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' OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS GOOGLE GEOFENCE DATA

The United States respectfully opposes 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"[1]).

This is not a close case. As Judge Contreras noted in rejecting a similar attempt to suppress evidence derived from the same Google Geofence Warrants in another January 6 case, *see United States v. Rhine*, 2023 U.S. Dist. LEXIS 12308 (D.D.C. Jan. 24, 2023), no court in the country has ever suppressed the results of a Google geofence search warrant authorized by a federal judge. *See id.* at *65-66 (summarizing cases). This Court should not rule otherwise.

First, this Court can—and should—deny the defendant's motion for a simple reason: any "search" in this case was supported by valid, judicially authorized warrants. Contrary to the defendant's conjectures, the Google Geofence Warrants were not overbroad and did not seize data

[1] A "geofence warrant" is "a warrant to obtain cellular phone data generated in a designated geographic area." *In re Information Stored by Google*, No. 21-sc-3217, 2021 WL 6196136, at *2 (D.D.C. Dec. 30, 2021) (citation omitted). The "geofence" in a "geofence warrant" is "the boundary of the area where the criminal activity occurred and is drawn by the government using geolocation coordinates on a map attached to the warrant." *Id.*

for people who were merely "near a crime scene," as the defendant repeatedly (but erroneously) claims. Def.'s Mot. at 3; *see also, e.g.*, *id.* at 16-17, 31-32. In arguing otherwise, the defendant ignores that *no member of the general public* was allowed to be inside the restricted perimeter on the afternoon of January 6, 2021, and thus there was probable cause to believe that *every device* found to be within the restricted perimeter during the riot, other than those possessed by people on the control lists, was carried by a person who (1) likely violated, at minimum, 18 U.S.C. § 1752(a)(1) (Entering or Remaining in a Restricted Building or Grounds); and (2) in addition, likely witnessed offenses committed by others within the restricted perimeter on that day. Moreover, the Google Geofence Warrants were appropriately particularized to date, time, place, and suspected crimes, and thus complied with the Fourth Amendment's requirements.

Second, the government went beyond its constitutional obligations here. Even though the government used search warrants to obtain the contested data from Google out of an abundance of caution, no warrants were required under the Fourth Amendment in the first place. The defendant lacked a protected Fourth Amendment interest in the short-term location information provided by Google for three independent reasons: (1) the defendant had no reasonable subjective or objective expectation of privacy in his location on restricted U.S. Capitol grounds or inside the restricted Capitol building during the riot on January 6, 2021, particularly when he willingly exposed his presence to others and surveillance cameras; (2) more generally, under the third-party doctrine, *see e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966), the defendant had no reasonable expectation of privacy in the "Location History" data[2] that he voluntarily opted to provide to

[2] "Location History" is a term of art for Google. It does not mean all location data held by Google for a given subscriber account. Instead, it refers to a specific subset of location data gathered by Google that records where a user's cellular device was located when it communicated with, or transmitted information to, Google. Users must opt-in for Google to gather and save Location History data, which users may access—and even delete—through their Google accounts. Google's gathering of Location History data is designed to enhance its users' experience of Google

Google in exchange for its services and which covered only one location and, at most, 9.5 hours; and (3) the defendant lacks standing to assert *other people's* Fourth Amendment rights, which forecloses any attempt by the defendant to prove that the Google Geofence Warrants were unconstitutionally overbroad because they swept up data for devices carried by people who did not trespass on restricted Capitol grounds or otherwise participate in the January 6 riot.

Third, even if the Court finds that the defendant had a reasonable expectation of privacy in the data received by the government from Google here, *and* that a Fourth Amendment search occurred, *and* that the Google Geofence Warrants were either overbroad or lacking particularity, the Court *still* should not grant the defendant's motion and suppress the evidence. Two different federal magistrate judges authorized the Google Geofence Warrants and agents relied on those warrants in good faith. Binding Supreme Court precedent thus bars the Court from excluding the evidence. *United States v. Leon*, 468 U.S. 897 (1984); *Davis v. United States*, 564 U.S. 229, 236-37 (2011); *Herring v. United States*, 555 U.S. 135, 144 (2009); *see also United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) (suppression inappropriate in cases involving novel technologies when investigators consult with prosecutors and then obtain a warrant); *United States v. Chatrie*, 590 F. Supp. 3d 901, n.4 (E.D. Va. 2022) (holding that under *Leon* and *McLamb* the Court could not suppress location history evidence generated by a Google geofence search warrant, even though the Court found the warrant unconstitutional).

For all of the above reasons, the Court should deny the defendant's motion.

I. FACTUAL BACKGROUND

The facts of this case—at least with respect to the facts underlying the defendant's

applications and products, such as by helping them find nearby gas stations and/or restaurants or serve them targeted advertisements. *See* Def.'s Mot., Ex. 1 (Google *amicus curiae* brief filed in *Chatrie*).

suppression motion—are undisputed and detailed in previous filings by the government and defense. *See, e.g.*, ECF No. 38; *see also* ECF No. 29; Def.'s Mot; *Rhine*, 2023 U.S. Dist. LEXIS 12308. The government will thus not repeat those well-established facts here and incorporates those prior filings by reference. In short, as part of its investigation into the January 6, 2021 riot on the United States Capitol grounds, the government used two "geofence" warrants to obtain location data from Google concerning cellular devices captured as being within the restricted perimeter during the riot—indicating their users were, at minimum, likely unlawfully present on restricted Capitol grounds, in violation of 18 U.S.C. § 1752(a)(1). *See Rhine*, 2023 U.S. Dist. LEXIS 12308 at *51-59 (explaining the technology involved and summarizing the government's use of the Google Geofence Warrants to investigate the January 6 riot); *see also In re Search of Information That is Stored at the Premises Controlled by Google LLC*, No. 21-SC-3217, 2021 WL 6196136, at *1-4 (D.D.C. Dec. 30, 2021) (hereinafter "*Unrelated D.D.C. Google Geofence Warrant*") (explaining the technology involved). Ultimately, Google provided the government with anonymized Location History data for 12,370 devices in response to those warrants, *see id.* at *55-59, and the government "unmasked" subscriber data for the account holders of 7,806 of those devices, *see* ECF No. 38. The defendant's Location History data was within that unmasked set, and now the defendant seeks to suppress not just his data, but "all information obtained by the government" from the Google Geofence Warrants. Def.'s Mot. at 3-4.

Like so-called cellular "tower dump" warrants, *see Carpenter v. United States*, 138 S.Ct. 2206 (2018), the investigative theory behind Google geofence warrants is that agents investigating a crime (or a series of apparently related crimes) may be able to identify suspects, victims, and/or witnesses by looking to see what e-mail accounts—or, in the case of tower dump warrants, what cellular phone numbers—registered in the area(s) of the crime(s) at the time(s) it/they occurred.

Both tower dump and geofence warrants are useful—and constitutional—investigative tools when the government knows where and when the crime occurred, but not who committed it. Like tower dump warrants, geofence warrants are particularized by time, date, location, and crime under investigation. Contrary to the defendant's assertions, however, this does not render geofence warrants—or tower dump warrants—unconstitutional "general warrants" or "digital dragnets." *See generally* Def.'s Mot. The Fourth Amendment does not require search warrants to target a *specific individual* in order to be sufficiently particularized. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978) ("Search warrants are not directed at persons; they authorize the search of places and the seizure of things.").

II. DISCUSSION

A. The Defendant's Overbreadth and Particularity Claims Fail Because the Google Geofence Warrants Satisfied All Fourth Amendment Requirements.

Even assuming, *arguendo*, that the defendant had a cognizable Fourth Amendment interest in his Google Location History data (*but see infra*), his motion to suppress fails for a simple reason: the government obtained the defendant's Location History data pursuant to valid warrants, which satisfied all Fourth Amendment requirements. This Court thus can—and should—deny the defendant's motion to suppress on that basis, without considering the defendant's other contentions. *See Rhine*, 2023 U.S. Dist. LEXIS 12308 at *90-108 (finding the Initial Google Geofence Warrant to be valid and denying motion to suppress).

The defendant repeatedly characterizes the Google Geofence Warrants as unconstitutional "general warrant[s]." *See, e.g.*, Def.'s Mot. at 32-35. But that characterization is historically and legally baseless. Historically, a general warrant "specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220

(1981). Such warrants are unconstitutional because an application for a search warrant must "particularly describ[e]" the scope and object of the proposed search and seizure. U.S. Const. amend. IV. The Google Geofence Warrants bore no resemblance to such general warrants. They directed Google to search its records for specific, limited information directly tied to one incident that occurred at a particular place, on a particular date, during a particular time range. "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justifications." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

i. The Google Geofence Warrants Were Not Overbroad.

Although he implicitly concedes that the Google Geofence Warrants established probable cause to believe that many people committed crimes on the U.S. Capitol grounds during the riot on the afternoon of January 6, 2021, the defendant argues that the Google Geofence Warrants were nevertheless overbroad because they *may* have captured false positives, *i.e.* "both those suspected of being involved in criminal conduct and those who were merely present within or in the vicinity of the geofence parameters." Def.'s Mot. at 25. The defendant's argument relies on a false dichotomy. The criminal conduct that occurred at the Capitol on January 6, 2021 was not limited to assaults against police officers and destruction of government property. Because the boundaries of the Expanded Google Geofence Warrant were the same as the restricted perimeter on January 6, people "who were merely present within . . . the geofence parameters" and "those suspected of being involved in criminal conduct," *id.*, are the same. There was probable cause to believe that all such people were unlawfully on restricted Capitol grounds in violation of 18 U.S.C. § 1752(a)(1) (Entering or Remaining in a Restricted Building or Ground), one of the crimes identified by both Google Geofence Warrants but which the defendant ignores throughout his

argument. *See generally* Def.'s Mot. (repeatedly falsely distinguishing between those who engaged in "criminal conduct" and those who were merely on the restricted Capitol grounds without authorization). The Google Geofence Warrants were not unconstitutionally overbroad for seeking Location History for every device that registered within the restricted perimeter because there was, indeed, probable cause to believe the users of all such devices were either perpetrators or witnesses. This geofence warrant is not about a needle in a haystack (which has been repeatedly upheld in any event); it is about a stack *of needles*. *See Rhine*, 2023 U.S. Dist. LEXIS 12308 at *96 (recognizing the "unusually broad scope of probable cause" underlying the Google Geofence Warrants).[3]

The sufficiently targeted nature of the Google Geofence Warrants is underscored by comparing the Google Geofence Warrants at issue in this January 6 case to the Google geofence warrant found to be overbroad by the district court in *Chatrie,* 590 F. Supp. 3d 901, which concerned a bank robbery. The *Chatrie* court held that the Google geofence warrant used in that case, which covered a 300-meter area surrounding the victimized bank, violated the Fourth Amendment. *Id.* at 918. Although the *Chatrie* investigators sought Google location data to "identify potential witnesses and/or suspects," the court found that "the Geofence Warrant [was] completely devoid of any suggestion that all – or even a substantial number of – the individuals searched had participated in or witnessed the crime." *Id.* at 929. Rather, in the court's view, the warrant captured device location data for users "who may not have been remotely close enough to the Bank to participate in or witness the robbery," such as patrons at a nearby restaurant, occupants

[3] *See also Rhine*, 2023 U.S. Dist. LEXIS 12308 at *96 ("Based on an unusual abundance of surveillance footage, news footage, and photographs and videos taken by the suspects themselves while inside the Capitol building, there is much more than a "fair probability" that the suspects were within the geofence area and were carrying and using smartphones while there, such that their devices' [Location History] would provide evidence of a crime.")

in a nearby hotel, and residents of a nearby apartment complex and senior living center. *Id.* at 930.[4]

The situation is drastically different here. Given the scope and breadth of the mob's activities on January 6, the geographically and temporally tailored Google Geofence Warrants in this case articulated probable cause to believe that every person on the U.S. Capitol grounds, or inside the U.S. Capitol building, during the time span of the riot had either engaged in or witnessed criminal activity, including, at a minimum, trespass violations under 18 U.S.C. § 1752(a)(1).[5] The Google Geofence Warrants thus presented little risk that the search "swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." *Id.; see also Rhine*, 2023 U.S. Dist. LEXIS 12308 at *101 (noting that "the area around the Capitol is unusual for its lack of nearby commercial businesses or residences"). Moreover, the government undertook a multi-step review of the anonymized identifiers and excluded 4,564 devices from unmasking, demonstrating the government's efforts to further tailor the warrant results to those who likely committed a crime. *See id.* (holding that there was a "substantial basis for [Magistrate Judge Harvey] to have identified a fair probability that all of" the devices Google identified and the government unmasked pursuant to the Initial Geofence Warrant "were linked to suspects of witnesses").

Nor is there merit to the defendant's reliance on cases addressing physical searches of persons pursuant to warrants to search premises, including *Ybarra v. Illinois*, 444 U.S. 85, 91

[4] Even then, the *Chatrie* court declined to suppress evidence under the good-faith exception to the exclusionary rule. *Chatrie*, 590 F. Supp. 3d at 938. *See infra*.

[5] Moreover, the entire grounds were generally closed on January 6, 2021, as they had been for months, due to COVID-19 precautions. Accordingly, it is even more unlikely that the boundaries of the Google Geofence Warrants subjected a meaningful number of innocent patrons at a nearby restaurant, occupants in a nearby hotel, or residents of a nearby apartment complex and senior living center to their device data being captured and reviewed by the government. *See Chatrie*, 590 F. Supp. 3d at 930.

(1979), in which the Supreme Court held that the probable cause that supported a warrant to search a tavern and its bartender for drugs did not extend to a search of tavern patrons. *See* ECF No. 45 at 17, 30-31, 36. The defendant misunderstands *Ybarra* and its progeny, which explicitly address limitations on physical searches of persons pursuant to warrants, not the standard for searching property (such as the Google records at issue here) for evidence. As *Ybarra* stated: "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." 444 U.S. at 91 (emphasis added). The Google Geofence Warrants, in contrast, authorized obtaining evidence *from Google* about a crime scene; they did not authorize the arrest, search, or seizure of *any person*. And, in any event, given the unique circumstances of the January 6 mob and the carefully calibrated parameters of the Google Geofence Warrants, probable cause in this case was, as noted, particularized with respect to each person whose device (1) hit within the geofence but (2) was not included in the control lists.

ii. *The Google Geofence Warrants Were Sufficiently Particularized.*

The defendant's claim that the Google Geofence Warrants lacked particularity fares no better. The Fourth Amendment requires that search warrants contain "a 'particular description' of the things to be seized." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The particularity requirement protects against "exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). While the particularity requirement "ensures that the search will be carefully tailored to its justifications," that is, to the probable cause shown," *Garrison*, 480 U.S. at 84, a "broader sweep" may be permissible "when a reasonable investigation cannot produce a more particular description" prior to obtaining and executing the warrant, *Griffith*, 867 F.3d at 1276. "In assessing particularity, courts are concerned with realities of administration of criminal justice," so it suffices if the warrant "is particular enough if read with reasonable effort by the

officer executing the warrant." *United States v. Dale*, 991 F.2d 819, 846 (D.C. Cir. 1993) (internal quotations omitted). The test for particularity "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979).

Here, the defendant claims that the Google Geofence Warrants lacked particularity because "probable cause must be particularized as to the person subject to the search," Def.'s Mot. at 37, and the Google Geofence Warrants did not target any specific individual but rather every device (and by extension, device holder) within the designated boundaries. The defendant mischaracterizes the law. True, the Google Geofence Warrants resulted in the government obtaining data for 12,370 devices, but that does not render the warrants "digital dragnets," as the defendant claims. *See generally, e.g.*, *Unrelated D.D.C. Google Geofence Warrant*.

The defendant's objection to the warrants' lack of targeting specific individuals is based on a misunderstanding of the law. "Search warrants are not directed at persons; they authorize the search of places and the seizure of things." *Zurcher*, 436 U.S. at 555 (internal quotation marks and brackets omitted). To that end, "valid warrants to search property may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id.* at 559. Warrant affidavits may accordingly establish probable cause to search a location for any kind of evidence – including evidence that might identify unknown perpetrators of an offense. Indeed, the Supreme Court in *Zurcher* affirmed the constitutionality of a warrant authorizing the search of a newsroom on the ground that it might contain "evidence material and relevant to the identity of the perpetrators of felonies." *Id.* at 551; *see generally In re Search of Twenty-Six Digital Devices & Mobile Device Extractions*, No. 21-sw-233, 2022 WL 998896, at *2 (D.D.C. Mar. 14, 2022) (explaining that the government must present "probable

cause to believe that evidence relevant to specific criminal conduct is reasonably likely to be found in a particular location."). Simply put, "a suspect's identity is not a prerequisite to a search warrant." *In re Information Stored by Google*, 579 F. Supp. 3d 62, 83 n.19 (D.D.C. 2021) (magistrate judge) (cataloguing cases).

Here, the Google Geofence Warrants appropriately provided "a 'particular description' of the things to be seized." *Coolidge*, 403 U.S. at 467. Like tower dump warrants, the Google Geofence Warrants provided precise parameters for Google to search—dates, times, and geographical boundaries, rendered in GPS coordinates. First, the government sought device-location information for a "discrete geographical area." *In re: Information Stored at Premises Controlled by Verizon Wireless*, No. 21-sc-59, 2022 WL 2922193, at *7 (D.D.C. July 25, 2022); *see also id.* (observing that "[t]he warrants … focus exclusively on cell tower information collected in the limited relevant area of interest"); *accord In re Geofence Location Data*, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020) (finding a proposed geofence warrant sufficiently particular where the government had "structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses"). Specifically, the boundaries of the Expanded Geofence were particularly described with precise GPS coordinates that corresponded with a particularized, identifiable place—the boundaries of the U.S. Capitol grounds' restricted area— in which the offenses under investigation occurred. The Google Geofence Warrants limited the search to only those mobile devices that Google detected to be within those longitudinal and latitudinal coordinates.

Second, the warrants limited the search to a particular date (January 6, 2021) and a particularized time frame: the 9.5-hour time span that corresponded with the time period between when rioters began breaching the Capitol's restricted perimeter, marking the beginning of the riot,

and when the House of Representatives resumed the Joint Session, marking the end of it.

Third, by providing Google with a detailed description of the records Google was to search and produce, the Google Geofence Warrants were "also particularized and limited to the types of data, *i.e.*, phone numbers and unique device identifiers, that can be used to identify the [s]ubject[s], associates of that [s]ubject[s], and potential witnesses in furtherance of the criminal investigation" into the riot that took place at the U.S. Capitol in the afternoon of January 6. *Matter of Search of Info. Associated with Cellular Tel. Towers Providing Serv. to [Redacted] Stored at Premises Controlled by Verizon Wireless*, No. 1:21-SC-59 (BAH), 2022 WL 2922193, at *7 (D.D.C. July 25, 2022).

Fourth, the Google Geofence Warrants contained "directions as to how the government must handle the … data, including limiting the data that may be seized to the precise terms of the temporal and geographic scope set out in the warrant[]." *Id.* The Google Geofence Warrants' use of a multi-step procedure involving an initially anonymized data set, control lists used to exclude innocent subjects, and follow-up judicially authorized "unmasking" warrants supported by probable cause, allowed the government to "analyz[e] the raw data disclosed by [Google] to identify the relevant data for seizure" before obtaining user-identification information – a procedure that "mitigated" the likelihood that the searches would identify mobile devices that "'would not belong to either a suspect or witness.'" *Id.* at *8.

The warrants thus contained no ambiguity, were constrained in time and space, and granted Google no discretion. This is all that the Constitution requires for the warrants to be sufficiently particularized. This was not a "wide-ranging exploratory search[]" of Google's records. *Garrison*, 480 U.S. at 84. In sum, "[t]he government … carefully tailored the warrants to the greatest degree possible to obtain cell phone data from [Google] to assist in identifying" those involved in the U.S.

Capitol siege on January 6. *Id.* The geographic, temporal, and procedural restrictions described above "demonstrate[] that the warrants are sufficiently particularized to provide specific guidance to law enforcement as to what data may be seized." *Id.*

The information specified by a warrant must be "no broader than the probable cause on which it is based," *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006), but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Here, step two of the Google Geofence Warrants' multi-step execution process allowed government agents discretion to review the anonymized list of accounts generated in step one and designate/prioritize specific devices for which they wished to receive information unmasking the subscribers of the accounts. Following the prophylactic process designed to guard against overcollection described within the Google Geofence Warrants and approved by both Magistrate Judges Harvey and Meriweather, the government used the control lists to eliminate devices present on the restricted Capitol grounds during the time period just before or after the riot, which suggested that the users of those devices were authorized to be there and not suspected of committing a crime, even 18 U.S.C. § 1752(a)(1). This step eliminated 4,564 devices, and the government sought to have the remaining 7,806 account holders unmasked. But step two did not allow government agents unlimited discretion to "search where they please[]," *Stanford v. Texas*, 379 U.S. 476, 482-83 (1965), and review all of Google's records or obtain identifying information about every Google user. Instead, agents could only request such identifying information about accounts that registered within the restricted perimeter.

Step two makes the warrant more targeted, not less; it reduces the intrusiveness of the warrant on uninvolved/unnecessary parties. Here, in response to step one, Google provided the government with approximately 12,370 unique, anonymized devices that were present within the

restricted perimeter during the riot. While under the terms of the Google Geofence Warrants agents could have asked Google for identifying information about all 12,370 accounts on the anonymized list, they only asked for identifying information on 7,806 of them (approximately 63%).[6]

The defendant's argument suggests that he believes the warrant would have been more particularized if steps one and two were combined, *i.e.*, if the agent's review and prioritization step was eliminated and Google was directed to provide the government with full identifying information for every one of the 12,370 devices that registered within the restricted perimeter during the riot. This is nonsensical. There is no viable argument that the first step was insufficiently particularized, or that Magistrate Judges Harvey and Meriweather could not have authorized Google to provide full identifying information for every account record responsive to step one. Accordingly, the warrant cannot be made unconstitutional by the addition of step two, which imposed constraints beyond those required by the constitution and limited the data produced to the government. *See id.* The overbreadth concern and particularity requirements are designed to prevent the government from seizing more than probable cause justifies. But here, the warrant requested, Magistrate Judges Harvey and Meriweather authorized, and the government obtained less. *See id.*

---

[6] The most-heavily litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that this design did not violate the Fourth Amendment. Eleven courts of appeals have considered various challenges to the Playpen warrant, and all ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019).

Approximately 100 district court cases have resolved suppression motions challenging the Playpen warrant. *See, e.g.*, *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016). Some defendants argued that the discretion given the FBI in executing the Playpen warrant violated the Fourth Amendment's particularity requirement, but courts uniformly rejected this argument. *See, e.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016) (holding that "the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site.").

B. Even More Fundamentally, the Defendant's Motion Fails Because He Lacked a Protected Fourth Amendment Interest in the Location History Data Provided by Google.

The defendant's motion presumes that he had a protected Fourth Amendment interest in his locations while he was on the restricted Capitol grounds and within the restricted Capitol building during the riot. It also presumes that he had a protected Fourth Amendment interest in the Location History data that Google provided to the government pursuant to the warrants. But the defendant had neither, which means he lacks standing, and thus the Court could—and should—consider his motion dead on arrival before even considering the constitutional sufficiency of the Google Geofence Warrants. *See Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980) ("[Defendant], of course, bears the burden of proving . . . that he had a legitimate expectation of privacy. . . .").

The first step in any Fourth Amendment analysis is for the Court to examine the totality of the circumstances and assess whether the defendant has standing. *Rakas v. Illinois*, 439 U.S. 128, 134 (1978). "Fourth Amendment rights . . . are personal, and only individuals who actually enjoy the reasonable expectation of privacy have standing to challenge the validity of a government search." *United States v. Cooper*, 203 F.3d 1279, 1284 (11th Cir. 2000). Without a reasonable expectation of privacy in the place searched, a defendant cannot win suppression, even if the police searched unlawfully. *See Rakas*, 439 U.S. at 134. Put differently, if the defendant has "no reasonable expectation of privacy" in the area searched, "no Fourth Amendment search occurred, and *ipso facto*, there was no violation of constitutional right." *Townsend v. United States*, 236 F. Supp. 3d 280, 324 (D.D.C. 2017).

To establish a legitimate expectation of privacy, a defendant must demonstrate that his conduct exhibits "an actual (subjective) expectation of privacy," showing that "he seeks to preserve something as private." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citation and

alternation omitted). The defendant must further demonstrate that his subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *Id.* (citation omitted). "[D]efendants always bear the burden of establishing that the government violated a privacy interest that was protected by the Fourth Amendment." *United States v. Sheffield*, 832 F.3d 296, 305 (D.C. Cir. 2016).

Here, the defendant has failed to carry that burden. He has failed to show a cognizable Fourth Amendment interest for three reasons, each of which is discussed in detail below. First, the defendant had neither a subjectively nor objectively reasonable expectation of privacy in his location during the riot on January 6, 2021, particularly during the time period he was inside the Capitol building, a public, heavily secured building blanketed by surveillance cameras. Second, the third-party doctrine dictates that the defendant has no reasonable expectation of privacy in optional Location History data he voluntarily disclosed to Google in exchange for its services and over which he maintained control. Finally, the Google Geofence Warrants did not result in searches within the meaning of the Fourth Amendment because the government obtained a mere 9.5 hours' worth of Location History data over a one-day period.[7]

i. The defendant did not have a subjectively or objectively reasonable expectation of privacy in his unlawful locations within the restricted Capitol grounds and building during the riot on January 6, 2021.

The defendant cannot demonstrate that he had the requisite subjectively and objectively reasonable expectation of privacy in the information disclosed by Google corroborating that, on January 6, 2021, he was present within the restricted perimeter for at least 34 minutes and inside the U.S. Capitol building for at least 12 minutes, all during times and at locations where the riot

[7] The government raised similar lack of standing arguments in *Rhine* but Judge Contreras declined to address them because he denied the defendant's motion to suppress the Google Geofence Warrants on other grounds. *See id.* at *87-88.

was unfolding. *See* ECF No. 1-1 at 6-8.

First, as to the subjective prong, the defendant has failed to make any showing that he held a subjective expectation of privacy in his location during the afternoon of January 6, 2021. Having first walked on restricted U.S. Capitol grounds unmasked, in full view of thousands of other people, the defendant entered the U.S. Capitol building through the East Rotunda Doors on the second floor of the U.S. Capitol and then roamed the building, as the U.S. Capitol Police's network of closed-circuit surveillance cameras readily recorded his movements. ECF No. 1-1 at 6-8. Even while inside the Capitol building, the defendant remained in open view of hundreds of other people, which he observed. The defendant therefore cannot credibly claim that he intended to keep his location on Capitol grounds or within the U.S. Capitol building a secret. *See Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public … is not a subject of Fourth Amendment protection.").

Second, with respect to the objective prong, any assertion by the defendant that he expected privacy in this circumstance cannot be regarded as reasonable. The U.S. Capitol – the seat of this country's legislative branch – is secured 24 hours a day. ECF No. 1-1 at 1. "Nothing is private about entry into the Capitol." *United States v. Bledsoe*, 630 F. Supp. 3d at 14 n.2 (D.D.C. 2022) (denying motion to suppress analogous user-generated location data from Facebook in January 6 case because the defendant had no reasonable expectation of privacy under the third-party doctrine and *Carpenter*). Access to the U.S. Capitol is restricted—as it was on January 6, 2021—to authorized people with appropriate identification who must clear security barriers staffed by the U.S. Capitol Police. ECF No. 1-1 at 1. Surveillance cameras then monitor individuals after they enter the building. *Id.* at 6-8; *see also Bledsoe*, 630 F. Supp. 3d at 14 n.2 ("Not only would any lawful entrants to the restricted areas of the Capitol building be required to reveal their

identification to the government prior to entering, but the government continuously monitors the halls of the Capitol through CCTV cameras."). Additionally, as stated above, the defendant was surrounded by hundreds of other people while outside and inside the U.S. Capitol, a fact of which he was well aware. Given his lack of mask or disguise, as well as the U.S. Capitol building's function, access restrictions, security, and crowdedness, the defendant cannot credibly assert that he had an objectively reasonable expectation that he would be able to enter and roam the building anonymously on January 6, 2021.

In fact, on January 6 specifically, it was doubly true that such an expectation would not be reasonable because members of Congress and the Vice President convened in a joint session to certify the results of the 2020 presidential election, complete with special—and more restrictive—security measures. "That day, the Capitol building and its exterior plaza were closed to members of the public." *United States v. Sandlin*, 575 F. Supp. 3d 16, 20 (D.D.C. 2021). As the video evidence shows in this case, however, the defendant entered the U.S. Capitol building alongside many other rioters, none of whom had authorization or appointments, and none of whom had been through a security screen or magnetometer. *See* ECF No. 1-1 at 1, 6. If the defendant asserted an expectation that his presence beyond the restricted perimeter and inside the Capitol building was private, such an expectation of privacy would not "be one that society is prepared to accept as reasonable … considering the blatant criminal conduct occurring within the usually secured halls of the Capitol building during the constitutional ritual of confirming the results of a presidential election." *Bledsoe*, 630 F. Supp. 3d at 3.

Because the defendant lacked a legitimate expectation of privacy in his locations beyond the restricted perimeter and within the U.S. Capitol building during the riot on January 6, he cannot credibly assert that the government violated the Fourth Amendment by obtaining information that

revealed his unlawful locations during that time period.

ii. ***The Defendant has no reasonable expectation of privacy in Location History data he voluntarily disclosed to a third-party, Google, in exchange for its optional, nonessential services.***

The defendant lacked a protected Fourth Amendment interest in his Location History data for a second reason as well. The well-established third-party doctrine holds that an individual cannot reasonably expect something to be private if he/she voluntarily shared it with a third-party, *see, e.g.*, *United States v. Knotts*, 460 U.S. 276, 281 (1983) (no reasonable expectation of privacy in public movements that an individual "voluntarily conveyed to anyone who wanted to look"), and thus that individual has no Fourth Amendment standing to block the third-party from disclosing that information to the government, *see, e.g.*, *Hoffa*, 385 U.S. at 302 (holding that the Fourth Amendment does not protect an individual's "misplaced belief that a person to whom he voluntarily confides [information] will not reveal it."). *See also Bledsoe*, 630 F. Supp. 3d at 1 (holding, in January 6 case, no reasonable expectation of privacy in user-generated location information provided to Facebook in exchange for non-essential services).

i. The Third-Party Doctrine Applies

For decades, the Supreme Court has applied this principle in cases ranging from private communications to business records to reject Fourth Amendment challenges by defendants who voluntarily conveyed information—even sensitive information—to third parties. *See, e.g.*, *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party). Here, this principle independently forecloses the defendant's objection to Google providing his Location History data to the government in response to the Google Geofence Warrants.

Applying the third-party doctrine in the realm of telephone-based information, the Supreme Court has held that some information conveyed to the phone company in exchange for service is not protected by the Fourth Amendment. *Smith*, 442 U.S. at 743-45 (holding that a telephone user has no reasonable expectation of privacy in the numbers he voluntarily dialed on the phone, and thus conveyed to the phone company, to place a call). Similarly, in *United States v. Miller*, 425 U.S. 435, 443 (1976), the Supreme Court held that customers held no reasonable expectation of privacy in bank business records. The Supreme Court has explained that the customers in those cases "'voluntarily conveyed'" the information to a third-party entity "'in the ordinary course of business'" and, accordingly, "assumed the risk that the company would reveal [the information] to the police." *Id.* at 744 (quoting *Smith*, 425 U.S. at 442).

In *Carpenter*, however, the Court declined to apply *Smith* and its progeny to cell site location information (CSLI). 138 S.Ct. at 2220. Instead, *Carpenter* held that CSLI—which is data automatically exchanged between a cellular device and its service provider whenever the cellular device is powered on (and able to connect to the service provider's network) that is necessary to establish and maintain cellular service—is not voluntarily "shared" with the phone company "as one normally understands the term." *Id*. The *Carpenter* Court distinguished CSLI from the numbers dialed in *Smith* by noting that (1) "carrying [a cell phone] is indispensable to participation in modern society" and (2) CSLI is generated by "[v]irtually any activity on the [cell] phone" "without any affirmative act by the user beyond powering up." *Id.* Accordingly, "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." *Id. Carpenter* thus held that CSLI is not covered by the third-party doctrine. *Id.*

CSLI and Google Location History data are fundamentally different, however. Moreover, neither of *Carpenter*'s animating concerns are applicable here, and the same reasoning shows why a Google user has no reasonable expectation of privacy in the Location History data Google stores. First, while carrying a cell phone may be "indispensable" for modern life, *id.*, using Google and its products is not. Although Google and its products may be helpful, convenient, and reliable, other companies, like Microsoft and Apple, offer virtually the same suites of services with similar features and performance. A person can participate in modern society by using Bing for searching, AOL for e-mail, WhatsApp for texting, Meta (formerly Facebook) for social networking, Yahoo! for watching videos, X (formerly Twitter) for news, and Apple Maps for directions, none of which are Google products. The defendant was by no means compelled to use Google at all. *See Bledsoe*, 630 F. Supp. 3d at 13 (holding that Facebook was similarly unessential to modern life).

Second, even if using Google products was somehow "indispensable to participation in modern society," allowing Google to collect Location History data is not. This point is made obvious and inescapable by the fact that Google itself makes its Location History service optional for its users. Indeed, Google describes Location History collection as something Google users "can … turn on … if [they] want to create a private map of where you go with your signed-in devices." Google Privacy Policy (Sept. 30, 2020).[8] Indeed, unlike *Carpenter*'s concern about the mechanisms by which CSLI is generated, Google users must act affirmatively and complete a multi-step process to authorize Google to collect their Location History data, a fact detailed in the affidavits and *amicus curiae* brief Google filed in *Chatrie*, on which the defendant relies, *see* Def.'s Mot. 4-5, 23, Ex. 1, Ex. 2, but which he omits from his motion.

[8] https://policies.google.com/privacy/archive/20200930?hl=en-US (last visited October 10, 2023).

Activating Location History collection takes an intentional choice. Google accountholders must opt-in to the Location History collection function and enable location reporting for each specific device and application on which they use their Google account in order for that usage to be recorded in the Location History application. *See* Def. Mot., Ex. 1 at 23. In the *amicus curiae* brief Google submitted in *Chatrie*, and which the defendant attached to his motion, Google detailed the five steps a user must take to share Location History with Google. *See id.* at 7-8 ("[Location History] functions and saves a record of the user's travels only when the user opts into [Location History] 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, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it."); Def.'s Mot., Ex. 2 at 2 ("[Location History] is a service that Google account holders may choose to use to keep track of locations they have visited while in possession of their compatible mobile devices. … Users must explicitly opt in to the service."). Here, the simple fact that Google Location History existed for the defendant's account on January 6 indicates that he affirmatively opted-in to the service for the cellular device he carried that day.

Google's Privacy Policy confirms that Location History users turn over their information to Google knowingly. At the time relevant here, the policy informed users like the defendant:

> Your location information.
>
> We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Google Privacy Policy (Sept. 30, 2020).[9] The policy further stated that "[t]he types of location data [Google] collect[s] depend in part on your device and account settings," and provided

[9] https://policies.google.com/privacy/archive/20200930?hl=en-US (last visited October 10, 2023).

users with instructions on how to turn "location on or off." *Id.* And the policy again informed users that participation in Google's Location History service was voluntary and operated on an opt-in basis: "You can also turn on Location History if you want to create a private map of where you go with your signed-in devices." *Id.* Finally, the policy notified users that Google would share "personal information … if [it] ha[s] a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to … [m]eet any applicable law, regulation, legal process, or enforceable governmental request"; or to "[p]rotect against harm to the rights, property or safety of Google, [its] users, or the public as required or permitted by law." *Id.*

Nevertheless, as Google states, "it is the user who controls the [Location History] information. The user can review, edit, or delete her Timeline and [Location History] information from Google's servers at will." *Id.* at 8. Google correctly advised the court in *Chatrie* that "[t]he user thus controls her Google [Location History] data—unlike, for instance, the CSLI at issue in *Carpenter* or cellular data obtained via a 'tower dump.'" *Id.* The government agrees with Google's assessment. Like the defendant in *Chatrie*, the defendant here "voluntarily shared [his] information with Google." *See id.* at 9 (internal citation omitted). And he took no steps to suspend that sharing before or during January 6, notwithstanding the ease by which he could have turned off his phone or disabled the Location History function.

Judge Howell rejected a similar claim in *Bledsoe*, another January 6 case, where Facebook had disclosed to the government a list of accounts that had live-streamed or uploaded videos from within the U.S. Capitol building on January 6, based on location data collected by Facebook. Judge Howell found that the defendant there had "voluntarily conveyed to Facebook the information contained in Facebook's disclosure." *Bledsoe*, 630 F. Supp. 3d at 13. She noted that "Facebook's Data Policy inform[ed] users of how and when it collects information regarding account activity

generated by users of its services," including "'information from or about the computers, phones, or other devices where [users] install or access its Services'" and "'device locations" generated by "'GPS, Bluetooth, or WiFi signals.'" *Id.* Judge Howell found no evidence that "Facebook usage is essential to modern life" or that its collection of the defendant's location information was "automatic and inescapable." *Id.* For these reasons, she held that "[t]he volitional aspect of the [user-generated location] data at issue in th[at] case places the conduct into the heartland of the third-party doctrine recognized in *Smith* and *Miller*." *Id.* at 14. (internal quotation marks and citation omitted).

For all the reasons described above, the third-party doctrine applies here and dictates that the defendant lacks standing. The CSLI addressed in *Carpenter* is fundamentally different than Google Location History data, which is neither generated automatically nor indispensable to participate in modern society. *See Carpenter*, 138 S.Ct. at 2220. Thus, while *Carpenter* holds that the third-party doctrine does not cover CSLI, the same reasoning does not apply to Google Location History data, and this Court should not be the first in this Circuit to extend *Carpenter* in this manner.

Moreover, given the optional nature of Google's collection of Location History data, the affirmative steps the defendant took to enable it, and the control he continually exercised over that data but declined to assert, the defendant here cannot assert a reasonable expectation of privacy in the Location History data Google disclosed to the government in response to the Google Geofence Warrants, just as the defendant in *Bledsoe* could not establish a reasonable expectation of privacy in similar data disclosed by Facebook. Consequently, the defendant lacks standing to assert his claim, no Fourth Amendment violation occurred, and the Court should deny his motion.

ii. The Defendant's Reliance on *Carpenter* Is Misplaced

The defendant relies on *Carpenter* to assert that he had a reasonable expectation of privacy in the 9.5 hours of location information disclosed by Google. *See* Def.'s Mot. at 22-23. He is incorrect.

Carpenter concerned the sufficiency, under the Fourth Amendment, of court orders issued pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(d)—which requires a showing that "falls well short of the probable cause required for a warrant," 138 S. Ct. at 2221—for the government to obtain historical cell-site location information ("CSLI") for a cell phone used by a suspect in a series of robberies, where the responsive CSLI tracked the defendant's device for a period of over 120 days, *id*. at 2212, with no geographic limitation. The Court held that individuals have a "reasonable expectation of privacy in the whole of their physical movements," and "that accessing seven days of [CSLI] constitutes a Fourth Amendment search" requiring a warrant. *Carpenter*, 138 S. Ct. at 2217 & n.3.

But the *Carpenter* Court emphasized that its decision was "a narrow one," *id.* at 2220, where it "decide[d] no more than the case before [it]," *id*. at 2220 n.4, and thus its holding is specific to cell phone provider location data only, and even then only of 7 days or more. The Court summarized the scope of its ruling to be that "accessing seven days of CSLI constitutes a Fourth Amendment search," and explicitly declined to determine whether there is a "limited period" under seven days for which the government can acquire CSLI without implicating the Fourth Amendment. *Id.* at 2217 n.3.[10] No court has extended Carpenter beyond the limits the Court built

[10] *See also United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) (noting the Supreme Court's unresolved questions whether "the government [can] obtain less than seven days' worth of [CSLI] without a warrant," whether "the government [can] collect [CSLI] in real time or through 'tower dumps' not focused on a single suspect" without a warrant, and whether "other [non-CSU] business records that might incidentally reveal location information" require a warrant (internal quotations and citations omitted)).

into the opinion. In essence, *Carpenter* is best understood as a carve out from the *Smith*/*Miller* third-party doctrine that is based on the essentialness of cell phones to modern life and that attempts to otherwise leave the third-party doctrine untouched.

Carpenter also explicitly refused to decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant here because the investigative theory behind, technology involved in, and information disclosed via cell tower dump warrants are all similar to that for Google geofence warrants. As *Carpenter* explained, a tower dump provides the government with "information on all the devices that connected to a particular cell site [tower] during a particular interval." *Id.* Similarly, Google geofence warrants provide the government with information on all devices that were within a particular area during a particular interval. The only difference is whether the device connected to the cellular service provider (via a cellular account interacting with a tower), or Google (via an e-mail account interacting with a tower, Wi-Fi signal, GPS signal, or Bluetooth connection). *Cf. United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (holding that *Carpenter* "does not help" a serial robber identified via warrantless tower dumps because *Carpenter* "did not invalidate warrantless tower dumps," to which Google geofence warrants are analogous).[11]

---

[11] Other Courts have found that tower dump information may be obtained by a SCA § 2703(d) order, and that doing so raises no Fourth Amendment issue. *See United States v. Walker*, Case No. No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *7-8 (E.D.N.C. July 20, 2020) (distinguishing *Carpenter*, finding that cell tower location data for a particular place and time was properly obtained under § 2703(d) orders, and thus there was "no basis for attaching a Fourth Amendment interest to tower dump CLSI"). Pre-*Carpenter*, other courts also so held. *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d) …*, 42 F. Supp. 3d 511, 512-14 (S.D.N.Y. 2014) (M.J. Francis) (cell tower data available via 2703(d) order); *see also id*. at 515 (rejecting ACLU argument that "the Government's application here raises the spectre of 'wholesale surveillance' . . . . Such concerns center on the possibility of the Government tracking an individual's (or a number of individuals') every movement over a period of time."); *In the Matter of Application for Cell Tower Records Under 18 U.S.C. § 2703(D)*, 90 F. Supp. 3d 673, (S.D. Tex. 2015) (concurring with M.J. Francis, "conclud[ing] that the SCA authorizes the

Although *Carpenter* does not explicitly resolve whether obtaining 9.5 hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it does not. *Carpenter* is focused on protecting an individual's privacy interest in long-term, comprehensive location information. Indeed, the Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212 (emphasis added). The Court emphasized that long-term cell-site information created a "detailed" and "encyclopedic" record. *Id.* at 2216–17. *Carpenter* explained that "this case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220 (emphasis added).

In contrast, this case is about "a person's movement at a particular time"—the defendant's movements from 12:00 p.m. to 9:30 p.m. on January 6, 2021, *see* Expanded Google Geofence Warrant, *i.e.* the 9.5 hours spanning from the approximate beginnings of the Capitol riot to the time the House of Representatives resumed the 2020 presidential election certification proceeding.

---

compelled disclosure of cell tower log data" under § 2703(d) under Fifth Circuit precedent); *but see In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770-71 (S.D. Tex. 2013) (finding such request required a warrant after denying § 2703(d) order). As the Seventh Circuit explained in a cell tower data / robbery case, *Carpenter* "did not invalidate warrantless tower dumps which identified phones near one location (the victim stores) at one time (during the robberies)." *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019). The Seventh Circuit concluded that *Carpenter* "does not help" a robbery defendant who has challenged the cell tower data used to identify him. *Id.*; *see also United States v. Yang*, 958 F.3d 851, 862 (9th Cir. May 4, 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for defendant was not a search under Carpenter because "the information in the database did not reveal 'the whole of [the defendant's] physical movements.'"). In short, because one-time cell tower data information does not fall within the scope of *Carpenter*'s protection for long-term, comprehensive location information, it remains subject to the long-standing principle (described above) that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed to the government.

Here, the Google Geofence Warrants sought Location History data for only one location (the U.S. Capitol) during a discrete period of time on January 6 spanning at most 9.5 hours (from 12:00 p.m. to 9:30 p.m., plus two 15-minute control periods). Unlike the disclosure in *Carpenter*, then, the temporally and geographically limited disclosure in this case plainly did not involve the government seeking or obtaining a "detailed," "encyclopedic," "comprehensive record of [the defendant's] movements," *id.* at 2216-17, "compiled every day, every moment, over several years," *id.* at 2220. Instead, the government obtained a mere 9.5 hours of the defendant's location data on one date and, by definition, only within a carefully delimited geographic area. *See* Expanded Google Geofence Warrant. Nine and a half hours of location data is less than 6% of the period that *Carpenter* held constituted a search (i.e. 7 days, which equates to 168 hours). This data does not provide the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the *Carpenter* Court. 138 S. Ct. at 2217.

Contrary to the defendant's assertions and misplaced reliance, *Carpenter* neither held nor signaled that a defendant has a reasonable expectation of privacy in such a small quantity of location data. Given that *Carpenter* took pains to declare that it was not addressing whether a person has a reasonable expectation of privacy in less than seven full days of location history (let alone location history limited to one geographic area), *Carpenter* cannot be said to hold what the defendant claims it does. *Compare Id.* at 2217 n.3 *with* Def.'s Mot. at 22-23. The defendant is arguing that *Carpenter* should be enormously expanded to cover a much smaller total quantity of location data spread over a much shorter period of time. This Court should decline defendant's invitation to extend *Carpenter* to the drastically different circumstances presented in this case.

The defendant further asserts that the greater precision of Google's Location History data makes it more sensitive than CSLI and thus triggers a reasonable expectation of privacy in smaller

time periods of data, which he suggests justifies expanding *Carpenter*. *See* Def.'s Mot. at 23-24. But the defendant's argument is fatally flawed because the Supreme Court already incorporated this analysis into the balance it struck in *Carpenter*. In deciding that the government obtaining seven days or more of CSLI constituted a search but declining to hold that a person has a reasonable expectation of privacy in less than that, the Court stated that cell-site information "is rapidly approaching GPS-level precision," and its holding "t[ook] account of more sophisticated systems that are already in use or in development." 138 S. Ct. at 2218-19. Because the Supreme Court grounded *Carpenter*'s holding in an assumption that cell-site information would soon reach the precision of GPS, any distinction in precision between CSLI and Google Location History data cannot be used to justify expanding *Carpenter*. It would be double counting the same argument.

iii. *The Defendant Erroneously Relies on the Privacy Interests of Others*.

Finally, the defendant asserts that the Google Geofence Warrants were overbroad because they intruded on others' reasonable expectations of privacy, potentially generating false positives, *see* Def.'s Mot. at 6, 23, 34-35, but this argument fails for two separate reasons. First, the Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas*, 439 U.S. at 133-34 (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). The defendant therefore lacks standing to challenge the government's acquisition of others' location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting defendant's argument that investigator's use of a cell-site simulator violated the privacy rights of third parties, because the defendant was "not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated"). Second, these other individuals also voluntarily disclosed their location information to Google. Google's disclosure of their location information therefore did not infringe their Fourth Amendment rights either.

C. In Any Event, the Good-Faith Exception to the Exclusionary Rule Precludes Suppression Because the Investigators Relied on the Google Geofence Warrants in Good Faith and Thus the Exclusionary Rule Is Inapplicable.

Even if the Google Geofence Warrants somehow violated the defendant's Fourth Amendment rights, suppression would not be an appropriate remedy because the good-faith exception forecloses it in these circumstances. The exclusionary rule is not a "personal constitutional right." *United States v. Calandra*, 414 U.S. 338, 348 (1974). Application of the exclusionary rule "exacts a heavy toll on both the judicial system and society at large" because its effect often "is to suppress the truth and set the criminal loose in the community without punishment." *Davis*, 564 U.S. at 237. Therefore, suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Id.* at 236-37.

"The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring*, 555 U.S. at 140. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. Suppression is thus generally only appropriate "[w]hen the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights," *Davis*, 564 U.S. at 238 (citation and quotation marks omitted).

In contrast, the exclusionary rule should not be applied when an officer has in good faith obtained a search warrant from a judge or magistrate and acted within its scope. *Leon*, 468 U.S. at 921, 926. When police act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. In such

situations, "there is no police illegality and thus nothing to deter." *Id.* at 921.

Here, the agents who authored the affidavits in support of the Google geofence warrants did not "exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *Davis*, 564 U.S. at 238. Instead, they acted in good faith at every stage, following the exact process the Supreme Court, the D.C. Circuit, and other appellate courts have endorsed. There is "'nothing to deter'" by suppressing the evidence. *Ibid*.

Before submitting the Initial Google Geofence Warrant application to Magistrate Judge Harvey and before submitting the Expanded Google Geofence Warrant application to Magistrate Judge Meriweather, the agents consulted with federal prosecutors, who approved the affidavits' and warrants' sufficiency and constitutionality. *See also United States v. Matthews*, 12 F.4th 647, 656 (7th Cir. 2021) (noting the "general principle that attorney involvement supports a finding of good faith"). Then, when ready to submit the Initial Google Geofence Warrant application to Magistrate Judge Harvey and the Expanded Google Geofence Warrant application to Magistrate Judge Meriweather, the agents acted in concert with federal prosecutors, who submitted the filings in conjunction with associated motions to seal and applications for non-disclosure. *See* Application for Nondisclosure Order and to Seal Initial Google Geofence Warrant, 1:21-sc-77, ECF Nos. 4, 10 (signed by federal prosecutor); Application for Nondisclosure Order and to Seal Expanded Google Geofence Warrant, 1:21-sc-1660, ECF No. 2 (same). In both instances, the agents then obtained authorization for the warrant from a neutral and detached United States magistrate judge. *See Herring*, 555 U.S. at 144; *Chatrie*, 590 F. Supp. 3d at 937-941. Under *Leon*, "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." 468 U.S. at 922. In *McLamb*, the Fourth Circuit held that when considering

a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant. 880 F.3d 685. This is exactly what the affiant agents did.

Finally, the agents reasonably relied on Magistrate Judge Harvey's and Magistrate Judge Meriweather's authorizations for the Initial Google Geofence Warrant and Expanded Google Geofence Warrant, respectively. While Google geofence search warrants make use of "a rapidly developing technology," *McLamb*, 880 F.3d at 691, they are also widespread and increasingly common. Magistrate Judge Harvey's and Magistrate Judge Meriweather's decisions to authorize the Google Geofence Warrants were no rarities or outliers. "According to a recent report, Google received over 11,554 geofence warrants in 2020, up from 982 in 2018." *Unrelated D.D.C. Google Geofence Warrant* at *1. "Each of those warrants was authorized by a judge." *Id.* No federal court in the country has suppressed evidence derived from a judicially authorized Google geofence warrant. *See Rhine*, 2023 U.S. Dist. LEXIS 12308 at *65-66. The defendant fails to acknowledge, let alone address, this crucial fact. *See generally* Def.'s Mot.

Given this context, the federal prosecutor's blessing, and the fact that—as noted above—no court has ever suppressed the results of a Google geofence search warrant, the agents had no reason to question the reasonability of relying on Magistrate Judge Harvey's and Magistrate Judge Meriweather's authorizations of the warrants here. *See Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012) ("In the ordinary case, an officer cannot be expected to question the magistrate's probable cause determination' because '[i]t is the magistrate's responsibility to determine whether the officer's allegations establish probable cause, and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment.'" (quoting *Leon*)). To hold otherwise, this Court would have to find that "a reasonably well-trained officer would know that the warrant was illegal

despite the magistrate's authorization." *United States v. Martin*, 297 F.3d 1308, 1318 (11th Cir. 2022) (citing *Leon*, 468 U.S. at 922 n.23). There is no basis to make such a finding here.

The defendant argues that the *Leon* good faith exception is inapplicable because "the Geofence Warrants are so obviously lacking in any particularized probable cause . . . that no officer could have reasonably relied on [them]." Def.'s Mot. at 36-37.[12] To support this assertion, the defendant cites to a string of cases in which the reviewing court declined to apply the *Leon* good faith exception because of the "bare bones" nature of the affidavits supporting the warrants in question. *See id.* (citing cases). None of the cases the defendant relies upon are applicable because no reasonable person could describe the affidavits supporting the Google Geofence Warrants as "bare bones." The Initial Google Geofence Warrant affidavit was 32 pages long, *see id.*, and the Expanded Google Geofence Warrant affidavit was 57 pages long, *see id.* Both contained detailed descriptions of the riot's events to establish probable cause to believe that large numbers of people committed federal crimes on the Capitol grounds *and* inside the Capitol building on January 6, 2021, including violations of 18 U.S.C. §§ 1752(a) (Unlawful Entry on Restricted Buildings or Grounds) and 2101 (Rioting). *See* Initial Google Geofence Warrant ¶ 4; Expanded Google Geofence Warrant ¶ 4. Both affidavits described specific probable cause to believe that many rioters carried cellular devices, including video footage of the riot broadcast on national news coverage that appeared to have been recorded on handheld cell phones, *id.* ¶ 25, video and

[12] In making this argument, the defendant implicitly relies on one of the four situations *Leon* outlined where the good faith exception to the exclusionary rule would not apply: (1) the affiant misled the magistrate judge by swearing to information "the affiant knew was false or would have known was false except for his reckless disregard for the truth;" (2) the magistrate judge "wholly abandoned his judicial role;" (3) the "warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;" and (4) the warrant was "so facially deficient – *i.e.*, in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid." *Id.* at 923. The defendant argues the third scenario only. As such, he waives reliance on the first, second, and/or fourth.

photographs capturing people holding and/or using cellular devices during the riot, *id.* ¶¶ 27-28, and the agent's training and experience that such behavior is commonplace in modern life, *id.* ¶ 26. Both affidavits detailed the technology Google employs to capture location data for its users. *Id.* ¶¶ 31-45. And both affidavits detailed how the government would use the Google location data to identify suspects, victims, and/or witnesses who were within the restricted area during the riot without authorization, *see id.* ¶ 47, which at minimum provides probable cause that such a person violated 18 U.S.C. § 1752(a)(1) (Entering or Remaining in a Restricted Building or Grounds).

The Google Geofence Warrants are thus not remotely similar to the "bare bones" affidavits that are the subjects of the cases cited by the defendant. For example, the defendant relies on *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017). *See* Def.'s Mot. at 37. In *Griffith*, the government suspected the defendant of being the getaway driver in a gang-related homicide and obtained a warrant to search his girlfriend's apartment, in which he was living, for cell phones and/or other electronic communication devices. *Griffith*, 867 F.3d 1269. "The lion's share of the affidavit supporting the warrant application [was] devoted to establishing Griffith's suspected involvement as the getaway driver." *Id.* at 1271. Just two sentences of the affidavit addressed the actual topic of the search—cell phones and other electronic devices potentially used by Griffith to communicate with other gang members about the homicide—and those two sentences relied entirely on the affiant's general knowledge and experience concerning the ubiquity of cell phones and how gang members often use them. *Id.* at 1269. The affidavit "conveyed no reason to think that Griffith, in particular owned a cell phone," particularly since he had only recently been released from jail, *id.* at 1272; that, even if he did, it would be located in the apartment, *id.* at 1273-74; or any specific reason to believe that such a phone would contain incriminating evidence, *id.* at 1274-75.

Here, in contrast, the affidavits for both Google Geofence Warrants articulated specific probable cause to believe that rioters carried and used cell phones during the riot while on restricted grounds, including supporting photographs of rioters doing just that. Unlike the affidavit for Griffith's apartment, the Google Geofence Warrant affidavits articulated specific probable cause to believe that the location data sought would be found in servers, records, or premises maintained by Google. And the Google Geofence Warrant affidavits explained how and why that location data would provide incriminating evidence: it would, at minimum, show who was on restricted Capitol grounds without authorization. No reasonable person can equate the Google Geofence Warrants to the "bare bones" affidavit at issue in *Griffith*. The other cases relied upon by the defendant are similarly poor comparisons. *See* Def.'s Mot. at 37 (citing, *e.g.*, *United States v. Wilhelm*, 80 F.3d 116 (4th Cir. 1996) (affidavit to search a home for drugs and related evidence relied solely on report of unnamed informant, none of whose information was corroborated); *United States v. Underwood*, 725 F.3d 1076 (9th Cir. 2013) (affidavit to search a home for drugs and related evidence relied on "only two facts, foundationless expert opinion, and conclusory allegations.")).

The defendant's assertion that "the Geofence Warrants are so obviously lacking in any particularized probable cause . . . that no officer could have reasonably relied on [them]," Def.'s Mot. at 36-37, is also meritless because its foundation is at odds with binding precedent and regular police practice. The defendant asserts—in direct opposition to the Supreme Court precedent, *see Zurcher*, 436 U.S. at 555—that to be sufficiently particularized, a search warrant "must be particularized as to the *person* subject to the search," Def.'s Mot. at 37 (emphasis added). The government is unaware of any Supreme Court or D.C. Circuit case that has ever held this, and the defendant does not cite one, beyond misconstruing the holdings of *Ybarra* and similar cases (*see* discussion *supra*).

Moreover, the defendant's assertion that search warrants must be particularized to specific people runs contrary to routine application of the Fourth Amendment and police practice nationwide. For example, according to the defendant's novel interpretation of the Constitution, police cannot lawfully obtain a search warrant for a package, suitcase, empty parked car, or storage unit when a trained narcotics-detecting canine alerts to it without first identifying a real person as the sender/recipient/carrier/owner/driver/renter/etc. Similarly, according to the defendant's theory, police investigating a robbery of a cell phone store could not lawfully obtain a search warrant for a house where a tracking device attached to one of the stolen phone packages indicates the stolen phones were taken. Thus in addition to being contrary to well-established Supreme Court jurisprudence, the defendant's interpretation of the Fourth Amendment flies in the face of the daily experience of law enforcement officers, who routinely obtain warrants that identify a *thing or location* to be searched and not necessarily a *person or suspect* attached to that thing or place. Yet the defendant asserts that it is so obvious and well-established that search warrants must be particularized to a specific person that no reasonable officer could rely on a search warrant—like the Google Geofence Warrants—that was arguably not. This argument fails for the reasons stated above.

Accordingly, even if the defendant's particularly argument had a modicum of merit, which it does not, the defendant certainly cannot establish that his desired particularity standard is so obvious and well-established that "a reasonably well-trained officer would know that the warrant was illegal despite the magistrate's authorization." *Martin*, 297 F.3d at 1318 (citing *Leon*, 468 U.S. at 922 n.23). The defendant has thus failed to show that the agents acted in bad faith by relying on Magistrate Judge Harvey's and Magistrate Judge Meriweather's authorizations of the Google Geofence Warrants, which is what *Leon* requires before suppression of evidence would be

appropriate.

For all of the reasons stated above, the Court should reject the defendant's assertion that "the Geofence Warrants are so obviously lacking in any particularized probable cause . . . that no officer could have reasonably relied on [them]," Def.'s Mot. at 36-37, and find instead—as Judge Contreras held in *Rhine*, *see id.* at *108-109—that the agents reasonably relied in good faith on Magistrate Judge Harvey's and Magistrate Judge Meriweather's authorizations of the Google Geofence Warrants. Binding precedents—*Leon*, *Davis*, *Herring*, *Messerschmidt*, and their progeny—thus properly prevent the suppression of the evidence the government obtained from Google here.

III. CONCLUSION

For the reasons stated above, the United States requests that this Court deny the defendant's motion to suppress, 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