

and account identifier and subscription information from the geofence warrants lacks merit. While the defense disagrees with the government's view of the merits of a potential motion to suppress, that is beside the point. At this stage, the government should not be permitted to unilaterally decide what discovery it has obtained in the course of its investigation of Mr. Easterday that is material to his defense. This is especially true when the discovery Mr. Easterday is requesting was relied on by the government in its initial investigation, in a subsequent search warrant, and in the affidavit in support of criminal complaint charging Mr. Easterday in this case.

Accordingly, for the reasons set forth more fully below, Mr. Easterday respectfully requests that the Court compel the government to produce the raw data related to three location zip files that Google produced in response to the January 13, 2021 Search Warrant. *See* Ex. 1 at 5. This discovery is necessary so that Mr. Easterday's expert can verify the accuracy of certain data provided by the government, which is material to the defense's anticipated motion to suppress based on the geofence warrants. *See generally* Ex. 2. Given that the defense requests this information prior to filing a motion to suppress, Mr. Easterday further requests that the Court continue the suppression motions deadline, currently set for July 7, 2023 (Dkt. No. 26), for two weeks after this motion is resolved. The defense will simultaneously file a motion to continue the suppression motions deadline, which government counsel has indicated it will oppose.

I. RELEVANT FACTUAL BACKGROUND

a. Geofence Warrants.

On January 13, 2021, the government applied for a search warrant to Google LLC requesting location history data and identifying information for Google accounts associated with

responsive location history data. The warrant included initial search parameters, such as a date (January 6, 2021), time period (2:00 – 6:30 PM), and the target location (geographical coordinates – i.e., the “Initial Geofence” area). The warrant further outlined a three-step process for obtaining responsive information: first, Google would initially disclose unique Google Device IDs that fell within the above-mentioned initial search parameters, as well as two separate control lists of unique Google Device IDs that fell within the same parameters except two different timeframes (second control list included Device IDs that fell within 12-12:15 PM, and third control list included Device IDs that fell within 9-9:15 PM); second, the government would review the three lists to identify information “that [was] not evidence of a crime” and to also remove any Device IDs that fell within the control lists, and then later identify to the Court through a supplemental affidavit the unique Google Device IDs for which it sought the account identifiers and basic subscriber information; and third, Google would then be required to disclose such account identifier and subscriber information to the government.

As a result of the initial search warrant, on January 13 and 15, 2021, Google produced two categories of information (a) lists of unique Google Device IDs that were within the U.S. Capitol building and (b) lists of unique Google Device IDs that were deleted but preserved by Google. For (a), Google produced the three lists of unique Google Device IDs to the government, totaling 5,518 devices.² And for (b), Google produced a list of 70 devices that had been deleted on January 6 or 7, 2021. On January 18, 2021, the government filed a supplemental affidavit requesting to “unmask” 1,498 unique Google Device IDs that fell within the U.S. Capitol and 37 unique Google Device IDs for devices that were deleted by requesting the account identifier and

² In total, 5,723 unique Google Device IDs were identified; but after comparing the initial list against the second and third control lists and removing those devices, 5,518 devices remained.

subscriber information because the 1,498 devices geolocated within the Initial Geofence area with a margin of error that also fell entirely within the geofence and the 37 devices had at least one record that geolocated in the Initial Geofence area but some part of their margin of error fell outside the geofence. In response, on January 21, 2021, Google produced a list of corresponding account identifier and subscriber information for those requested unique Google Device IDs. The government did not request Mr. Easterday's unique Google Device ID in the January 18 supplemental affidavit, and therefore his account identifier and subscriber information was not provided at that time.

Instead, the government requested Mr. Easterday's unique Google Device ID months later in the April 14, 2021 supplemental affidavit. In that affidavit, the government requested an additional 2,264 unique Google Device IDs from the 5,518 devices located within the U.S. Capitol that Google identified in response to the first step of the warrant. Specifically, the government sought a "second unmasking" of additional unique Google Device IDs because further investigation showed that additional violations occurred on the U.S. Capitol grounds "outside the [initial] geographic search parameters used in the original search warrant." Specifically, "a much larger area around the grounds of the Capitol building was restricted than just the building itself" and therefore law enforcement developed an "Expanded Geofence" that had larger geographic coordinates, i.e., the "Expanded Geofence" area:

**INITIAL GEOFENCE****EXPANDED GEOFENCE**

In support of this expanded list of devices to “unmask,” the government stated that 2,264 of the remaining 4,561 devices fell within the Initial Geofence area and the margin of error fell entirely within the Expanded Geofence area. The government stated that “[a]nyone falling within this area would have been a witness, victim, or subject to the violations” that occurred on January 6, 2021. Accordingly, pursuant to the Expanded Geofence, the government requested to “unmask” Mr. Easterday’s unique Google Device ID. And on April 28, 2021, Google provided Mr. Easterday’s account identifier and subscriber information.

b. Government’s investigation into Mr. Easterday.

The government’s investigation into Mr. Easterday started on January 26, 2021. The government interviewed two individuals, both of whom stated that Mr. Easterday was a passenger in the vehicle that they traveled in to attend a rally in support of Former President

Donald Trump in Washington, D.C. Those two individuals did not provide any further identifying information regarding Mr. Easterday or his conduct on January 6, 2021. As stated above, as a result of the April 14, 2021 supplemental affidavit with the Expanded Geofence area, the government received Mr. Easterday's unique Google Device ID, his account identifier, and his subscriber information.

Almost a year later, on March 10, 2022, the government pulled two "identification photos" from online dating back to approximately September 2020 and noted that the true identity of the individual in the photos was "[u]nknown." A few days later, on March 14, 2022, the government appears to have run an Individual Plus Associates Report for Mr. Easterday, which provided basic identifying information, such as a phone number, driver's license, property address, vehicle information, etc. Then on April 25, 2022, the government appears to have run a search on its internal database containing Google's returns in response to the geofence warrants for Mr. Easterday's phone number, which returned his location history on January 6, 2021 (including a map of his location history data points on January 6), as well as his account identifier and subscriber information.

At that point, and equipped with this information from the geofence warrants, within the next few months (from April to December 2022), the government contacted the Hart County Sheriff Deputy in Kentucky to confirm Mr. Easterday's identification, ran additional database searches to confirm his identity, and applied for a search warrant to Meta requesting Mr. Easterday's social media profiles and additional subscriber information from Google.

Importantly, both the search warrant to Meta and the statement of facts in support of the criminal complaint set forth the government's reliance on the geofence warrants in Mr.

Easterday's case to demonstrate evidence of criminal conduct on January 6, 2021. Both documents stated verbatim that on April 21, 2022, FBI Bowling Green Resident Agency was notified by the FBI Washington Field Office of Mr. Easterday "based on, among other things, information showing that a Google account associated with EASTERDAY was located inside or near the U.S. Capitol on January 6, 2021. Specifically, FBI submitted EASTERDAY's identifiers to the FBI's 'geofence' database, which . . . returned positive results for [his] Google ID number . . . and further showed that this Google ID number is associated with EASTERDAY's name and billing address that matches the address on [his] Kentucky driver's license." *See, e.g.*, Statement of Facts in Support of Criminal Complaint (Dkt. No. 1-1) at 5.

Accordingly, there is no doubt that starting from the government's initial investigation into Mr. Easterday to the filing of the charging documents in this case, the government has relied on Google's returns from the geofence warrants to both obtain location history and identify Mr. Easterday in connection with the offense conduct on January 6, 2021.

II. ARGUMENT

Federal Rule of Criminal Procedure 16 provides defendants with broad discovery rights. The rule requires the production, upon the defendant's request, of documents and objects within the government's possession, custody, or control that are "material to preparing the defense." *See* Fed. R. Crim. P. 16(a)(1)(E). "Materiality" is "not a heavy burden." *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993). Evidence is material – whether exculpatory or inculpatory – "as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assist impeachment or rebuttal." *United States v. Marshall*, 132 F.3d 63, 68 (D.C. Cir. 1998) (quoting *Lloyd*, 992 F.2d

at 351). A defendant makes an adequate showing of materiality where they “present any facts which would tend to show that the government was in possession of information that would be helpful to the defense.” *United States v. Cadet*, 727 F.2d 1453, 1466 (9th Cir. 1984)

To date, Mr. Easterday has made three requests for discovery related to the geofence warrants.³ The most recent request was on June 16, 2023, where Mr. Easterday specifically requested the raw data for three specific location history files that Google provided to the government in response to the January 13, 2021 search warrant. *See* Ex. 1 at 5. Although the government has provided a summary of this data to defense counsel, it has not provided the original files themselves, which the defense’s expert needs to “verify the integrity of the files containing the data used to create a map report [of Mr. Easterday’s location history data points] by the government.” *See* Ex. 2 at ¶ 6. The summary that the government has provided is not sufficient “because it did not come from Google in [that] format” and “the only way to verify the accuracy of the data is to view the properties of the file and match the current hash value to the hash value that Google provided in their letter,” which “cannot be done without the original file from Google.” *See id.* This is a narrow request for Mr. Easterday’s location history to be

³ Mr. Easterday first made a request on March 21, 2023 for two categories of documents related to the geofence warrants, including (a) additional Google response letters to the supplemental warrants and (b) Google’s actual returns in response to such warrants. He also requested the map display radius, which should have been included in Google’s returns. In response, the government produced documents obtained from Google related to Mr. Easterday’s location history on January 6, 2021, including a location return map and related data showing his location history that was summarized by the government and not provided directly by Google. And then on April 19, 2023, Mr. Easterday made a second discovery request for all of the raw data and original files that it received from Google in response to the geofence warrants, and specified three categories of raw data and original files needed. In response, the government provided the original files from Google’s return for Mr. Easterday’s account identifier and subscriber information; however, it did not provide the original files from Google’s return regarding location history, including Mr. Easterday’s data.

provided in the format that Google produced such data to the government. Otherwise, the defense is just relying on the government's representations about this data. In response to this request, the government has indicated that it will not produce such files because it believes that such data is not encompassed by Rule 16 and that the defense's potential motion to suppress based on the geofence warrants lacks merit. Without more, these are not proper bases under Fed. R. Crim. P. 16 to refuse to produce discovery that is material to the defense's case and is in the government's possession.

In determining what to disclose under Rule 16, "the government cannot take a narrow reading of the term 'material' . . . [n]or may it put itself in the shoes of defense counsel in attempting to predict the nature of what the defense may be or what may be material to its preparation." *United States v. Safavian*, 233 F.R.D. 12, 15 (D.D.C. 2005). Rather, "[t]he language and the spirit of the Rule are designed to provide a criminal defendant, in the interest of fairness, the widest possible opportunity to inspect and receive such materials in the possession of the government as may aid him in presenting his side of the case." *United States v. Libby*, 429 F. Supp. 2d 1, 5 (D.D.C. 2006) (internal quotation omitted); *see also* Fed. R. Crim. P. 16, advisory committee note (amend. 1974) (explaining how "broad discovery contributes to the fair and efficient administration of criminal justice" and that Rule 16 provides "the *minimum* amount of discovery to which the parties are entitled") (emphasis added). Because it is in the interest of fairness that criminal defendants have "the widest possible opportunity to inspect and receive" material in the government's possession that may aid in the defense, disputes regarding the discoverability of information under Rule 16 "should be resolved in the defendants' favor." *United States v. Karake*, 281 F. Supp. 2d 302, 306 (D.D.C. 2003).

In this case, the limited discovery that Mr. Easterday is requesting is material to preparing a motion to suppress evidence obtained from the geofence warrants. The crux of that argument is that first, Mr. Easterday has a reasonable expectation of privacy in his unique Google Device ID and second, that the geofence warrants lacked particularized probable cause to search every device that fell within the Initial Geofence area and/or fell within the margin of error radius in the Expanded Geofence area. The data that Mr. Easterday is requesting from the Court is necessary to provide to the defense's expert to support both arguments attacking the geofence warrants in this case. Specifically, the defense expert's report will utilize the requested location history data to support the arguments that Mr. Easterday's unique Google Device ID is not anonymized but instead reveals critical information about his user identification and that the Initial Geofence and Expanded Geofence areas in fact capture location history data for devices – and therefore, individuals – that were outside the location where any suspected criminal activity occurred. Accordingly, such data is critical to the defense's anticipated motion to suppress. Moreover, the defense's request for this data is further compounded by the fact that the government has relied on the geofence warrants starting from its investigation into Mr. Easterday and as probable cause to support the criminal charges against him.

III. CONCLUSION

For the reasons set forth above, and for such other reasons as this Court may determine, Mr. Easterday respectfully requests that the Court order the government to provide defense counsel with the raw data relating to three specific location zip files that Google produced in

response to the January 13, 2021 search warrant.⁴ Based on representations by the defense's expert, once the government produces this limited discovery, he will only need up to two weeks to finalize his report. Accordingly, if the government produces this discovery shortly, then the defense can be prepared to file a motion to suppress within the coming weeks and this will not impact the current trial date of September 18, 2023.⁵

Respectfully submitted,

ISREAL JAMES EASTERDAY

By counsel,

/s/ Jeremy C. Kamens

Jeremy C. Kamens

Va. Bar No. 41596

Federal Public Defender

Office of the Federal Public Defender

1650 King St, Suite 500

Alexandria, VA 22314

703-600-0848

703-600-0880 (fax)

Jeremy_Kamens@fd.org

⁴ Again, the defense just needs the zip file that contains Mr. Easterday's location history, not all three zip files. However, if the government cannot determine which file contains Mr. Easterday's data, then our expert needs to review all three files.

⁵ On March 1, 2023, the government extended a plea offer to Mr. Easterday requiring him to plead guilty to a one count of felony assault under 18 U.S.C. § 111(a)(1) in a Superseding Criminal Information (along with dismissal of the pending charges, include the charge under §111(a)(1) & (b)), with an agreed-upon advisory guidelines range that stipulated to the application of certain enhancements including one for use of a "dangerous weapon" under U.S.S.G. § 2A2.2. Based upon case law in this District and others providing that pepper spray does not necessarily constitute a "dangerous weapon" for purposes of § 111 or the guidelines depending on the facts of the case, the defense requested that the government allow the Court to determine at sentencing whether the enhancement should apply in this case. The government refused, and for this single reason the parties have not, to date, been able to resolve this case with a plea agreement. More recently, the government stated that it intends to file a superseding indictment containing an additional charge or charges based on conduct distinct from that reflected in the current indictment. Accordingly, the filing of the superseding indictment may impact the currently-scheduled trial date.

Brittany Davidson
Va. Bar No. 90660
Assistant Federal Public Defender
Office of the Federal Public Defender
1650 King St, Suite 500
Alexandria, VA 22314
703-600-0817
703-600-0880 (fax)
Brittany_Davidson@fd.org