UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **ISREAL EASTERDAY,** **Defendant.**	**Criminal Action No. 22-404 (JEB)**

MEMORANDUM OPINION

Defendant Isreal Easterday was a member of the crowd that stormed the U.S. Capitol on January 6, 2021. On October 26, 2023, a jury found him guilty of nine counts arising from his conduct on that day. Before trial, Defendant filed a Motion to Suppress identification evidence obtained from a geofence warrant, which the Court declined to rule on until it had received certain factual clarifications from the Government. Having now obtained this information, the Court concludes that the warrant process complied with the Fourth Amendment, and it will thus deny the Motion.

I. Background

Before turning to the specifics of the geofence warrant sought in this case, a quick word about that species of warrant. A geofence warrant is used to obtain location data generated by cellphones and other electronic devices, data that is collected and stored by third-party entities such as Google and Meta. One example is the Google location-history data at issue here, which is generated when a Google account user enables the "Location Reporting" feature on her device. See ECF No. 81 (Gov't Supp.) at 7. Once this feature is enabled, the user's device will begin to

collect location-history data more or less automatically, though such data is most likely to be collected when the user does something that involves "location information." Id. at 9. Examples of this include using Google Maps for directions or taking photographs and videos that capture location as metadata. Id.

Geofence warrants differ from "warrant[s] authorizing surveillance of a known suspect," since they are normally employed when the identity of a suspect is unknown. United States v. Rhine, 652 F. Supp. 3d 38, 86 (D.D.C. 2023) (emphasis added). Such warrant applications "identify the physical area and time range in which there is probable cause to believe that criminal activity occurred." Id. at 67. Upon disclosure, those devices that turn up within such parameters can then be traced back to their owners. Given that this data can reveal a smartphone owner's location with a high degree of precision, law-enforcement agencies have increasingly turned to this investigative tool in recent years. See ECF No. 45 (Motion to Suppress), Exh. 1 (Google Amicus Brief) at 3 ("Year over year, Google has observed over a 1,500% increase in the number of geofence requests it received . . . .").

As part of its January 6 investigation, the United States applied for a geofence warrant soon after the insurrection, requesting that Google produce certain "(1) location history data and (2) identifying information for Google accounts associated with such responsive data." Mot. at 7. The geographical parameters covered the Capitol building itself, but none of the surrounding grounds. See Mot. at 8–9 (depicting initial geofence); Gov't Supp. at 2. The application also set out three time windows for which the Government sought this data: 12:00 p.m.–12:15 p.m. ("Pre-Riot Control List"), 2:00 p.m.–6:30 p.m. ("Initial Riot List"), and 9:00 p.m.–9:15 p.m. ("Post-Riot Control List). See Gov't Supp. at 2. The temporal parameters of these lists more or less tracked the timeline of the January 6 events. See, e.g., Department of Defense, Planning and

Execution Timeline for the National Guard's Involvement in the January 6, 2021 Violent Attack at the U.S. Capitol (Jan. 8, 2021), https://perma.cc/PQ4F-DNHH (noting that D.C. National Guard received initial request for assistance at 1:49 p.m. and that Capitol Building was declared secure at 8:00 p.m.). These lists, in other words, identified the devices that were there only during the riot (most likely unlawfully) as well as those that were there before or after the riot (most likely lawfully).

Besides setting out these parameters, the warrant application also outlined a multi-step process that the Government would employ to handle the anonymized data and obtain deanonymized information later on. To begin, Google was to disclose the location-history data of the devices — represented as anonymized device IDs — that fell within the relevant area and the time period of the riot. See Mot. at 7. Also at this step, Google would provide the United States with two control lists corresponding to the non-riot time windows described above. Id. The Government would then review all of the data provided both to identify any accounts whose location history was not likely to be "evidence of a crime" — say, because the data placed their device "in an inaccessible place" — and to cross-reference the Initial Riot List with the two control lists. See Gov't Supp. at 3 n.3. Any information that was removed from that Riot List at this point would be "sealed and excluded from further review." Id. at 2. At the next and last step, and once it completed this culling process, the Government would return to the Magistrate Judge to obtain an order requiring Google to de-anonymize or unmask the remaining accounts. See Mot. at 7.

The search-warrant application was approved by Magistrate Judge Michael Harvey, and Google consequently disclosed the anonymized location history requested. See Gov't Supp. at 2–3. After aggregating the initial lists provided by Google, the Government determined that

5,723 accounts fell within the Initial Riot List time period, with 176 also falling within the Pre-Riot time period, and 159 also falling within the Post-Riot time period. Id. At this point, the Government took three additional steps to zero in on the accounts it wanted to unmask or deanonymize. First, it compared the Riot List with the two control lists furnished by Google and removed 215 accounts — presumably the nonoverlapping total of the 176 and 159 accounts just described — leaving a total of 5,508. Id. at 4. Second, it removed all accounts that "did not have at least one location data point where the margin-of-error radius was contained" entirely within the geofence, which brought the total down from 5,508 to 1,498. Id. Finally, it added back 37 accounts excluded at step two because these had at least one location-history hit that fell within the geofence and there was evidence that these account users had deleted their Location History data after January 6. Id. All in all, the Government sought to unmask 1,535 accounts it obtained from this geofence warrant, a request that was granted by Magistrate Judge Harvey on January 18, 2021. Id. Easterday, however, was not part of this initial batch of device holders.

Instead, Defendant's identifying information was disclosed as part of the Government's subsequent request to unmask an additional 2,264 user accounts that were part of the original 5,508 but different from the 1,535 accounts for which it had received identifying information. See Mot. at 10. To justify this request, the Government presented Magistrate Judge Harvey with an expanded geofence that covered both the Capitol and its surrounding grounds, which were also closed to the public on January 6. Id. at 9–10 (depicting expanded geofence). It further represented that the location-history data of these devices "fell within the Initial Geofence Area [*i.e.*, the Capitol building] and the margin of error fell entirely within the Expanded Geofence area." Id. at 10. This request was approved as well; once Google responded to this request on April 28, 2021, the Government received Easterday's "account identifier and subscriber

information." Id. As it itself has admitted, this information was "the start of the government's investigation of the defendant," though it was certainly not the end. See ECF No. 38 (Gov't Response to Motion to Compel) at 3; see id. at 3–4 (describing subsequent steps in investigation, including gathering video footage of Defendant's conduct).

This long and winding road finally brings us to the Motion at hand. On the eve of trial, which ultimately resulted in his conviction on nine counts, Defendant moved to suppress "all information obtained by the government as a result of" this warrant. See Mot. at 4. The Court now turns to explaining why it will deny this Motion.

II. Legal Framework

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Except in a few narrow circumstances, law-enforcement officers must obtain a warrant that complies with that provision before effecting a search. See Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) ("[O]fficial intrusion into [an individual's] private sphere generally . . . requires a warrant supported by probable cause."). To so comply, a warrant must be issued by a "neutral, disinterested magistrate[]," Dalia v. United States, 441 U.S. 238, 255 (1979), and the supporting affidavit must establish probable cause and "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

"Probable cause is more than bare suspicion but is less than beyond a reasonable doubt and, indeed, is less than a preponderance of the evidence." United States v. Burnett, 827 F.3d 1108, 1114 (D.C. Cir. 2016). The closely related particularity requirement ensures that a warrant is "no broader than the probable cause on which it is based." Rhine, 652 F. Supp. 3d at 72 (quoting United States v. Hurwitz, 459 F.3d 463, 473 (4th Cir. 2006)). While general searches

are plainly beyond the constitutional pale, a "broader sweep" may satisfy the particularity requirement "when a reasonable investigation cannot produce a more particular description." Griffith, 867 F.3d at 1276.

III. Analysis

In this case, Magistrate Judge Harvey found that this warrant was supported by probable cause. This Court's duty is thus "to ensure that the magistrate had a substantial basis for concluding that probable cause existed." Illinois v. Gates, 462 U.S. 213, 214 (1983). To that end, it will examine anew the warrant application submitted by the Government.

At the outset, the Government puts forth a number of reasons why Easterday has no reasonable expectation of privacy in his location-history data and thus lacks Fourth Amendment "standing" to attack the geofence warrant. See ECF No. 51 (Gov't Opp. to Motion) at 15–30. This point is certainly important and forcefully argued by both sides, but the Court need not resolve it. See Rhine, 652 F. Supp. 3d at 81 ("Because the Court denies Defendant's motion on other grounds, it . . . declin[es] to reach the issue of Fourth Amendment standing."); United States v. Sheffield, 832 F.3d 296, 304–05 (D.C. Cir. 2016) (explaining that Fourth Amendment standing "has nothing to do with jurisdiction"). Instead, it will start with the validity of the warrant — whether it was adequately supported by probable and particularized cause — before moving on to the good-faith exception to the exclusionary rule.

A. Probable Cause

As Judge Rudolph Contreras of this district observed in analyzing a nearly identical challenge to this same geofence warrant in a separate case, "January 6 was a unique event in a geographically unusual place such that the scope of probable cause was uncommonly" broad. Rhine, 652 F. Supp. 3d at 85. The Capitol building itself and most of the surrounding grounds

were restricted, so the very fact of entering or remaining in these areas was evidence of a crime. See 18 U.S.C. § 1752(a)(1). "Based on an unusual abundance of surveillance footage, news footage, and photographs and videos taken by the suspects themselves," there was also more than enough factual support for the idea that many individuals within both the initial and expanded geofences were carrying and using smartphones. Rhine, 652 F. Supp. 3d at 85. That the number of suspects connected to January 6 is "extremely large," moreover, is a fact that every court in this district can attest to. Id. As a result, there was "much more than a 'fair probability'" that some devices within the geofences generated location-history data and that this data "would provide evidence of a crime." Id.

In short, this warrant was supported by probable cause because there was at the very least a fair probability that: the members of this sizable group of suspects (Easterday included) were committing a crime; many were using devices (Easterday included, as it turns out) that generated the data sought by the Government; and this data (Easterday's included) would provide evidence of the crimes allegedly committed.

Undaunted by the mountain of factual support undergirding this warrant, Easterday insists that probable cause was lacking because it was based "solely" on these devices' "proximity to a crime scene and the fact that most individuals carry cellphones." Mot. at 28. This argument rests on a pair of misunderstandings. First, these devices were not just near a crime scene, as Defendant suggests, but were within the scene. That distinction matters because merely being in the identified area — the Capitol building and restricted grounds — was itself evidence of a crime on January 6, 2021, unless the person was authorized to be there, as indicated by the control lists. This case is thus distinct from cases like Ybarra v. Illinois, 444 U.S. 85 (1979), where police officers had probable cause to believe that only one of the many

individuals in a tavern had committed a crime. See id. at 90–91. Ybarra and all the other cases Easterday cites would be analogous to this one only if being in the tavern, without more, was a crime. In such a scenario, there is little doubt that law-enforcement officers would have probable cause as to each individual found there. Cf. Tinius v. Choi, 77 F.4th 691, 705–06 (D.C. Cir. 2023) (holding that police had probable cause to arrest individual standing in public at 11:00 p.m. because, under curfew order, "no person was allowed to stand in any public place within the District after 7:00 P.M.") (cleaned up). So they would here.

Easterday equally errs in contending that the Government's affidavit asserted that there was probable cause simply because "everyone now carries a cell phone." Mot. at 30 (quoting Griffith, 867 F.3d at 1275). On the contrary, the affidavit explained that there was probable cause not because people in general carry cellphones, but because many of these suspects were "seen on the news footage in the area of [the U.S. Capitol] . . . using a cell phone in some capacity." Mot. at 29 (quoting affidavit). As mentioned above, moreover, the volume of videos and photographs documenting the events of January 6 gave rise to a "fair probability" that the suspects captured by the numerous photos and videos of January 6 used smartphones. See Rhine, 652 F. Supp. 3d at 85. The Magistrate Judge therefore made the common-sense inference that the location-history data generated by these individuals "would provide evidence of a crime." Id.; United States v. Davis, 617 F.2d 677, 692 (D.C. Cir. 1979) ("Magistrates need not confine their evaluations within rigorous legalistic boundaries but instead may use their common sense."). Put differently, the Government's affidavit established a "nexus . . . between the item to be seized and the criminal behavior," and that is all that the Fourth Amendment demands. Griffith, 867 F.3d at 1271 (quoting Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 307

(1967) (internal quotation marks omitted)). This warrant, accordingly, was adequately supported by probable cause.

B. Particularity

Defendant further attacks the warrant on the separate ground that it flunks the particularity requirement. See Mot. at 9–10, 28–32.

1. Time

The geofence warrant here authorized the United States to obtain five hours' worth of location-history data. See supra Section I. Easterday gestures at but does not really raise an argument against this time period, either in his initial Motion or his subsequent Reply. See Mot. at 31 (mentioning "five-hour time frame" in passing); ECF No. 61 (Defendant Reply) at 15 (arguing only that short-term searches are covered by Fourth Amendment, which Court assumes is true). The Court therefore "has no occasion to second-guess the magistrate judge's determination that this period was at most co-extensive with the scope of probable cause." Rhine, 652 F. Supp. 3d at 88. To make assurance doubly sure, however, it reiterates that the time period targeted by the warrant tracked the January 6 timeline referenced earlier, so these parameters were "confined to the breadth of the probable cause that" supported them. United States v. Thorne, 548 F. Supp. 3d 70, 94 (D.D.C. 2021).

2. Location

The geographic parameters also pass constitutional muster. These were undoubtedly "drawn to capture location data from locations at or closely associated with the [crime]." In re Search of Information that is Stored at Premises Controlled by Google LLC (Google LLC), 579 F. Supp. 3d 62, 82 (D.D.C. 2021) (internal quotation marks and citation omitted). The initial geofence covered the Capitol building itself, while the expanded geofence almost exactly

covered the parts of the Capitol grounds that were restricted during January 6. See Mot. at 9–10 (depicting both geofences). And — not to beat a horse headed for the glue factory — since these areas were restricted to the public on that day, an individual's mere presence there was itself a crime or evidence thereof. So even after accounting for the 32% margin of error to which Easterday repeatedly points and which the Court will return to shortly, see Mot. at 5–6, 25 n.12, 32, there was a fair probability that the location-history data generated within these locations would accurately uncover evidence of a crime — *e.g.*, entering or remaining in a restricted area, in violation of 18 U.S.C. § 1752(a)(1).

3. Evidence to Be Seized

Defendant directs most of his arguments to the particularity of the evidence to be seized, though he does not argue that the category of evidence as described in the warrant is written in overly broad terms. What he seems to contend is that the warrant did not particularly describe the location-history data to be seized because it did not draw a connection between the data and the alleged crimes committed nor between the data and Easterday specifically. See Mot. at 28–32; Reply at 16–21. The former contention has no merit, as the location-history data of those devices within the restricted areas is clearly evidence of one of the crimes for which there is probable cause here — *i.e.*, 18 U.S.C. § 1752(a)(1).

The latter position is equally infirm. As the Government correctly points out, "Search warrants are not directed at persons; they authorize the search of places and the seizure of things." Gov't Resp. at 10 (quoting Zurcher v. Stanford Daily, 436 U.S. 547, 555 (1978)). More to the point, "a suspect's identity is not a prerequisite to a search warrant, which itself can be lawfully used to determine who a suspect is or develop a group of potential suspects." Google LLC, 579 F. Supp. 3d at 85 n.19; see also Zurcher, 436 U.S. at 555 (approving search warrant to

seize photographs taken by unidentified suspects even though owner of premises to be searched was "not then a suspect"). In other words, the Fourth Amendment does not demand that a search warrant name the owner of the items to be seized or the premises to be searched. All that it requires is: first, that the warrant particularly describe the "things to be seized"; and second, that the Government provide sufficient facts to support probable cause to believe that such items are evidence of a crime and will be found in the place to be searched. See U.S. Const. amend. IV. In addition to meeting the first of these requirements, which Defendant does not challenge, it also satisfied the second by drawing a connection between the data to be seized, the crimes allegedly committed, and the individuals whose devices came within the geofence's parameters, a group of suspects to which Easterday belonged. That the warrant did not single out Easterday is thus beside the point. Cf. United States v. Williams, 616 F.3d 760, 765 (8th Cir. 2010) (noting, in context of arrest warrants, that "[p]robable cause does not require certainty regarding [a suspect's] identity"). Sufficient particularization? Check. Probable cause? Check.

C. Overbreadth

Next up is an argument that can best be described as an overbreadth objection to the warrant. A warrant is unconstitutionally overbroad to the extent that it is not "limited by the probable cause on which [it] is based." United States v. Ginyard, 628 F. Supp. 3d 31, 48 (D.D.C. 2022). Defendant argues that the geofence warrant obtained by the United States was too broad because it "certainly gathered data from people who were neither suspects nor witnesses because they were not on the Capitol grounds." Reply at 19; Mot. at 32–33. We know this, Defendant continues, because the location-history data sought here generally has a 32% margin of error and because some of Easterday's own location-history hits fell outside the parameters of the initial geofence. See Mot. at 32–33.

The Court is unconvinced. Easterday might be right that "none of his 16 location history coordinates fell entirely within the initial geofence," id. at 32 (emphasis added), but he does not seem to dispute that the margin of error for his location-history hits — or anyone else's — fell entirely within the expanded geofence, which itself was almost 1:1 with the grounds that were restricted on January 6. Easterday, in fact, points the Court to four of his location coordinates, three of which appear to place him inside or right next to the Capitol building itself. See Mot. at 33. Add in the fact that this warrant is, as the Court just concluded, sufficiently particularized as to time and location, and it becomes evident that the risk of false positives was close to non-existent. The geofence warrant here thus survives this challenge, too.

D. Good-Faith Exception

Even if Magistrate Judge Harvey had erred, the Government is protected by the good-faith exception to the exclusionary rule. This exception precludes the suppression of evidence so long as it was obtained "in objectively reasonable reliance on a subsequently invalidated search warrant." United States v. Leon, 468 U.S. 897, 922 (1984). The exception does not apply, however, in at least two circumstances: (1) when the warrant was based on a "bare bones" affidavit, see Griffith, 867 F.3d at 1278, and (2) when the affidavit contains information that "the affiant knew was false or would have known was false except for his reckless disregard of the truth." Leon, 468 U.S. at 923. The Court in Rhine held that the good-faith exception applied to the same geofence warrant there, see 2023 WL 372044, at *89–90, and the Government urges the same result here. See Opp. at 30. Defendant, for his part, contends that the affidavit supporting this warrant could not have given rise to reasonable reliance and that the Government is not entitled to the good-faith exception because it misled the Magistrate Judge. See Mot. at 36; Reply at 22.

Following Rhine, this Court concludes that the Government has the better of the argument. For starters, Defendant's initial objection that the affidavit here is bare bones is simply a rehashing of the Fourth Amendment contentions the Court just rejected. No matter, because even if the warrant ultimately fell short of probable cause, the affidavit itself was not so "lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." Leon, 468 U.S. at 923 (citation omitted). Prior to submitting this warrant application, law-enforcement agents "consulted with federal prosecutors, who approved the affidavits' and warrants' sufficiency and constitutionality." Opp. at 31; cf. Messerschmidt v. Millender, 565 U.S. 535, 555 (2012) (explaining that approval of warrant affidavit by prosecutors "is certainly pertinent in assessing whether" warrant was supported by probable cause). The Government then submitted a 32-page affidavit in support of its request, which was granted by a "detached and neutral magistrate." Leon, 468 U.S. at 907; Opp. at 33. Indeed, this exact warrant was also found constitutionally valid under the Fourth Amendment by Judge Contreras in Rhine. See 2023 WL 372044, at *33. As a result, the affidavit here was not so obviously deficient that a "reasonably well-trained officer would know that the warrant was illegal despite the magistrate's authorization." Leon, 468 U.S. at 922 n.23.

Easterday's second argument, which he did not debut until his Reply, fares no better. He posits that the Government misled Magistrate Judge Harvey when it told him that the data it was to receive from Google would be anonymized. See Reply at 22–23. As a result, the inclusion of this "false" information, whether done "knowingly or recklessly," means that the Government is not entitled to the good-faith exception. Id. This is a very serious accusation. Yet it, too, ultimately rests on a misunderstanding of what occurred here. The location-history data and device information that Google gave the Government was anonymized, in the sense that the

device IDs representing individual accounts did not reveal the identifying information of users like Easterday. The Government represented nothing more to Magistrate Judge Harvey. See Opp. at 4. Although each anonymous device ID was "unique" and "consistent across" the various account lists Google produced, the IDs were still anonymous because they could not be tied to any one individual absent Herculean efforts by law-enforcement officials. See Rhine, 2023 WL 372044, at *69; see also id. at *28 n.22 (noting that it would have been nearly impossible, considering warrant parameters and number of suspects, for Government to deanonymize account "indirectly by cross-referencing more revealing location points"). Were the Government's task simple, as Easterday insists, it would have had no need to return to Magistrate Judge Harvey to seek unmasking of the accounts suspected of having a connection to January 6.

Defendant retorts that the data was still not anonymous because the Government could have "simply sen[t] a Stored Communication[s] Act request to Google" to obtain each user's unique account information. See Reply at 23. That may well be true in general, but the Government here bound itself to a multi-step process that required it to go back to the Magistrate Judge to obtain such an order to prevent the exact scenario Defendant now raises. See supra Section I. This procedure, in other words, did the opposite of what Easterday believes it did: it limited the Government's ability to uncover identifying information because it placed "the ultimate decision as to which subscribers, if any, Google [would] be compelled to identify" in the hands of a neutral magistrate judge. See Google LLC, 579 F. Supp. 3d at 88. Regardless, in the same way that "[l]awful investigative tactics do not suddenly become unconstitutional simply because they put the government in a position" to serve a subpoena, the location-history data does not become deanonymized simply because the Government could seek to deanonymize it

by serving a Stored Communications Act request on Google. See Rhine, 2023 WL 372044, at *28 n.22. This accusation of wrongdoing thus has no basis and does not change the Court's conclusion that the good-faith exception precludes suppression in this case.

IV. Conclusion

The Court, accordingly, will deny Defendant's Motion. A separate Order so stating will issue this day.

/s/ *James E. Boasberg*
JAMES E. BOASBERG
Chief Judge

Date: January 18, 2024