UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Case No. 1:21-CR-725 (MAU)**
	:	
JARED SAMUEL KASTNER	:	
	:	
Defendant.	:	

GOVERNMENT'S OPPOSITION TO DEFENDANT KASTNER'S MOTION TO SUPPRESS

The Court should deny Defendant Jared Samuel Kastner's motion to suppress the location evidence obtained by warrant from Google. ECF No. 109. Because Kastner has failed to show that the government violated the Fourth Amendment in collecting this information, his motion should be denied.

BACKGROUND

I. Offense Conduct

On December 8, 2021, the government filed a criminal information, charging Kastner with knowingly entering or remaining in a restricted building or grounds without lawful authority, in violation of 18 U.S.C. § 1752(a)(1); disorderly and disruptive conduct in a restricted building or grounds, in violation of 18 U.S.C. § 1752(a)(2); disorderly conduct in a Capitol building or grounds, in violation of 40 U.S.C. § 5104(e)(2)(D); and parading, demonstrating, or picketing in a Capitol building, in violation of 40 U.S.C. § 5104(e)(2)(G). ECF No. 7. These charges address Kastner's participation in the events of January 6, 2021, at the U.S. Capitol.

A joint session of the U.S. Congress convened at the U.S. Capitol on January 6 to certify the Electoral College vote count for the 2020 Presidential Election. ECF No. 1-1, at 1. At the time,

the U.S. Capitol building was locked and secured; only authorized individuals with appropriate identification could access it. *Id.* Temporary and permanent barricades were placed around the building's exterior. *Id.* In addition, the exterior plaza of the U.S. Capitol was closed to the public. *Id.*

As the joint session convened, a mass of individuals congregated outside. *Id.* Around 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of the U.S. Capitol Police, as others in the crowd encouraged and assisted those acts. *Id.* At 2:20 p.m., members of Congress and the Vice President evacuated the House and Senate chambers. *Id.* The joint session remained suspended until 8:00 p.m. *Id.* In the intervening period, scores of individuals entered the building without authority. *Id.*

For his part, Kastner drove from Ohio to the Washington, D.C. area on January 4, 2021, arriving in Maryland, where he was staying, in the early morning hours of January 5. *Id.* at 6-7. On January 6, 2021, Kastner entered U.S. Capitol building through the breached Senate Wing Door at approximately 2:17 p.m. with co-defendant Luke Faulkner. *Id.* at 4-5. After entering, he walked toward the Crypt, where he was confronted by a line of law enforcement officers who were preventing rioters from progressing into the building. ECF No. 22, at 3. During the standoff that ensued, rioters yelled at the law enforcement officers and moved forward toward the officers. *Id.* Instead of leaving, Kastner remained in the Crypt until a crowd of rioters pushed forward into the law enforcement officers, eventually breaking the line. *Id.* Ultimately, Kastner remained in the building for about 18 minutes. *Id.*

On January 6, 2021, Google recorded the location of a mobile device associated with Kastner's email address and phone number at the U.S. Capitol from approximately 2:14 p.m. until 2:52 p.m. ECF No. 1-1, at 2. Later that day, Kastner's mobile device traveled northwest out of

Washington, D.C., at approximately 4:15 p.m. *Id.* at 7. On January 7, 2021, Kastner's mobile device traveled back to his then residence in Beavercreek, Ohio. *Id.* Google estimates a device's location using GPS data, nearby Wi-Fi access points, and Bluetooth beacons. *Id.* Law enforcement obtained this information through search warrants. *Id.* at 2.

Due to his participation in the riot, the defendant was arrested on December 8, 2021. ECF No. 5. The FBI interviewed Kastner, and he admitted that he entered the U.S. Capitol building on January 6. ECF No. 22, at 6. The government also has extensive video evidence showing Kastner inside the U.S. Capitol building on January 6, as well as several witnesses placing Kastner in the U.S. Capitol building and in Washington, D.C. on January 6. *Id.*

II. Search Warrants

In an effort to identify individuals who breached the U.S. Capitol building, the government obtained search warrants for mobile-device location information stored at Google.

A. Google Geofence Warrant

On January 13, 2021, a magistrate judge issued a warrant directing Google to search its records for the location history of devices that connected to its services from a specific geographic area—the U.S. Capitol Building—during a specific time window on January 6, 2021.[1]

[1] This "geofence" warrant is "a warrant to obtain cellular phone data generated in a designated geographic area." *In re Information Stored by Google*, 579 F.Supp.3d 62, 69 2 (D.D.C. 2021) (citation omitted). "The 'geofence' 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.*

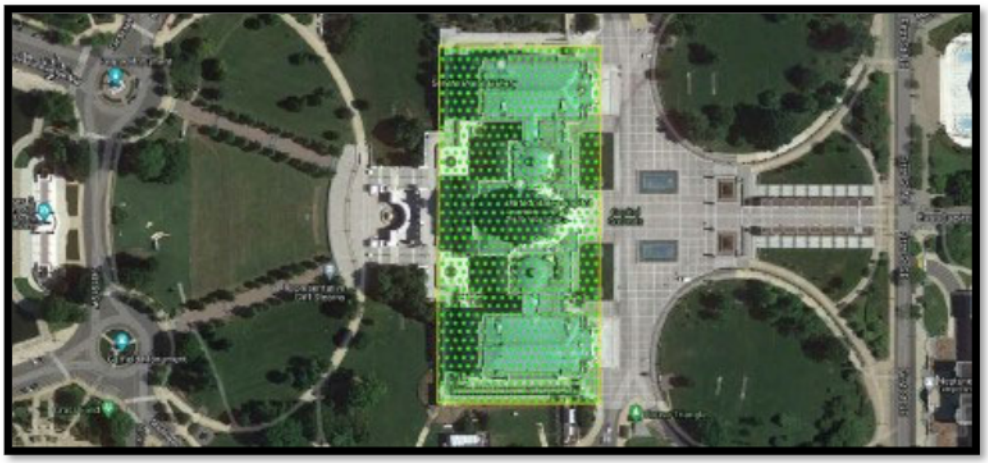

Image 1 – Depiction of approximate geographic area searched

See In re Information Stored at Google, 1:21-sc-77 (D.D.C. Jan. 13, 2021) ("Google Warrant"), at 4-5. Google was instructed to disclose a list of such devices. *Id.* at 6. The warrant specified that the government would review the information and confirm that it fell within the scope of its January 6 investigation. *Id.* at 10. Any information that fell outside the scope would be sealed and excluded from further review. *Id.*

A search-warrant affidavit summarized the government's investigatory steps. It noted that "video footage … appeared to be captured on mobile devices of persons" at the U.S. Capitol on January 6 "depicting evidence of violations of local and federal law." *Id.* at 17 (Aff. ¶ 25). In addition, news footage displayed "[m]any subjects … using a cell phone in some capacity." *Id.* at 18 (Aff. ¶ 27). The affidavit accordingly concluded that "evidence of the presence of cell phones within the [U.S. Capitol] may provide information regarding individuals who were in close proximity to the area of the target offense." *Id.* at 19 (Aff. ¶ 29).

The affidavit noted that Google offers applications, services, and internet browsing to users with a Google account. *Id.* at 21-22 (Aff. ¶¶ 36-37). It further noted that Google offers a service called "Location History," where users authorize Google to collect and retain a record of the locations where their mobile device transmitted information to Google. *Id.* at 22 (Aff. ¶ 39).

Google determines the device's location based on GPS data, the Wi-Fi access points, and Bluetooth beacons. *Id.* (Aff. ¶ 40). The affidavit stated that "[a] Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded." *Id.* at 23 (Aff. ¶ 41). When this function is enabled, "Google collects and retains location data for each device with Location Services enabled, [and] associates it with the relevant Google account." *Id.* That account is linked to "certain personal identifying information." *Id.* at 24 (Aff. ¶ 43).

As a result, the affidavit asserted "probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the [U.S. Capitol building] … during the time period described …for evidence of the crime(s) under investigation." *Id.* at 25 (Aff. ¶ 45).

ARGUMENT

The Court should deny Kastner's motion to suppress the evidence obtained from the warrant-authorized searches of records held by Google. As a preliminary matter, Kastner had no reasonable expectation of privacy in his location inside the U.S. Capitol building on January 6, 2021, or in the device-location information that Google collected in its normal course of business. He cannot therefore maintain his Fourth Amendment challenge. But even if Kastner has standing to raise his objections, they fail on the merits. The government obtained search warrants that were supported by probable cause and that specified their objects with particularity. These were not impermissible "general warrants." Finally, suppression would be inappropriate in all respects because investigators relied on the warrants in good faith.

I. Kastner has failed to show a reasonable expectation of privacy in the location information provided by Google.

To assert a Fourth Amendment claim, the defendant must demonstrate "a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). 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).

For two independent reasons, Kastner has failed to satisfy his burden

A. Kastner had no reasonable expectation of privacy in his location within the U.S. Capitol building on January 6.

Kastner cannot demonstrate a subjective expectation of privacy in the fact that he was inside the U.S. Capitol building on January 6 around 2:17 p.m. Nor would any such expectation be reasonable.

As to the former, Kastner has not demonstrated a subjective expectation of privacy in his location. He entered and departed the U.S. Capitol building through the Senate Wing Doors—where closed-circuit surveillance cameras readily recorded his movements. ECF No. 1-1, at 4-5.

Moreover, Kastner appeared on a news reporter's camera as he walked through the Crypt. *Id.* at 6. As a result of these video appearances, Kastner cannot credibly claim that he intended to keep his location 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.").

As to the latter, any assertion of 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 2. "Nothing is private about entry into the Capitol." *United States v. Bledsoe*, ---F.Supp.3d ---, No. 21-cr-204, 2022 WL 3594628, at *9 n.2 (D.D.C. Aug. 22, 2022). Access is restricted 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 4-5; *see also Bledsoe*, 2022 WL 3594628, at *9 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."). Given the U.S. Capitol building's function, access restrictions, and security, Kastner cannot assert a right to enter and roam it with anonymity.

That was doubly true on January 6, when members of Congress and the Vice President convened in a joint session to certify the results of the 2020 Presidential Election. "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). But Kastner approached and entered the U.S. Capitol building as part of a large mob. ECF No. 1-1, at 4-5. Any asserted privacy expectation by Kastner as to this location 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*, 2022 WL 3594628, at *9, *see also United States v. Lloyd Casimiro Cruz, Jr.*, 22-cr-00064-RBW, Hearing Transcript, January 13, 2023 (denying motion to suppress Google Location History data and finding defendant did not have a reasonable expectation of privacy in the U.S. Capitol Building on January 6) (attached as Exhibit A).

Because Kastner lacked a legitimate expectation of privacy in his whereabouts within the U.S. Capitol building on January 6, he cannot assert a Fourth Amendment violation with respect to his location information.

B Kastner also had no reasonable expectation of privacy in location information that he voluntarily shared with Google.

Kastner lacks Fourth Amendment standing for a second reason. The Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)). That principle independently forecloses Kastner's objection to the location information produced by Google.

Individuals lack a reasonable expectation of privacy in business records of banks, *see Smith*, 425 U.S. at 437-443, and pen-register records of telephone companies, *see Miller*, 442 U.S. at 742-744. 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). That principle applies here: when Kastner enabled the location-history function on his Google applications, he assumed the risk that Google would disclose his device-location information. That activity reflects a "business record[]" of Google for

which Kastner can "assert neither ownership nor possession." *Id.* at 440; *see United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) (cataloging cases holding that "subscriber information disclosed during ordinary use of the internet, including internet protocol addresses and email addresses, falls within the third-party doctrine").

In response to the geofence warrants, Google disclosed that a mobile device associated with Kastner's account had transmitted information from the U.S. Capitol building on January 6 at 2:17 p.m. This disclosure is the modern-day equivalent of the deposit slip in *Miller* showing that a customer deposited money into an account at a particular bank on a particular date, or the pen register in *Smith* showing that a person dialed a particular number on a particular date from the customer's home-telephone line. An individual "cannot assert a reasonable expectation of privacy" where he "affirmatively chose to disclose location data" through a smartphone application. *Sanchez v. Los Angeles Dep't of Transportation*, 39 F.4th 548, 559 (9th Cir. 2022); *see also Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020) ("[T]he allegation that Facebook collected 'IP addresses showing locations where plaintiff Heeger accessed his Facebook account' describes a practice akin to a pen register recording the outgoing phone numbers dialed on a landline telephone.") (brackets and citation omitted). Consistent with *Miller* and *Smith*, Kastner cannot assert a reasonable expectation of privacy in this information.

That is particularly so given Google's Privacy Policy, which informs users like Kastner that "[Google] collect[s] information about your location when you use [its] services, which helps [Google] offer features like driving directions for your weekend getaway or showtimes for movies playing near you." Google Privacy Policy (Sept. 30, 2020), at 4. The policy further states that that the "[t]he types of location data [Google] collect[s] depend in part on your device and account settings," and provides users with instructions on how to turn "location on or off." *Id.* Finally, the

policy notifies users that Google shares "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.* at 12.

In this circumstance, Kastner cannot assert a reasonable expectation of privacy in the information disclosed here: the fact that his mobile device connected to a Google application from inside the U.S. Capitol building. No Fourth Amendment violation accordingly occurred.

Judge Howell rejected a similar claim in *Bledsoe*, 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. Judge Howell found that the defendant had "voluntarily conveyed to Facebook the information contained in Facebook's disclosure." 2022 WL 3594628, at *8. 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.* The defendant also "t[ook] no available steps to avoid disclosing his location" on January 6; he instead uploaded a video from within the U.S. Capitol "during the normal course of using Facebook." *Id.* Finally, 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 *9 (internal quotation marks and citation omitted).

The same is true here. Kastner created a Google account and linked it to his phone. ECF No. 1-1, at 2. Kastner also would have enabled the Google location-history function for those services, thereby sharing his location voluntarily with Google. *See* Google Warrant 23 (Aff. ¶ 41); Google Privacy Policy (Sept. 30, 2020), at 4. Finally, Kastner took no steps to suspend that sharing on January 6—notwithstanding the ease by which he could have turned off his phone or disabled the location-history function. As in *Bledsoe*, Kastner has failed to establish a Fourth Amendment privacy interest in the location information that he voluntarily disclosed to Google and that the government later obtained by warrant.[2]

II. Even if the searches triggered the Fourth Amendment, the warrants articulated probable clause and were sufficiently particular.

Even assuming that the information obtained from Google implicated Kastner's reasonable expectation of privacy, the searches complied with the Fourth Amendment. The warrants were supported by probable cause and identified the records to be seized with sufficient particularly.

A. Ample probable cause supported the Google search.

The probable-cause standard "is not a high bar," *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018) (citation omitted), and "is less than a preponderance of the evidence," *United States v. Burnett*, 827 F.3d 1108, 1114 (D.C. Cir. 2016). In the context of a search warrant, a magistrate need only determine whether "reasonable inferences" from the evidence described in

[2] Kastner also cannot assert a Fourth Amendment interest under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), because the location information obtained from Google—confirming his location for a brief period of time in the U.S. Capitol Crypt—did not provide the government with "a detailed and comprehensive record of [his] movements." *Id.* at 2217. In addition, transmission of this information required "an[] affirmative act on the part of the user" to connect with the Google platform and enable location sharing. *Carpenter*, 138 S. Ct. at, 2220; *see also United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (*Carpenter* inapplicable to disclosure of IP information because "an internet user generates the IP address data … only by making the affirmative decision to access a website or application"). Finally, subscribing to Google's services is not "indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220.

the warrant application establish a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 240 (1983). Because the probable-cause standard deals not "with hard certainties, but with probabilities," *id.* at 231 (citation omitted), the facts presented to the magistrate need only "'warrant a person of reasonable caution in the belief' that contraband or evidence of a crime is present," *Florida v. Harris*, 568 U.S. 237, 243 (2013) (brackets and citation omitted).

The warrant affidavits in this case easily pass muster. First, they noted that the U.S. Capitol building was locked and secured on January 6. Only authorized individuals could enter it. Second, the warrants documented how the mob forced entry into the building: breaking windows, assaulting U.S. Capitol Police officers, and forcing the suspension of the joint session of Congress. Third, they observed that many individuals in the crowd carried cell phones. Fourth, the warrants explained that Google collected location data from mobile devices connected to their networks, and that Google likely had records documenting the devices that had connected from within the U.S. Capitol building on January 6. Fifth, the warrants noted that Google could identify the user registered to a particular mobile device.

These facts amply demonstrate a fair probability that records in Google's possession would identify individuals who entered the U.S. Capitol building on January 6 as part of the mob. That, in turn, would allow law enforcement to identify individuals who either committed or witnessed various federal crimes that occurred within the building that day. Those offenses included assaults on federal officers (18 U.S.C. § 111), civil disorder (18 U.S.C. § 231); conspiracy (18 U.S.C. § 371); unauthorized access of a protected computer (18 U.S.C. § 1030)[3]; possession of firearms in federal facilities (18 U.S.C. § 930); destruction of government property (18 U.S.C. § 1361);

[3] The affidavit mistakenly cites 18 U.S.C. § 1035 for this offense.

obstruction of a congressional proceeding (18 U.S.C. §§ 1505 & 1512); unlawful entry into a restricted building or grounds (18 U.S.C. § 1752(a)); rioting (18 U.S.C. § 2101); and violent or disorderly conduct within a Capitol Building (40 U.S.C. § 5104(e)(2)). *See, e.g.*, Google Warrant 3.

In response, Kastner states that "[t]he government didn't even know who they were searching for or even what specific crimes they were investigating." ECF No. 109, at 7. That contention is false. As the affidavits make clear, the government sought records identifying the individuals who entered the U.S. Capitol building as part of the mob on January 6. And the government did so to locate the individuals who either perpetrated or witnessed criminal activity. This record, combined with the "great deference" afforded to issuing magistrate's determination, *Gates*, 462 U.S. at 236 (citation omitted), leads to only one conclusion: probable cause supported these warrants.[4] *See also* Exhibit A, *Cruz* Hearing Transcript (Judge Walton denying motion to suppress Google Location History data and finding geofence warrants in a January 6 case were supported by probable cause).

[4] To the extent Kastner argues that a warrant must identify the particular suspects under investigation to satisfy the probable-cause standard, he is wrong. "Search warrants are not directed at persons; they authorize the search of places and the seizure of things." *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978) (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 n.19 (D.D.C. 2021) (cataloging cases).

B. The warrants contained particularized descriptions of the location to be searched at Google.

The warrants likewise delineated the particular locations to be searched—namely, the records linked to the geographically bounded area for Google. This location was as reasonably particularized as any other warrant for a physical space or a provider's records. The mere fact that it covered a large geographic location does not mean that the warrants lacked particularity; it simply reflects that the offenses here occurred across the entire U.S. Capitol building. That location was, in all respects, particularly described.

C. The warrant contained particularized descriptions of the targeted records.

The Fourth Amendment also 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 serves "to prevent general searches" that "take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The Google warrant satisfied this requirement. The search was constrained to records associated with a particular geographic location: the U.S. Capitol building. The Google warrant limited the search to only those mobile devices that Google detected to be within the longitudinal and latitudinal coordinates of the building. The search was also constrained to specific time periods of the U.S. Capitol siege on January 6, minimizing the likelihood that "tourists or bystanders [would] be found in any of this data." Google Warrant 25 (Aff. ¶ 46). As a result, this was not a "wide-ranging exploratory search[]" of Google's records. *Garrison*, 480 U.S. at 84, *see also United States v. David Charles Rhine*, 21-cr-00687-RC, ECF No. 79, at 36-78 (denying motion to suppress Google Location History data in a January 6 investigation and finding "Geofence Warrant was supported by particularized probable cause").

Several features of the warrant confirm its particularized nature. *First*, the government sought device-location information for a "discrete geographical area." *In re: Information Stored at Premises Controlled by Verizon Wireless*, 616 F.Supp.3d 1, 11 (D.D.C. 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"). As explained above, the scope of the geographic area here—the U.S. Capitol building—was tailored to the area in which the offenses occurred.

Second, "the information sought … [was] also particularized and limited to the types of data, *i.e.*, phone numbers and unique device identifiers, that can be used to identify" the subjects of the investigation: individuals who entered the U.S. Capitol building on the afternoon of January 6. *Verizon Wireless*, 616 F.Supp.3d at 11.

Third, the warrant 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.* For instance, the warrant directed Google to first provide a list of anonymized account identifiers representing the mobile devices that connected from within the U.S. Capitol building between 2:00-6:30 p.m. on January 6. Google Warrant 26-28 (Aff. ¶¶ 47a, 47c). The government then struck identifiers for devices that were also present within the building before (12:00-12:15pm) and after (9:00-9:15 p.m.) the mob siege—as those devices would not likely constitute evidence of a crime. *Id.* (Aff. ¶¶ 47b, 47c, 47e). Finally, the government sought an order from the magistrate judge directing Google to provide identification information for the

remaining devices. *Id.* (Aff. ¶¶ 47f, 47h). This sequence allowed the government to "analyz[e] the raw data disclosed by the Service Providers 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.'" *Verizon Wireless*, 616 F.Supp.3d at, at 12.

All told, "[t]he government … carefully tailored the warrants to the greatest degree possible to obtain cell phone data from the Service Providers to assist in identifying the Subject[s]" involved in the U.S. Capitol siege on January 6. *Id.* The geographic, temporal, and procedural restrictions cataloged above "demonstrate[] that the warrants are sufficiently particularized to provide specific guidance to law enforcement as to what data may be seized." *Id.*

In response, Kastner offers conclusory assertions that the warrants were "disconnected from particularity." ECF No. 109, at 7. He cites two examples of impermissible general warrants: a common-law warrant permitting British authorities to search every author, printer, and publisher in London for a treasonous publication; and a 1963 Texas warrant authorizing officers to search every book, record, or writing in the defendant's home for evidence of Communist Party affiliation. *Id.* at 5-7. Given the particularized descriptions and limitations in the Google warrant, these analogies fail.

This case also does not implicate overbreadth concerns. For instance, in *United States v. Chatrie*,590 F.Supp.3d 901 (E.D. Va. 2022), the district court held that a search warrant for mobile-device-location information within a 300-meter geofence in which a bank robbery had occurred violated the Fourth Amendment. Law enforcement had sought this information to "identify potential witnesses and/or suspects," but the court observed 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, the warrant broadly 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 in a nearby hotel, and residents of a nearby apartment complex and senior living center. *Id* at 930

In this case, by contrast, the Google warrant was geographically and temporally tailored. Given the scope and breadth of the mob's activities on January 6, the warrant articulated probable cause to believe that every person in the U.S. Capitol building at the time of the siege had either engaged in or witnessed criminal activity. There was thus little risk that the searches here "swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." *Id.* Moreover, the government undertook a multi-step review of the anonymized identifiers and excluded devices that were present in the U.S. Capitol during the hours before or after the siege, showing its efforts to further exclude individuals who likely did not participate in it. *See* p.15, *supra*, *see also Rhine,* 21-cr-00687-RC, ECF No. 79, at 64-75 (finding Google "Geofence Warrant's authorization was no greater than the scope of probable cause on which it issued, and therefore that it was not overbroad").

The remote possibility that the Google search identified mobile devices immediately adjacent to the U.S. Capitol building does not alter this calculus. *See* ECF No. 1-1, at 2 (noting that "Google estimate[d] that its location data [was] accurate to within 10 meters"). Access to these adjacent areas was also restricted. *See* Google Warrant 14 (Aff. ¶¶ 8-9). A fair probability accordingly existed that persons immediately adjacent to the U.S. Capitol building had also either engaged in or witnessed criminal activity on January 6. *See, e.g.*, 18 U.S.C. § 1752(a)(1) (authorizing punishment for any person who "knowingly enters or remains in any restricted building *or grounds* without lawful authority to do so") (emphasis added); 40 U.S.C.

§ 5104(e)(2)(F) (authorizing punishment for any person who knowingly and willfully "engage[s] in an act of physical violence *in the Grounds* or any of the Capitol Buildings") (emphasis added).

III. The good-faith exception independently forecloses relief.

Even assuming that one of the warrants was insufficiently particular, the good-faith exception forecloses application of the exclusionary rule in this case.

The exclusionary rule is a "'judicially created remedy"' that is "designed to deter police misconduct." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984) (citation omitted). The Supreme Court has explained that in order to justify suppression, a case must involve police conduct that is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system" in suppressing evidence. *Herring v. United States*, 555 U.S. 135, 144 (2009); *see Davis v. United States*, 564 U.S. 229, 236-239 (2011).

Leon recognized a good-faith exception to the exclusionary rule in the context of search warrants: evidence should not be suppressed if officers acted in an "objectively reasonable" manner in relying on a search warrant, even if the warrant was later deemed deficient. 468 U.S. at 922. *Leon* noted, for instance, that an officer's reliance would not be objectively reasonable when a warrant was "so facially deficient … 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 (citation and internal quotation marks omitted). "[T]he threshold for establishing" such a deficiency "is a high one, and it should be." *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 or his judgment that the form of the warrant is technically sufficient." *Leon*, 468 U.S. at 921.

The circumstances here do not come close to overcoming *Leon*'s good-faith exception. As in *Messerschmidt*, it would "not have been unreasonable—based on the facts set out in [the Google and AT&T] affidavit[s]—for an officer to believe" that the requested device information constituted evidence relevant to the January 6 attack. 565 U.S. at 549. The affidavits clearly articulated a fair probability that the individuals who stormed the U.S. Capitol building carried cell phones with them and that the providers had records identifying those individuals. It also would not have been unreasonable—based on the geographic, temporal, and procedural restrictions outlined in the Google warrant—for the executing officer to believe that the warrant complied with the Fourth Amendment's particularity requirement, particularly given that Chief Judge Howell recently cited those features in finding that a similar tower-dump warrant was sufficiently particularized. *See Verizon Wireless*, 616 F.Supp.3d at 11-12.

Because the officer who executed the Google warrants reasonably relied on the magistrate judge's approvals, they engaged in "nonculpable, innocent police conduct." *Davis*, 564 U.S. at 240. Suppression is thus unwarranted in all respects.

CONCLUSION

The motion to suppress should be denied.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
DC Bar No. 481052

By: /s/ Will N. Widman

Will N. Widman
Trial Attorney, Detailee
NC Bar No. 48158
District of Columbia
United States Attorney's Office
601 D Street, NW
Washington, DC 20530
(202) 353-8611
Will.Widman@usdoj.gov