further factual information about how the government determined which Google accounts it would seek to unmask, the Court also asked the government to answer two questions related to the underlying technology and Google's search of its own records. Specifically, the Court wanted to know (1) what type of user activity on a user's cell phone is necessary or sufficient to create a Location History ("LH") record and thus trigger a "hit" on the geofence? and (2) how could the Control List searches for the Initial Google Geofence Warrant

have generated hits for only 215 unique devices/accounts when Google applications are so ubiquitous and presumably between 1,500-2,000 people were lawfully present in the Capitol building in the time periods before and after the riot? The government addresses these questions below.

i. What Triggers a Geofence "Hit"

To begin, it is essential to understand that compared to the full universe of cell phone users, a relatively small percentage of them have Google's LH service enabled on their phones. Google's LH is an optional service that is relatively cumbersome to activate and only enabled by approximately one-third of Google users. *See* Ex. A, McGriff Decl. ¶¶ 10-13. Thus, while cell phones and Google applications are ubiquitous, LH data is much less so.

As Google employee Marlo McGriff, a project manager for the LH service/product, explained in her Declaration, filed in a recent case in the Eastern District of Virginia,[5] a Google user must take five affirmative steps to opt into LH and enable Google to collect the kind of location data that Google provided to the government in response to the Google Geofence Warrants. *See* Ex. A, McGriff Decl. ¶ 10. "LH functions and saves a record of the user's travels only when the user opts into LH as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it." *Id.*; *see also* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (ECF NO. 29), *United States v. Chatrie*,

[5] Google submitted an *amicus curiae* brief in response to the defendant's motion to suppress geofence results in *United States v. Chatrie*, 2019 WL 8227162 (E.D. Va. Mar. 3, 2022) and attached McGriff's Declaration to it.

2019 WL 8227162 (E.D. Va. Mar. 3, 2022), at 10 ("'Location History' (or 'LH') is an optional account-level Google service. It does not function automatically for Google users. But when users opt into LH on their Google accounts, it allows those users to keep track of locations they have visited while in possession of their mobile devices.").

In practice, most Google users do not enable LH. McGriff Decl. ¶ 13. According to McGriff, "[w]hile a more precise percentage is difficult to calculate in part due to fluctuating numbers of users, in 2019, roughly one-third of active Google users (i.e., numerous tens of millions of Google users) had LH enabled on their accounts." *Id.*

When LH is enabled, a Google user's "precise device location is regularly saved – to [the user's] device and Google's servers, even when Google apps aren't being used." Google Help Center, *Turn Location History on or off*, available at: https://support.google.com/maps/answer/6258979 (last accessed Nov. 24, 2023). That being said, in the government's experience examining Google LH returns, the government has found that even when Google's LH service/product is activated on a particular device and account, Google LH data is collected less frequently than, for example, cell phone cell site location information (CSLI). Google Amicus Br., *Chatrie*, 2019 WL 8227162, at 13-14 ("Mobile device users cannot opt out of the collection of CSLI or similar records, nor can they retrieve, edit, or delete CSLI data. Google LH information, by contrast, … is controlled by the user, and Google stores that information in accordance with the user's decisions (e.g., to opt in or out, or to save, edit, or delete the information), including to enhance the user's experience when using other Google products and services.").

As described below, how frequently LH is collected depends on the circumstances of a user's location, movements, and usage of his/her device. Based on the government's reviews of

Google statements and publications, relevant Google patents, and LH data gathered via warrants, it appears that LH is sometimes collected automatically, but is primarily and most frequently collected when a user is doing something with his or her device that specifically involves location information (such as following Google Maps directions or taking photographs or videos that record location as part of their metadata).

Moreover, in the government's experience examining Google LH returns, the range of activities that generate a LH point is narrower on Apple's iPhones than Android phones. Apple iPhones apparently collect LH data primarily when the user is specifically using Google Maps. In the United States, iPhone users comprise more than half of all cell phone users. *See, e.g.,* Statista Research Department, *Subscriber share held by smartphone operating systems in the United States from 2012 to 2023, Statista* (Oct. 4, 2023), available at https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/ (last visited November 20, 2023); Patrick McGee, *Apple overtakes Android to pass 50% share of US smartphones*, Financial Times (Sept. 2, 2022), available at https://www.ft.com/content/75891d95-4432-4571-83df-b4cdf82d5da5 (last visited November 20, 2023); iPhone vs Android User Stats (2023 Data), Josh Howarth, *Exploding Topics* (Oct. 13, 2023), available at https://explodingtopics.com/blog/iphone-android-users (last visited November 20, 2023). Thus the more than half of cell phone users that use iPhones generate LH data relatively infrequently, even when LH is enabled.

In contrast, Android phones can collect LH data when the user uses a wider array of Google-based applications, or even when the device is not in use at all, such as when it is sitting on a user's bedside table overnight. Additionally, if an Android phone detects that a user is moving, the Android phone specifically and automatically requests location data from the server about

every two minutes, leading to a LH data point being collected by Google. However, if the phone determines that the user is standing relatively still, or remaining within the same Wi-Fi network's range, Android phones will request location data much less frequently, as the phone is effectively not moving. Similarly, devices will not automatically request location data from the server—or will do so less frequently—when they are low on battery.

ii. Why Only 215 Devices Were Captured on the Control Lists

Due to the factors described above, it is not surprising that, in many instances, relatively little LH data is created in any fifteen-minute period when people are inside a building, not moving about much or remaining within range of the same Wi-Fi network, and not making location-based requests from their phones. For the people lawfully inside the U.S. Capitol building on January 6, the time periods used for the Control Lists (*i.e.,* the fifteen-minute periods just before and after the riot) fit that criteria.

As a rough illustrative calculation, assume 1,500 people were legitimately inside the U.S. Capitol building immediately before and after the riot. It is reasonable to assume that while nearly all of those people possessed cell phones at the time, only a subset was comprised of Google users. Of that subset, only an estimated one third would have enabled LH, leaving, at most, an estimated 500 devices/accounts potentially collecting LH data. Even among those devices/accounts, only some of those users would have been using an application that involved location information or moving around enough to change Wi-Fi networks or otherwise indicate to their devices that they were traveling, thus prompting the devices to generate LH data outside of any regular, automatic LH collection.

It is reasonable to assume that in the two fifteen-minute control periods, relatively few Congresspeople or staff members were moving around much, using Google Maps or other

applications that involve requesting location information from the server, or using other device features—such as taking photos or videos—that generate location information. Instead, they would have mostly been in their offices or on the House or Senate floors, working to certify the election, and thus the only LH collected for those users would have been LH occasionally and automatically generated in the background for users with sufficient battery life. Moreover, given Apple's market share, it is reasonable to assume that a substantial portion of those people's devices were iPhones, which generate LH data less frequently than Android phones. In that context and given those limitations, the Control List results of 215 unique devices make logical sense.

CONCLUSION

With the addition of this supplemental factual information, the United States requests that this Court deny the defendant's pending motion to suppress the results of the geofence warrants, ECF No. 45.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar Number 481052

/s/ Michael M. Gordon
MICHAEL M. GORDON
Senior Trial Counsel, Capitol Siege Section
Assistant United States Attorney, Detailee
Florida Bar No. 1026025
400 N. Tampa Street, Suite 3200
Tampa, Florida 33602-4798
michael.gordon3@usdoj.gov
(813) 274-6000

/s/ Samantha R. Miller
SAMANTHA R. MILLER
Assistant United States Attorney
New York Bar No. 5342175
United States Attorney's Office
For the District of Columbia
601 D Street, NW 20530

Samantha.Miller@usdoj.gov