FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Positive returns from U.S Capital Geo-Fence and Cell Phone tower dump **Date:** 03/22/2021

From: SEATTLE
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 176-SE-3382991 (U) Anonymous tip regarding David Rhine's illegal entry into U.S. Captial on January 6, 2021.

Synopsis: (U) Positive returns for phone number [redacted] in U.S. Capital Geo-Fence device database

Enclosure(s): Enclosed are the following items:
1. (U) Google Geo-Fence raw data and map overlay
2. (U) Google Geo-Fence raw data and map overlay

Details:

According to records obtained through a search warrant which was served onVerizon, on January 6, 2021, in and around the time of the incident, the cellphone associated with [redacted], subscribed to by David Rhine, was identified as having utilized a cell site consistent with providing service to a geographic area that included the interior of the United States Capitol building.

According to records obtained through a search warrant which was served on Google, a mobile device associated with phone number [redacted], subscribed to by subject David Rhine, was present at the U.S. Capitol on January 6, 2021. [redacted]

Title: (U) Positive returns from U.S Capital Geo-Fence and Cell Phone tower dump
Re: 176-SE-3382991, 03/22/2021

[redacted]

♦♦

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Case No. 1:21-cr-687 (RC)**
	:	
DAVID CHARLES RHINE,	:	
	:	
Defendant.	:	

UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION
TO SUPPRESS GEOFENCE EVIDENCE

Defendant David Charles Rhine asks this Court to suppress the location evidence for the defendant's smartphone device that the government obtained from Google via a "geofence" warrant. ECF No. 43 at 36. He also asks this Court to suppress all evidence derived from that evidence. *Ibid.* This Court should deny the defendant's motion. *First,* the defendant has failed to show that his Fourth Amendment rights were violated. *Second*, even if the defendant could show a Fourth Amendment violation, the good-faith exception to the exclusionary rule would preclude suppression. *Third*, and at a minimum, any defect in the geofence warrant would not invalidate the subsequently obtained warrant to search the defendant and his electronic devices, which was supported by ample independent evidence.

BACKGROUND

A. Factual and Procedural Background

1. At 1:00 p.m. on January 6, 2021, a Joint Session of the United States Congress, consisting of the House of Representatives and the Senate, convened in the Capitol Building. The Joint Session assembled to debate and certify the vote of the Electoral College of the 2020 Presidential Election. Prior to January 6, 2021, the U.S. Capitol Police, with authority over security on the Capitol grounds, had set up security barriers on the Capitol grounds. With the Joint

Session underway and with Vice President Mike Pence presiding, a large crowd gathered outside the U.S. Capitol. At approximately 2:00 p.m., certain individuals in the crowd forced their way through, up, and over the barricades and officers of the U.S. Capitol Police, and the crowd advanced to the exterior façade of the building. Members of the U.S. Capitol Police attempted to maintain order and keep the crowd from entering the Capitol; however, shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows. Shortly thereafter, at approximately 2:20 p.m., members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to – and did – evacuate the chambers.

The defendant, a resident of Bremerton, Washington, traveled to Washington, D.C. in early January 2021. On January 6, 2021, at approximately 2:42 p.m., the defendant entered the U.S. Capitol Building through the Upper House Door. He was carrying cowbells and a blue flag with white stars. Although a metal detector was present at the door, the defendant walked around it and did not go through any security screening. While inside, the defendant walked through multiple locations in the Capitol and climbed stairs to the third floor.

On the third floor, the defendant encountered law enforcement officers with weapons drawn. The officers directed the defendant and others present to drop to the floor. The defendant complied and was patted down for weapons. An officer found that the defendant was carrying two knives and a container of pepper spray. The officer seized these items and secured the defendant's hands behind his back with flex cuffs. Officers then escorted the defendant and others along a hallway and then down to the second floor, until they reached an interior area near the Rotunda Doors. Once in the vicinity of the Rotunda Doors, the escorting officer directed the defendant to exit the building and left. After the officer left, another rioter removed the flex cuffs from the defendant's hands. The defendant then exited the building through the Rotunda Doors at

approximately 3:05 p.m.

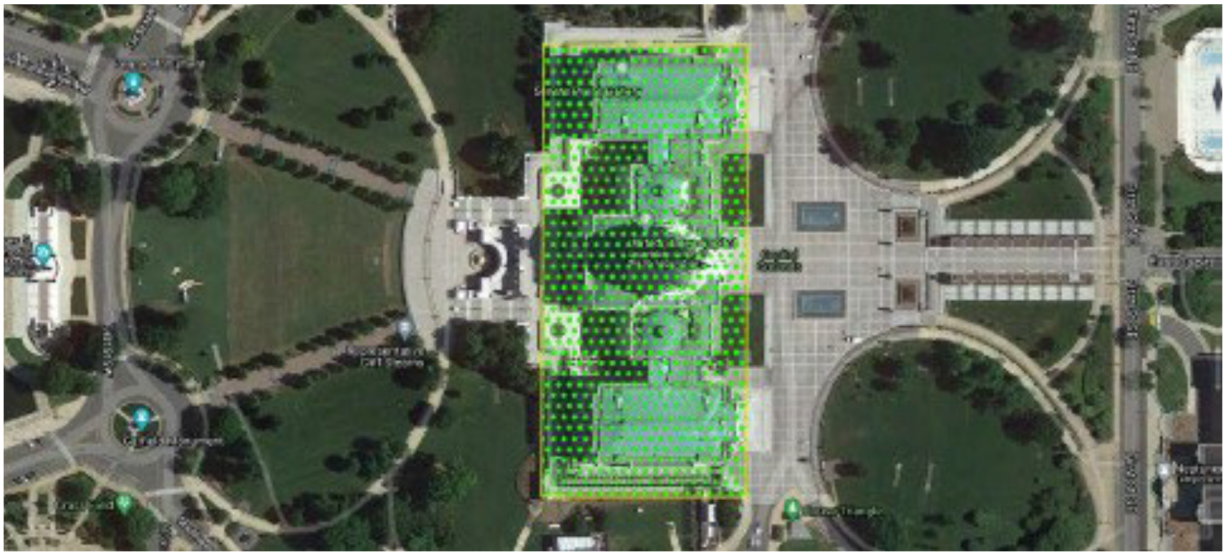
2. Based on his actions on January 6, 2021, the defendant was arrested and later charged by Information with Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority, in violation of 18 U.S.C. § 1752(a)(1); Engaging in Disorderly or Disruptive Conduct in any Restricted Building or Grounds, in violation of 18 U.S.C. § 1752(a)(2); Disorderly Conduct in a Capitol Building, 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).

The defendant now moves to suppress certain "Location History" data, which the government obtained from Google pursuant to a geofence warrant and which places the defendant in the U.S. Capitol in the afternoon of January 6. The defendant also moves to suppress any evidence derived from the geofence data.

B. The Google "Geofence" Warrant

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*.

On January 13, 2021, the government applied for – and a magistrate judge issued – a geofence warrant directing Google to disclose certain Location History information for devices that connected to its services from a specific geographic area corresponding approximately to the U.S. Capitol Building during specific time windows on January 6, 2021:



Def. Ex. A at 5. The warrant directed Google to disclose an anonymized list of such devices. *Id.* at 6-7. The warrant specified that the government would review the anonymized list and confirm that it fell within the scope of its January 6 investigation. *Id.* at 10. Any information that was determined to fall outside the scope would be sealed and excluded from further review. *Id.*

The search warrant affidavit described the government's investigatory steps. It noted that, during news coverage of the January 6 attack, video footage seemingly recorded with the mobile devices of persons at the U.S. Capitol on January 6 depicted evidence of criminal offenses. Def. Ex. A at 17. In addition, news footage showed many individuals using a cell phone inside the U.S. Capitol on that day for various purposes, including to record the events or take photos. Def. Ex. A at 18. The affidavit concluded that evidence of the presence of cell phones within the U.S. Capitol may provide information regarding individuals who were at or in near proximity of the January 6 attack. Def. Ex. A at 19.

2. The affidavit further explained that Google offers applications, services, and internet browsing to users with a Google account. Def. Ex. A at 21-22. These services include a service known as "Location History," whereby users can, when certain prerequisites are satisfied, authorize Google to collect and retain a record of the locations from which their mobile device

transmitted information to Google. Def. Ex. A at 22. Users of this service may later view their Location History through their Google account. *Id.*

Google's Location History service determines the device's location based on GPS data, Wi-Fi access points, and Bluetooth beacons. Def. Ex. A at 22-23. For each location data point, Google records the margin of error for its calculation as a meter radius (also known as the "maps display radius"). *Id.* Each data point has its own unique margin-of-error radius, which depends on the number and type of data sources and other information used to calculate the device's location at that particular time. *Id.* Google aims to have the radius accurately capture at least 68% of its users' locations. *Id.*; Def. Ex. D at 7-9. Thus, for example, a margin-of-error radius of 100 meters reflects Google's estimation that there is a 68% likelihood that the user is located within a 100-meter radius of the point estimate. Def. Ex. A at 23.

The affidavit further explained that Google accountholders 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. Def. Ex. A at 23.[1] When the Location History function is enabled, Google collects and retains location data for each device that has the location services function enabled, and associates it with the relevant Google account. *Id.* Google has stated that, in 2019, roughly one third of active Google users had location history enabled on their accounts. Def. Ex. D at 4.

3. The warrant set up a three-step process to obtain Location History data.

Step One. At the first step, the warrant directed Google to create, based on its Location

[1] *See also* Def. Ex. C at 13 ("[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. Ex. D at 2 ("Users must explicitly opt in to the service.").

History data, an anonymized list of devices that Google estimated, within its margin of error, were within the geofence (*i.e.*, the U.S. Capitol building) between 2:00 p.m. and 6:30 p.m. on January 6, 2021. Def. Ex. A at 4-6. At this first step, Google was also directed to create two additional anonymized lists of devices: one for devices that were estimated to have been within the geofence between noon to 12:15 p.m. on January 6, and one for devices that were estimated to have been within the geofence between 9:00 p.m. and 9:15 p.m. Def. Ex. A at 6, 25-27. These latter lists were created for the sole purpose of identifying devices of individuals very likely not involved in the riot,[2] so they could be culled before any identifying information was disclosed to the government. *Id.*

Critically, at step one, Google would not disclose any identifying information about any subscriber. To anonymize the preliminary data, Google was directed to identify each device via an anonymized identifier. Def. Ex. A at 27; Def. Ex. B at 6. For each anonymized device, Google was directed to provide only the basic Location History information that placed the device within the geofence (*i.e.*, point coordinates, time stamp, margin of error/maps display radius, and signal type (GPS, Wi-Fi, or Bluetooth)). Def. Ex. A at 27; Def. Ex. B at 6-7.

At step one, Google created three lists of anonymized devices reporting Location History data within the geofence between 2:00 p.m. and 6:30 p.m. Def. Ex. B. at 6. The first list was based on Google data as it existed on January 13, 2021; the second list was based on data as it existed in the evening of January 6, 2021; and the third list was based on Google data as it existed in the morning of January 7, 2021. Def. Ex. B. at 6. The lists ranged between, approximately, 5,600 and 5,700 unique (and anonymized) devices, with the lists based on January 6 and January

[2] Persons inside the U.S. Capitol between noon and 12:15 p.m. or between 9:00 p.m. and 9:15 p.m. on January 6, 2021, were very likely there lawfully; while they could have been witnesses to the various riot offenses (as were others not so excluded), as described below, this was a step the government took to narrow the focus of the warrant.

7 data containing several dozens more devices than the list based on January 13 data. Def. Ex. B. at 6.

Step Two. At step two, the government reviewed the anonymized data to identify information that was unlikely to be evidence of crime, so it could be culled from further steps. Def. Ex. A at 27. The government narrowed and refined the pool of relevant devices in three principal steps. First, the government compared the 2:00 p.m. to 6:30 p.m. data with the noon and 9:00 p.m. "control" lists, and then struck the control-list devices from the main list. Def. Ex. A at 27. That process eliminated over 200 unique devices. Def. Ex. B. at 7. Second, the government eliminated all devices except those that had at least one location data point within the Capitol building with a margin-of-error radius entirely within the geofence. Def. Ex. B. at 7. This process reduced the pool to approximately 1,500 unique devices. *Id.* Third, the government added back 37 devices that, despite not having a margin-of-error radius entirely within the geofence, still hit on the geofence between 2:00 p.m. and 6:30 p.m. and, in addition, had another indicator of criminal activity: the account's Location History data was deleted at some point between January 6 and January 13. Def. Ex. B. at 7-8.

Step Three. At step three, the government returned to the Court, requesting a second warrant directing Google to disclose additional information for the approximately 1,500 unique devices identified through the process above. Def. Ex. B. at 9-10. The warrant directed Google to provide its account identifier (*i.e.*, the subscriber's email address) and basic subscriber information. Def. Ex. B. at 10.

The defendant's device was identified as present within geofence in the afternoon of January 6 and had the parameters for which the magistrate authorized disclosure of identifying information. *See* Def. Exs. B. at 65, G, H. Google's Location History data showed that the defendant's device returned positive geofence hits between 2:24 p.m. and 4:37 p.m. on January 6,

2021. Def. Ex. H (listing 22 location data points within the U.S. Capitol and 26 location data points within the geofence between 2:24 p.m. and 4:47 p.m. on January 6, 2021).

C. The FBI's Investigation into the Defendant

On or about January 10, 2021, a tipster called the FBI to report that an individual named David Rhine, who resided in Bremerton, Washington, had entered the U.S. Capitol building on January 6, 2021. Def. Ex. M at 12. The tipster also provided the suspect's cell phone number and partial home address. *Id.* Among other information, the tipster stated that, on January 6, 2021, the defendant's wife had posted on Facebook that the suspect had entered the Capitol building that day. *Id.* The tipster stated that, after seeing the post, he confronted the suspect and suggested that he report himself. *Id.* According to the tipster, the suspect did not deny entering the Capitol building and said that the Capitol police moved the barriers to let him into the building. *Id.*

On January 12, 2021, a second tipster submitted an online tip that, based on second-hand knowledge, an individual named David Rhine had been inside the Capitol during the riot. Def. Ex. M at 12. The second tipster also provided the suspect's business phone number and full business address. *Id.*

Based on a search of open-source information and law enforcement databases, the FBI identified the defendant. Def. Ex. M at 12. The defendant's cell phone and other identifying information also matched the information provided by the first tipster. *Id.* In addition, location records obtained from Verizon pursuant to a search warrant[3] showed that, during the January 6, 2021 riot, the defendant's cell phone connected to a cell site in Washington, D.C. that provided

[3] The defendant has not moved to suppress the Verizon cell site data. He merely states, in a footnote and with no argument, that "the warrant and search that yielded [the Verizon] information was also constitutionally suspect." ECF No. 43 at 12 n.8. By not filing a timely motion to suppress, the defendant has waived any suppression claim as to that evidence.

service to the interior of the U.S. Capitol building. Def. Ex. M at 12.

In mid-March 2021, the FBI interviewed the first tipster. Def. Ex. M at 13. The tipster had known the defendant since 2017, but had no indication that the defendant had traveled to Washington D.C. in January 2021 until learning, through a friend, of the Facebook post by the defendant's wife. *Id.* In the post, the defendant's wife had reportedly stated that she was proud of her husband for being at the January 6 rally and for entering the Capitol. *Id.*[4] When the tipster contacted the defendant and his wife by text about his presence in the U.S. Capitol, the defendant claimed that he saw no violence, and that Capitol Police removed barriers and let people in. Def. Ex. M at 13-14. The tipster believed that the defendant's wife had deleted the Facebook post shortly after posting it. *Id.*

In June 2021, the FBI's principal investigator spent approximately 10 hours reviewing videos from the U.S. Capitol Building, attempting to locate the defendant and his activities during the January 6 riot. Def. Ex. O. During this initial review, the investigator already had access to the geofence data, which the FBI investigators received in March 2021. Gov't Ex. 1. Despite having access to the geofence data, the investigator's initial efforts were not successful. Def. Ex. O. After receiving additional training about the FBI's video system, the investigator was able to locate the defendant in the Capitol Police footage. Def. Exs. O, P. The FBI then traced the defendant through U.S. Capitol based on his clothing and appearance. Def. Ex. O at 1-4 (trace of the defendant through the U.S. Capitol); Def. Ex. M at 15-22.

In September 2021, the first tipster identified the defendant in the following screenshot, which was obtained from the Capitol Police's closed-circuit surveillance system inside the U.S. Capitol building on January 6, 2021:

[4] Although the tipster did not see the actual post, he did see a screenshot of it, which the tipster's friend sent to him. Def. Ex. M at 13.

Def. Ex. M at 14-15. The tipster also reviewed several other screenshots, but could not confirm the defendant's identification due to the poor quality of the images. *Id.*

On November 5, 2021, the government applied for – and a magistrate issued – a search warrant for the defendant, including his home, and any electronic devices found with him. *See* Def. Ex. M, N. In a supporting affidavit, the investigator described the evidence supporting probable cause: (i) the tipsters' initial information; (ii) the Verizon location data; (iii) the Google geofence data; (iv) the investigators' March 2021 interview with one of the tipsters; (v) the investigators' review of the FBI's video database and trace of the defendant throughout the Capitol; and (vi) the tipster's identification of the defendant in one of the screenshots from the Capitol Police's closed-circuit surveillance system. Def. Ex. M. at 12-22. When the government executed the warrant, it seized (and later searched) the defendant's cell phone. *See* Def. Ex. Q.

ARGUMENT

The Court should deny the defendant's motion to suppress the evidence obtained from the warrant-authorized search of records held by Google. As a preliminary matter, the defendant had no reasonable expectation of privacy in his location inside or around the U.S. Capitol building on

January 6, 2021. Nor did the defendant have a reasonable expectation of privacy with respect to the short-term Location History data that Google disclosed pursuant to the geofence warrant. The defendant therefore cannot maintain his Fourth Amendment challenge. But even if the defendant has standing to raise his objections, they fail on the merits. The government obtained search warrants that were supported by probable cause, were not overbroad, and specified the things to be searched and the items to be seized with particularity. These were not impermissible "general warrants." Furthermore, suppression would be inappropriate in all respects because the investigators relied on warrants issued by the magistrate in good faith. At a minimum, any defect in the geofence data did not invalidate the subsequent warrant to search the defendant, his home, and his devices, which was supported by ample untainted evidence.

I. The Defendant 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). Or, put differently, "'[s]uppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence." *United States v. Sheffield*, 832 F.3d 296, 303-304 (D.C. Cir. 2016) (quoting *Alderman v. United States*, 394 U.S. 165, 171-172 (1969)). 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." *Sheffield*, 832 F.3d at 305.

For two independent reasons, the defendant has failed to carry his burden.

A. The Defendant Had No Reasonable Expectation of Privacy in His Location Within the U.S. Capitol Building on January 6.

The defendant cannot demonstrate a subjective expectation of privacy in the fact that he was inside (or around) the U.S. Capitol building in the afternoon of January 6, 2021, as the riot was unfolding. Nor would any such expectation be reasonable.

As to the subjective prong, the defendant has not demonstrated a subjective expectation of privacy in his location. He entered the U.S. Capitol building through the Upper House Door on the second floor of the U.S. Capitol, where a closed-circuit surveillance camera readily recorded his movements. ECF No. 1-1, at 5. Moreover, in the afternoon of January 6, the defendant gave what appears to be an interview as he stood on the steps immediately outside the U.S. Capitol:

In the recording, the defendant is depicted holding a microphone, aware that he is being recorded and voluntarily participating in the recording. The defendant therefore cannot credibly claim that he intended to keep his location near 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.").

As to the objective prong, 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*, No. 21-cr-204 (BAH), 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 2. Surveillance cameras then monitor individuals after they enter the building. *Id.* at 4-10; Def. Ex. P at 1-4; *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, the defendant cannot assert a reasonable expectation 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). As the video evidence shows in this case, however, the defendant entered the U.S. Capitol building alongside many other rioters. ECF No. 1-1, at 4-10. Any asserted privacy expectation by the defendant 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.

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

B. The Defendant Also Had No Reasonable Expectation of Privacy in the Short-Term Location Information That He Voluntarily Shared with Google.

The defendant lacks Fourth Amendment standing for a second reason as well. 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*, 442 U.S. at 744 (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)). That principle independently forecloses the defendant's objection to the location information produced by Google.

1. 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 the defendant enabled the Location History function on his Google account (and device), he assumed the risk that Google might, in some circumstances, disclose some data points from those records. The location data was, in other words, a collection of "business records" of Google for which the defendant can "assert neither ownership nor possession." *Smith*, 425 U.S. at 440.

In response to the geofence warrant, Google ultimately disclosed that a mobile device associated with the defendant's account had transmitted information from the U.S. Capitol building during a four-and-one-half-hour period on January 6. *See* Def. Exs. G, H. 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*, the defendant cannot assert a reasonable expectation of privacy in the location history information he shared with Google.

That is particularly so in light of Google's opt-in protocol for sharing Location History and

Google's Privacy Policy. As explained in the warrant affidavit and the defendant's own exhibits, Google accountholders 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 in the Location History application. Def. Ex. A at 23; Def. Ex. D at 2. Indeed, to successfully opt in to Google' Location History functionality, a user must complete a multi-step process, both on his device and on his Google account. *See* Def. Ex. C at 13 ("[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. Ex. D 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.").

Google' 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).[5] The policy further stated that "[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.* And the policy again informed users that participation in Google's Location History service is voluntary and operates on an opt-in basis:

[5] https://policies.google.com/privacy/archive/20200930?hl=en-US (last visited November 30, 2022).

"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 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.*

Against this backdrop, the defendant cannot assert a reasonable expectation of privacy in the information disclosed here: the fact that his mobile device connected to an opt-in Google application from inside the U.S. Capitol building over a four-and-one-half-hour period on January 6. No Fourth Amendment violation accordingly occurred.

Chief Judge Howell recently 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. Chief Judge Howell found that the defendant there 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.* And Chief 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. Using Google's Location History option is in no way "essential to modern life," not least because Google makes clear it is optional even for its own users. Here, the defendant created a Google account and linked it to his cell phone. Def. Ex. G, H. The defendant also would have completed a multi-step process – both on his account and his device – to enable Google's Location History function, thereby sharing his location voluntarily with Google. *See* Def. Ex. C at 13; Google Privacy Policy (Sept. 30, 2020).[6] Finally, the defendant took no steps to suspend that sharing before January 6, notwithstanding the ease by which he could have turned off his phone or disabled the Location History function. As in *Bledsoe*, the defendant 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. Neither *Carpenter v. United States*, 138 S. Ct. 2206 (2018), nor the defendant's contrary contentions alter that conclusion.

The Court in *Carpenter* held that the government's actions in accessing seven days of cell-site location information data constituted a Fourth Amendment search. *Carpenter*, 138 S. Ct. at 2217 & n.3. Although cell-site records are created and maintained by third-party wireless carriers, *see id.* at 2219, the Court "decline[d] to extend *Smith* and *Miller* to cover the[] novel circumstances" at issue in *Carpenter*. *Id.* at 2217. The Court emphasized "the unique nature of cell phone location records," which can provide "a detailed and comprehensive record of the person's [physical] movements" resulting in "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Id.* at 2217-2218. The Court reasoned that the information in *Carpenter* was "not about 'using a phone' or a person's movement at a particular time," but instead implicated "a detailed chronicle of a person's physical presence compiled every

[6] https://policies.google.com/privacy/archive/20200930?hl=en-US (last visited November 30, 2022).

day, every moment, over several years." *Id.* at 2220. The Court explained, however, that its holding was "a narrow one" and did not cover different technologies, including "tower dumps" where the government seeks "a download of information on all the devices that connected to a particular cell site during a particular interval." *Id.*

Contrary to the defendant's assertions (ECF No. 43 at 13-20), *Carpenter* is distinguishable from this case in at least three critical respects. *First*, *Carpenter* involved an order to produce cell site data for (at least) seven continuous days and with no geographic limitation. 138 S. Ct. at 2217 & n.3. Such a disclosure, the Court explained, could provide the government with "a detailed and comprehensive record of [the defendant's] movements." *Id.* at 2217.[7] This case, in contrast, involves a warrant to disclose Location History data for only one location (the U.S. Capitol) during a discrete period of time on January 6 spanning at most five hours (from 2:00 p.m. to 6:30 p.m., plus two 15-minute periods). Def. Ex. A at 4-6. Unlike the disclosure in *Carpenter*, then, the temporally and geographically limited disclosure in this case plainly did not provide the government "with a detailed and comprehensive record of [the defendant's] movements." 138 S. Ct. at 2217; *see id.* at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of [cell site location information] constitutes a Fourth Amendment search."). At a minimum, because the geofence was limited to the U.S. Capitol, there is no merit to any suggestion that the disclosure in this case could have implicated the "risk of exposing information 'the indisputably private nature of which takes little imagination to conjure: the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-

[7] *See Carpenter*, 138 S. Ct. at 2217 (noting that "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts," and expressing concern that such "time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" (citation omitted)).

the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.'" ECF No. 43 at 15 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).[8]

Second, *Carpenter* found it significant that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." 138 S. Ct. at 2220. But the opposite is true of the Location History data at issue here. As explained above, "[u]sers must explicitly opt in to" Google's Location History service. Def. Ex. D at 2. Indeed, 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." *Id.* (emphasis added).

Third, and related, *Carpenter* relied on the fact that "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society." 138 S. Ct. at 2220 (internal quotation marks and citation omitted). Google's Location History service, in contrast, is not "indispensable to participation in modern society." *Id.* It is just an opt-in service that Google users "can … turn on … if [they] want

[8] The defendant's reliance (ECF No. 43 at 16) on the magistrate judge's decision in *Matter of Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763 (N.D. Ill. July 8, 2020), is misplaced for essentially the same reason: there, the geofence covered "a congested urban area encompassing individuals' residences, businesses, and healthcare providers," so that "the vast majority of cellular telephones likely to be identified in [that] geofence will have nothing whatsoever to do with the offenses under investigation." *Id.* at *5 (footnote omitted); *see also id.* at *5 n.7 (stating that "[t]he government's inclusion of a large apartment complex in one of its geofences raise[d] additional concerns … that it may obtain location information as to an individual who may be in the privacy of their own residence"). Again, the geofence here was limited to the U.S. Capitol during a time period when members of the public were not allowed to be in the area.

to create a private map of where you go with your signed-in devices." Google Privacy Policy (Sept. 30, 2020).[9]

The defendant's reliance on the Fourth Circuit's decision in *Leaders of a Beautiful Struggle v. Baltimore Police Dept.*, 2 F.4th 330 (4th Cir. 2021) (en banc), is also misplaced. *Leaders of a Beautiful Struggle* involved a Fourth Amendment challenge to a police-contracted aerial surveillance program over the City of Baltimore, whereby airplanes flew over the city for an estimated 12 hours each day, covered around 90% of the city, recorded every movement of every person who was outdoors within the area, and retained the data for 45 days. *Id.* at 334. When a crime occurred, the police could review photographs from the relevant area, retroactively track individuals, and order "reports" and "briefings" prepared by the contractor's analysts. *Id.* The Fourth Circuit concluded that *Carpenter* applied to the city's program because the program "enable[d] photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with." *Id.* at 342. In so holding, the court of appeals rejected the district court's characterization of Baltimore's aerial surveillance program as "capable of only short-term tracking" just because the airplanes did not fly at night, thus "prohibit[ing] the tracking of individuals over the course of multiple days.'" *Id.* The court of appeals found it dispositive that, despite the gaps, the program "record[ed] the movements of a city" and could, "[w]ith analysis, … reveal where individuals come and go over an extended period," "enabl[ing] police to deduce from the whole of individuals' movements." *Id.* at 346; *see also id.* at 343 (explaining that "most people do most of their moving during the daytime, not overnight" and, in any event, "police will at least sometimes be able to re-identify the same target over consecutive days").

[9] https://policies.google.com/privacy/archive/20200930?hl=en-US (last visited November 30, 2022).

This case is readily distinguishable. This case does not involve the tracking of the daytime movements of every person who steps outside within an entire city over a 45-day period. It involves a single provider's Location History data for individuals who opted into an elective location-based service and who were within (or in near proximity of) a single, highly surveilled government building over a specific four-and-one-half-hour period on January 6, 2021 – at a time when members of the public were not allowed to be in the area. Neither the holding nor the reasoning of *Leaders of a Beautiful Struggle* supports the defendant's position in this case.

The defendant also downplays (ECF No. 43 at 18-20) the voluntary, opt-in nature of Google's Location History service. He acknowledges (*id.* at 18) that Google's "Location History must be enabled by the user," but speculates that the opt-in process "is unlikely to have been knowing or informed" and might have been "deceptive." *Id.* His worst-case scenario is that a user *possibly* "would have seen" only "one line of text about Location History in a pop-up screen." *Id.* He also complains that it may not have been "clear" that "location data would be saved by Google, as opposed to stored locally on the device," and that "nothing explained that Location History will operate independently, regardless of whether the phone is in use." *Id.* at 18-19.

The defendant's speculative complaints are unavailing. To begin with, the defendant reverses the burden of proof. It is the defendant who "always bear[s] the burden of establishing that the government violated a privacy interest that was protected by the Fourth Amendment." *Sheffield*, 832 F.3d at 305. If the defendant wants to argue that he did not voluntarily agree to turn over his Location History data to Google, he must offer evidence – not speculation – of how he opted in and why that process was insufficient. He has failed to do so.

In any event, the defendant's complaints are unavailing even on their terms. As an initial matter, the steps described by the defendant do not appear to fully and accurately account for the steps he would have taken to create a Google account, set up the phone he used at the time of the

riot, and opt in to Google's Location History service. For example, the defendant's argument (ECF No. 43 at 18-20) does not address the steps involved in the initial creation of his Google account or signing into that account using his phone.

Nevertheless, assuming the defendant's description is complete and accurate, the defendant voluntarily disclosed his location information to Google. The defendant does not contest – and his own exhibit confirms – that during setup on his Android phone, a screen on the user's phone informs the user that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." Def. Ex. I at 6; *see also* Def. Ex. E at 392. The defendant also does not appear to dispute that, in response to this warning, he necessarily clicked "YES I'M IN." Def. Ex. I at 6. And he does not contest that, as any Google user who sets up a Google account, he agreed to Google's Terms of Service and Privacy Policy, Def. Ex. E at 382, which describe Google's use, storage, and deletion of location information.[10] These facts establish that the defendant voluntarily turned over his Location History data to Google.[11]

---

[10] The defendant complains that a user of Google's location-based services cannot tell that Google will store her location information (ECF No. 43 at 18-19), but the Supreme Court held in *Smith v. Maryland* that the third-party doctrine applies to information voluntarily disclosed to a third party regardless of any expectations regarding subsequent storage. In *Smith*, the defendant argued that the third-party doctrine should not apply to his dialed numbers because the phone company did not usually store information concerning local phone calls. The Supreme Court rejected his argument: "The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record." *Smith*, 442 U.S. at 745. Thus, the defendant would have no reasonable expectation of privacy in information he disclosed to Google even if he had not been informed that Google would store that information.

[11] The defendant also asserts (ECF No. 43 at 19-20) that "Google's Privacy Policy or Terms of Service have little if any bearing on an individual's Fourth Amendment expectations of privacy" because, he says, "Fourth Amendment rights do not rest on the terms of a contract." That's a non sequitur. While contract terms are not invariably dispositive, they do inform the reasonableness of those parties' expectation of privacy, the linchpin under the Fourth Amendment. *Smith*, which the defendant cites (ECF No. 43 at 20), actually *refutes* his position. *See Smith*, 442 U.S. at 742-743 (finding no subjective privacy expectation in dialed numbers in part because "[m]ost phone

3. Finally, the defendant asserts that he also had a "property interest in his Location History data." ECF No. 43 at 20-23. But this argument flies in the face of the fundamental principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443. The Supreme Court has recognized that a physical trespass for purposes of obtaining information is a search. *See United States v. Jones*, 565 U.S. 400, 404-05 (2012). But the investigation in this case involved no physical trespass; instead, the geofence warrant directed Google to produce specified information that some of its customers had disclosed to it. The defendant cites no precedent – and the government is aware of none – in which a court has relied on a "property-based theory" to discard the third-party doctrine of *Smith* and *Miller* and prevent a service provider from providing electronic evidence to the government. Justice Gorsuch's solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on a property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-2272 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding. *See Rodriguez de Quijas v. Shearson/Am. Exp., Inc.*, 490 U.S. 477, 484 (1989) (only the Supreme Court has "the prerogative of overruling its own decisions").[12]

In any event, the defendant's assertion that Google is a "mere bailee" of his Location History information has no merit. The defendant relies on statements by Google referring to user

---

books t[old] subscribers" that the phone company could help identify the source of unwelcome calls).

[12] Contrary to the defendant's suggestion (ECF No. 43 at 21), *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), did not adopt a property-based theory. There, the Sixth Circuit held that "if government agents compel an [internet service provider] to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception." *Id.* at 286. But the court relied on *Katz* and the subscriber's legitimate expectation of privacy in the content of his emails, not a property theory of the sort the defendant advocates here.

data as "your data" and "your information," and to the fact that Google gives users some control over their location data – including, in some respects, the option to manage, export, or delete the data. ECF No. 43 at 21. But defendant's theory ignores that Google does not merely store its customers' Location History data; it also uses that information to provide location-based services. *See, e.g.*, Def. Ex. D at 2 (describing services that Google provides to customers who opt into Location History). Under these circumstances, Google's disclosure of its customers' Location History to investigators does not implicate the Fourth Amendment. For example, the owner of documents may retain a property interest in documents shared with an accountant, but the owner's Fourth Amendment rights are not infringed when the accountant conveys them to the government. *See Couch v. United States*, 409 U.S. 322, 335 (1973). And the same principle applies even more forcefully here because Google's Privacy Policy squarely provides that "Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement." Google Privacy Policy (Sept. 30, 2020).[13]

II. Even If a Search Implicating the Defendant's Fourth Amendment Rights Occurred, the Geofence Warrant Articulated Probable Cause and Was Sufficiently Particular.

Even assuming that the information obtained from Google implicated the defendant's reasonable expectation of privacy, any search complied with the Fourth Amendment. The geofence warrant issued by the magistrate in this case was supported by probable cause and identified the records to be disclosed and the records to be seized with sufficient particularly.

A. Probable Cause Supported the Warrant Applications

1. The probable-cause standard "is not a high bar," *District of Columbia v. Wesby*,

[13] https://policies.google.com/privacy/archive/20200930?hl=en-US (last visited November 30, 2022).

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 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).

In addition to probable cause, 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. "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Because the permissible scope of a warrant depends on the breadth of the supporting probable cause, "the requirement of particularity is closely tied to the requirement of probable cause." *United States v. Griffith*, 867 F.3d 1265, 1275 (D.C. Cir. 2017) (internal quotation and citation omitted). "[A] broader sweep," however, may be permissible "when a reasonable investigation cannot produce a more particular description" prior to obtaining and executing the warrant. *Id.* at 1276.

2. The geofence warrant amply satisfies these standards. Here, the affidavit in support of the initial geofence warrant established an ample basis for the magistrate's finding of probable cause. In particular, the first affidavit (Def. Ex. A) established: (1) that the U.S. Capitol building and its exterior plaza were secured on January 6, so that only authorized individuals were permitted to enter it; (2) that, starting at around 2:15 p.m., the mob forced entry into the building, including

by breaking windows and assaulting Capitol Police officers, and forced the suspension of the joint session of Congress; (3) that, by 6:30 p.m., the U.S. Capitol Building was cleared of the rioters; (4) that many individuals in the mob carried and used cell phones; (5) that Google collects Location History data for users who have opted in to the service; (6) that Google likely had Location History records for devices that had connected from within the U.S. Capitol building on January 6, which would assist with the criminal investigation; and (7) that Google also had subscriber information that could, at a later time, identify the user associated with a particular mobile device. *See* Def. Ex. A.

The second affidavit established even more targeted probable cause for the devices for which the government requested identifying information. *See* Def. Ex. B at 7-8. It described the process used to (i) exclude devices that were unlikely to belong to rioters; (ii) exclude devices whose confidence radius was not entirely within the geofence; and (iii) add back certain devices for which there was a substantial probability that the user had engaged in criminal activity (because he or she had deleted her location data shortly after January 6). *Id.* To reiterate, Google calculates both a device location and as margin of error for that location. Although Google's location calculation alone could have established probable cause for a whole set of devices, the government further limited its second affidavit (and thus the only de-anonymized disclosure of data) to those devices for which not just the location but the entire confidence radius for at least one location data point fell within the geofence (approximately, the U.S. Capitol building) during the riot. 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.

This case therefore does not implicate overbreadth concerns. For example, 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. *Id.* at 918. 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 geofence 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 search 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.

3. The defendant argues that the geofence warrant was overbroad in several respects. His claims lack merit. At the outset, the defendant's overbreadth claim fails because the warrant was carefully limited based on location, dates, and times. The warrant sought only location information from Google regarding a four-and-one-half-hour interval for individuals present at the U.S. Capitol during the January 6 riot. Even if the warrant had requested identification of all responsive devices (which it did not), it would have been narrowly tailored for its investigatory

purpose, which was to identify the thousands of people who unlawfully entered the U.S. Capitol at a time when it was restricted to the public, as well as the people who witnessed those crimes. The significant additional limitations implemented at steps two and three of the geofence warrant further sharpened the warrant's narrow focus.

The defendant nonetheless contends (ECF No. 43 at 24) that the warrant was a "digital dragnet" because Google's own data management protocols make require its analysts to query a large body of data in order to comply with the geofence request. But the defendant cites no precedent for the proposition that a service provider may not review a large data set in order to produce a narrowly defined set of information. And no wonder: that proposition contravenes the foundational proposition that, aside from physical intrusions, a Fourth Amendment search occurs only "when government officers violate a person's 'reasonable expectation of privacy.'" *Jones*, 565 U.S. at 406 (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring)). Even assuming for sake of argument that Google users have a reasonable expectation of privacy in their Location History data vis-à-vis the world, they plainly have no such expectation vis-à-vis Google, which tracks, compiles, and uses the data. It therefore makes no sense to regard Google's mere act of querying (without disclosing) the users' Location History data as a "violat[ion of the user's] 'reasonable expectation of privacy'" in the data, just because the query is run in response to a warrant. *Jones*, 565 U.S. at 406. Any Fourth Amendment "search" must necessarily occur later in the process – at a minimum, no earlier than the point when the more limited data sought by the warrant is disclosed.[14]

[14] The defendant's reliance on *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), and *United States v. Griffith*, 867 F.3d 1265, 1272-1274 (D.C. Cir. 2017), for this point is unavailing for the reasons discussed in the text. In those cases, the officers' conduct violated the relevant individuals' legitimate expectations of privacy at the time of the officers' conduct; here, Google's initial querying of data across its Location History users – unaccompanied by any disclosure to the government of that data – did not violate the users' expectations of privacy.

Nor does the defendant's objection make sense in practice. Google's review of a large set of data to comply with the geofence warrant is a result of Google's internal data storage practices, not of an overbroad warrant. It would presumably be possible for Google to create an additional Location History database indexed by location. This database would enable Google to comply with a geofence warrant – and produce the exact same data as Google currently produces – without querying the data of all Location History users. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices, which are invisible to customers and the government alike. The appropriate measure for the breadth of the geofence warrant is the limited data *sought* by the warrant, which resulted in the government obtaining location information for many fewer individuals, all of whom were in or near the U.S. Capitol in the afternoon of January 6.

In a similar vein, the defendant asserts (ECF No. 43 at 25) that the geofence warrant's two "control" lists – comprised of anonymized devices that hit on the geofence before and after the riot – resulted in the Fourth Amendment search of data belonging people "suspected of no crime." But that contention, too, misapprehends the relevant Fourth Amendment moment. Again, a user's Fourth Amendment rights are not implicated (and there is no search) unless and until the user's privacy interests are invaded. *Jones*, 565 U.S. at 406. And that cannot logically happen unless and until the Location History data is de-anonymized. Until that point, the government has no private information about *that user*'s location history. And while the defendant insinuates that the lists "easily indicated the identities of the device IDs provided by google" (ECF No. 43 at 25), he provides no evidence to support that assertion, which is contradicted by the plain terms of the geofence warrant affidavit. Def. Ex. A at 25-26.[15]

[15] The defendant also appears to suggest (ECF No. 43 at 25) that the control lists captured Location History outside the geofence warrant. *Id.* (expressing privacy concern that "[t]his is a

The defendant also asserts (ECF No. 43 at 25) that the government "overstepped the bounds of the warrant itself by seizing data from *additional* searches that Google did of data it preserved at strategic times" – an apparent reference to the lists Google created based on the January 6 and January 7 data. He is incorrect. Google produced the January 6 and January 7 lists in response to the search warrant. Def. Ex. B. at 6. Indeed, those lists were responsive to the warrant. Def. Ex. A at 6-9.

Next, having chided the geofence warrant for using control lists, the defendant contends (ECF No. 43 at 26) that the de-anonymized list of devices in step three was overbroad because "[t]he government made no meaningful showing of probable cause in its follow up warrant affidavit." *Id.* But that assertion just ignores the geofence warrant's considerable minimization efforts, which, again, included the use of control lists as well conservative margin-of-error assumptions. Finally, the defendant quibbles (*id.*) that some users whose devices hit on the geofence but whose data was subsequently deleted *might* have had benign reason to delete the data. That, too, is unavailing. Probable cause requires a "fair probability" – not proof beyond a reasonable doubt – of involvement in criminal activity. The combination of a user's presence at or near the U.S. Capitol in the afternoon of January 6, absence from the U.S. Capitol during the control periods, and deletion of Location History data in the immediate aftermath of January 6 amply established such a fair probability for those users.

B. The Geofence Warrant Was Sufficiently Particular

The defendant next argues that the geofence warrant was insufficiently particular. His arguments are mistaken.

---

time when people can be expected to be at their home, hotel room, or otherwise enjoying personal time"). That, too, is incorrect. The whole point of the 9:00 p.m. control list was to exclude devices likely associated with individuals who *were at the Capitol* at that time – and who were therefore not rioters. Def. Ex. A at 25.

1. The Geofence Warrant Contained Particularized Descriptions of the Location to Be Searched at Google

The geofence warrant appropriately delineated the particular locations to be searched – *i.e.*, the Location History data and subscriber information for devices linked to the geographically bounded area corresponding to the U.S. Capitol Building in the afternoon of January 6. *See* Def. Ex. A at 4-5. These locations were as reasonably particularized as any other warrant for a physical space or a provider's records. The mere fact that they covered a relatively substantial geographic location – though just one building – 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.

The defendant contends (ECF No. 43 at 27) that the geofence warrant lacked particularity because it did "not specify the accounts to be searched and the data to be seized." But "[s]earch 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, 83 n.19 (D.D.C. 2021) (magistrate judge) (cataloguing cases).[16]

2. The Geofence 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." *Garrison*, 480 U.S. at 84.

The geofence warrant satisfied this requirement. The search described in the warrant was limited to records closely associated with a particular geographic location: the U.S. Capitol building. The 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 limited to the specific time period of the U.S. Capitol siege on January 6, minimizing the likelihood that tourists or bystanders would be found in any of this data. Def. Ex. A at 25. This was not a "wide-ranging exploratory search[]" of Google's records. *Garrison*, 480 U.S. at 84.

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*, 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*

[16] The defendant discusses "John Doe" warrants, "all persons" warrants, and anticipatory warrants (ECF No. 43 at 27-28). For the reasons stated in the text, none of those rubrics is relevant.

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 [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. *Verizon Wireless*, 2022 WL 2922193, at *7.

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[]." *Verizon Wireless*, 2022 WL 2922193, at *7. Importantly, the warrant directed Google to first provide a list of anonymized account identifiers representing the mobile devices estimated to have connected from within the U.S. Capitol building between 2:00 p.m. and 6:30 p.m. on January 6. Def. Ex. A at 26-28. The government then eliminated from the list devices that were also present within the building before (12:00 p.m. to 12:15pm) or after (9:00 p.m. to 9:15 p.m.) the mob siege – as those devices would not likely constitute evidence of a crime. Def. Ex. A at 27. Finally, after proposing additional narrowing criteria (and the inclusion of a relatively small number of devices linked to data deletion), the government sought (and obtained) a second warrant from the magistrate judge directing Google to provide identification information for the subset of responsive devices. Def. Ex. A at 28; Def. Ex. B at 6-9. This sequence, complete with repeated court involvement which assessed and found 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.'" *Verizon Wireless*, 2022 WL 2922193, at *8. This careful procedure readily distinguishes this case from instances in which courts have found the narrowing process inadequate.[17]

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. *Verizon Wireless*, 2022 WL 2922193, at *8. 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.*

In response, the defendant states (ECF No. 43 at 29) that "[t]he warrant left it up to Google and the government (largely the government) to decide which users would have their subscriber information handed over to the government." But that conclusory assertion disregards the warrant's plain terms. As already explained, the geofence warrant approved by the magistrate judge set forth a detailed process whereby devices were initially selected. *See* Def. Ex. A at 4-7. Furthermore, as the defendant acknowledges (in part) (ECF No. 43 at 30-31), the magistrate reviewed and approved the criteria subsequently used to narrow the devices for which subscriber information was seized. *See* Def. Ex. A at 6; Def. Ex. B at 7-8 (describing, in the affidavit supporting the application for the second warrant, the narrowing steps undertaken by the

---

[17] *See Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (magistrate judge) (finding that proposed geofence warrant lacked particularity where, unlike here, "the warrant put[] no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); *Matter of Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A*, No. 20 M 297, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020) (magistrate judge) (finding that proposed geofence warrant lacked particularity where, unlike here, it "contain[ed] [no] objective limits as to which cellular telephones agents could seek additional information").

government). The defendant now dismisses the narrowing procedure as "very simplistic" and "unlikely to remove innocent devices." ECF No. 43 at 31. But he never explains what alternative procedures might have been more effective. And he does not attempt to refute the fact that even "innocent devices" were likely to contain evidence documenting the crimes of others on January 6. *See Verizon Wireless*, 2022 WL 2922193, at *8.

The defendant also invokes "false positives" – the possibility that some devices, despite having a point estimate within the U.S. Capitol and despite passing the narrowing procedures described above, might nonetheless have been just outside the geofence. ECF No. 43 at 39. Elsewhere in his brief, however, the defendant takes a different view, asserting that Location History data "can … be as accurate as GPS." ECF No. 43 at 14. Regardless, the remote possibility that Google identified mobile devices immediately adjacent to the U.S. Capitol building is unavailing: access to these adjacent areas was also restricted. See Def. Ex. A at 14. A fair probability accordingly existed that persons immediately adjacent to the U.S. Capitol building had 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).[18]

Finally, the defendant takes issue (ECF No. 43 at 31) with some specific categories of information to be seized specified in Section II of the geofence warrant's Attachment B. *See* Def.

[18] The defendant also repeats (ECF No. 43 at 30) his assertion that "the government *exceeded* the bounds of the Search Warrant" when Google provided anonymized Location History data based on Google's data as of January 6 and 7. As already explained, those lists were within the scope of the geofence warrant. *See supra* p. 31; Def. Ex. A. at 6-7. Contrary to the defendant's suggestion (ECF No. 43 at 30), moreover, the magistrate did authorize the disclosure of subscriber data for devices that hit on the geofence and whose Location History data was later deleted. *See* Def. Ex. B at 7-8. Had the magistrate disagreed with the investigator's request to de-anonymize those devices, he would have declined to authorize disclosure of the subscriber data for those devices.

Ex. A at 8-9. But the defendant misapprehends the warrant's structure. Attachment A specified the information to be searched: the Location History data responsive to the geofence between 2:00 p.m. and 6:30 p.m. on January 6, 2021. Def. Ex. A at 4-5. Attachment B then authorized, in Section I, disclosure of particular items from the searched information, by describing the step two and step three device-selection process. Def. Ex. A at 6-7. And Section II described the information that the government was authorized to seize: all information described in Section I (*i.e.*, the disclosed Location History data) that constitutes evidence of various crimes committed at the U.S. Capitol on January 6. Def. Ex. A at 8. Section II then offered various explanatory illustrations of that evidence – as made clear by the phrase introducing those categories: "*including information pertaining to the following matters*." *Id.* Those subcategories by definition could not expand the warrant's scope, much less deprive it of the requisite particularity. By providing illustrations, the subcategories merely enhanced the warrant's particularity.

Contrary to the defendant's assertions, moreover, each of the illustrative subcategories cited by the defendant (ECF No. 43 at 31) did describe evidence of criminal activity. Indeed, they did so expressly: the subcategories impugned by the defendant expressly referred back to the "criminal activity under investigation." Def. Ex. A at 8-9. And while the defendant asserts that the affidavit did not support the existence of a conspiracy (one of the listed subcategories), conspiracy under 18 U.S.C. § 371 is among the crimes listed in both the affidavit and the warrant. Def. Ex. A at 8, 12. And the affidavit amply supports the fair inference that individuals in the mob acted in concert, agreement, and coordination. *See, e.g.*, Def. Ex. A at 15-16.

III. The Good-Faith Exception to the Exclusionary Rule Precludes Suppression

Even assuming that the geofence warrant somehow violated the defendant's Fourth Amendment rights, the good-faith exception to the exclusionary rule forecloses application of the exclusionary rule in this case.

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." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "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 v. United States*, 555 U.S. 135, 140 (2009). "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.

The traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), precludes suppression in this case. 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. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> [1] the magistrate or judge [who] issued [the] warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for reckless disregard for the truth[;] [2] the issuing magistrate wholly abandoned his judicial role[;] [3] [the] affidavit [was] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable[;] [or 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.

Leon, 468 U.S. at 923 (internal quotation marks and citation omitted).

None of these circumstances are present in this case. The defendant does not claim that the affiant misled the magistrate or that the magistrate abandoned his judicial role. Nor can the defendant show that the affidavit was so lacking in indicia of probable cause that reliance on it was unreasonable, or that the warrant so failed to particularize the place to be searched or the things to

be seized that no reasonable officer could have presumed it to be valid. "[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 rise to that level. As in *Messerschmidt*, it would "not have been unreasonable – based on the facts set out in [the Google] 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 geofence warrant – for the executing officer to believe that the geofence warrant complied with the Fourth Amendment's particularity requirement. A contrary finding would be especially striking after Chief Judge Howell recently cited similar features in finding that a similar tower dump warrant was sufficiently particularized. *See Verizon Wireless*, 2022 WL 2922193, at *7-8.

As the Fourth Circuit recognized in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), moreover, suppression is often inappropriate when the investigating officer confronted a novel investigative technique, consulted with counsel, and then sought a warrant:

> [I]n light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

Id. at 691. Consistent with *McLamb*, the district court in *Chatrie*, despite finding the geofence warrant at issue in that case defective, concluded that the *Leon* good-faith exception applied and precluded suppression. *Chatrie*, 590 F. Supp. 3d at 938 (finding that the exclusion of evidence obtained through a geofence "likely would not 'meaningfully deter' improper law enforcement conduct" where the investigator had consulted with counsel and obtained a warrant).

Here, the investigators followed the approach endorsed by *McLamb*. They worked closely with the United States Attorney's Office in applying for the geofence warrant. They then sought and obtained a search warrant from a magistrate of this Court. The investigators thus did precisely what *McLamb* expects, and the good-faith exception should preclude suppression here. Because the officers who executed the Google geofence warrant worked conscientiously and reasonably relied on the magistrate judge's approvals, they engaged in "nonculpable, innocent police conduct." *Davis*, 564 U.S. at 240. Suppression is unwarranted in all respects.

IV. Suppression of Evidence Obtained Pursuant to the November 2021 Warrant to Search the Defendant and His Electronic Devices Would Not Be Appropriate Even If the Geofence Warrant Were Invalid

Even assuming the geofence warrant were defective, the defendant errs in arguing (ECF No. 43 at 32-36) that the "evidence obtained by the search warrant for [the defendant's] home, property, and phone … must be suppressed." Even without the information obtained from the geofence warrant, the affidavit supporting the warrant to search the defendant and his devices (Def. Ex. M at 3-23, hereinafter "November 2021 Affidavit") established probable cause that evidence of the three listed offenses (*id.* at 1) would be found on the defendant's person and devices. *See United States v. Karo*, 468 U.S. 705, 719 (1984) (where information from an earlier unconstitutional search was included in a warrant affidavit, "the warrant was nevertheless valid" because "sufficient untainted evidence was presented in the warrant affidavit").

As explained above, the November 2021 Affidavit described, in addition to the results of

the geofence warrant, a constellation of evidence supporting probable cause. *First*, it described information reported by two separate tipsters who had learned that the defendant had entered the Capitol building during the riot on January 6. Def. Ex. M at 12. The first tipster also reported that, when confronted, the defendant did not deny entering the Capitol building and claimed that the Capitol police moved the barriers to let him into the building. Def. Ex. M. at 12. *Second*, the affidavit stated that, according to Verizon records, the defendant's cell phone had connected, during the riot, to a cell site whose service area included the U.S. Capitol building's interior. Def. Ex. M. at 12-13. *Third*, the affidavit reported that, in March 2021, investigators interviewed the first tipster. Def. Ex. M at 13. The tipster explained that, though he had not personally seen the Facebook post in which the defendant's wife referred to the defendant entering the Capitol on January 6, he had seen a screenshot of the post, which a friend had sent to him. *Id.* The tipster also stated that he believed the defendant's wife had deleted the Facebook post shortly after posting it. *Id.* And the affidavit included a screenshot of text messages that the tipster exchanged with the defendant and his wife after learning of the defendant's participation in the riot. *Id.* In the exchange, the defendant did not deny entering the Capitol; in fact, he implied the opposite, stating that he saw no violence, and that Capitol police removed barriers and let people in. Def. Ex. M. at 14 (Aff. ¶ 42). *Fourth*, the affidavit reported that, in September 2021, the tipster identified the defendant in a still photograph obtained from the Capitol Police closed-circuit surveillance system:

Def. Ex. M at 15. *Fifth*, the affidavit explained that investigators placed the same individual depicted in the photograph above at various locations inside the U.S. Capitol Building during the January 6 riot. Def. Ex. M. at 15-23. The affidavit included 10 supporting screenshots, complete with descriptions of the events depicted in the photographs. *See* Def. Ex. M at 16-23. Finally, the affidavit reported that, according to a Capitol Police officer who arrested the defendant inside the Capitol, the defendant was found in possession of two knives and pepper spray, which were seized. Ex. M, at 19. Even without the geofence evidence, the affidavit contained ample evidence of probable cause.

In response, the defendant downplays those various pieces of evidence, but his claims are insubstantial. For example, the defendant attempts to discredit the first tipster (ECF No. 43 at 33-34), asserting that he did not have "even meaningful *second-hand* information." *Id.* at 33. In fact, the affidavit stated that (i) the tipster had seen a screenshot of the defendant's wife's January 6 Facebook post referring to the defendant entering the U.S. Capitol; and (ii) the tipster provided a screenshot of a text exchange in which the defendant implied that he entered the U.S. Capitol building on January 6. Def. Ex. M at 13-14. Furthermore, while the defendant claims

contradiction between the tipster's initial tip and his statements in the March 2021 interview, the two statements are, in fact, consistent. *Compare* Def. Ex. M. at 12, *with* Def. Ex. M at 13-14. Finally, the defendant downplays the Verizon evidence as a "vague piece of evidence that does little more than place Mr. Rhine in the general vicinity of the Capitol Building." ECF No. 43 at 34. That, too, is wrong: the defendant's location in close proximity of the Capitol Building during the riot was itself compelling evidence that he was, at a minimum, within the Capitol's restricted Capitol area on January 6, 2021. It therefore established probable cause that he violated 18 U.S.C. § 1752(a)(1).

Finally, the defendant speculates (ECF No. 43 at 34) that, without the geofence evidence, the investigators would not have located the defendant in the Capitol Police's closed-circuit footage, which in turn led to the tipster's identification in September 2021. But the defendant has the burden of "showing … a causal nexus between the Fourth Amendment violation and the evidence he seeks to suppress," *e.g.*, *United States v. Holmes*, 505 F.3d 1288, 1292 (D.C. Cir. 2007) – a burden he cannot carry by offering only rank speculation. And while the defendant speculates that the geofence data was the decisive factor in overcoming the investigators' early difficulties in locating the defendant in the security footage (ECF No. 43 at 34), the investigative materials refute that theory. The investigators' initial unsuccessful efforts spanned the period between June 1 and 21, 2001, which was months *after* the investigators received, in March 2021, the geofence results for the defendant. *See* Gov't Ex. 1. It was only after the primary investigator on the case received additional training on the FBI's video system – training that focused on other tools – that he was able to locate the defendant in the Capitol Police footage in the following weeks. Def. Ex. O; *see also* Def. Ex. P.

CONCLUSION

For these reasons, the defendant's motion to suppress should be denied.

Dated: November 30, 2022

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

By: */s/ Francesco Valentini*
FRANCESCO VALENTINI
D.C. Bar No. 986769
Trial Attorney
United States Department of Justice, Criminal Division
Detailed to the D.C. United States Attorney's Office
601 D Street NW
Washington, D.C. 20530
(202) 598-2337
francesco.valentini@usdoj.gov