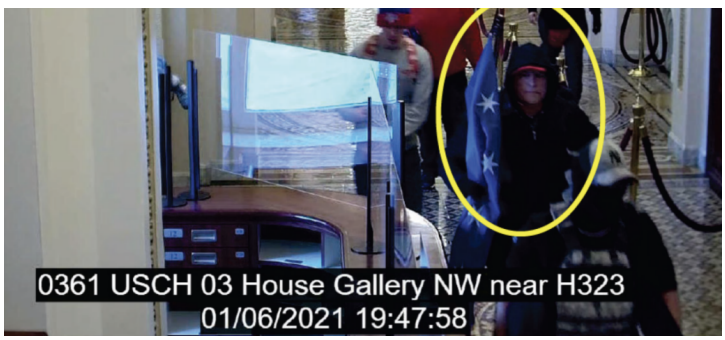
1,500 INVESTIGATIVE SUBJECTS: A COMPETENT GOOGLE GEOFENCE MOTION TO SUPPRESS FOR JANUARY 6

For some time, I've been waiting for a January 6 defendant to (competently) challenge the use of a Google GeoFence as one means to identify them as a participant in January 6. (There have been incompetent efforts from John Pierce, and Matthew Bledsoe unsuccessfully challenged the GeoFence of people who livestreamed on Facebook.)

The motion to suppress from David Rhine may be that challenge. Rhine was charged only with trespassing (though he was reportedly stopped, searched, and found to be carrying two knives and pepper spray, but ultimately released).

As described in his arrest affidavit, Rhine was first identified via two relatively weak tips and a Verizon warrant. But somewhere along the way, the FBI used the general GeoFence warrant they obtained on everyone in the Capitol that day. Probably using that (which shows where people went inside the Capitol), the FBI found him on a bunch of surveillance video, with his face partly obscured with a hat and hoodie.



The motion to suppress, written by Tacoma Federal Public Defender Rebecca Fish, attempts

to build off a ruling in the case of Okello Chatrie (and integrates materials from his case) to get the GeoFence used to identify Rhine and everything that stemmed from it thrown out.

The three-step GeoFence Warrant and the returns specific to Rhine are sealed in the docket.

EXH. #	DESCRIPTION
A	*SEALED* Geofence Warrant - Step 1; Filed: 01/13/21
B	*SEALED* Geofence Warrant and Application – Step 2 and 3; Filed 01/18/21
C	Google Amicus Curiae Re: Geofence General Warrant *United States v. Chatrie*, 3:19-cr-00130-MHL, dkt. 73; Filed 12/23/19
D	Marlo McGriff Declaration – Google Location History Product Manager *United States v. Chatrie*, 3:19-cr-00130-MHL, dkt. 96-1; Filed 03/11/20
E	*Chatrie* Suppression Hearing Transcripts, March 4-5, 2021, *United States v. Chatrie*, 3:19-cr-00130-MHL, dkt. 201-202; Filed 03/29/21
F	Google disclaimer regarding privacy of a deceased user's account
G	*SEALED* Geofence Warrant Return Location History as to Mr. Rhine
H	*SEALED* Geofence Warrant Return Map as to Mr. Rhine
I	Google, Android and Location Tracking History Summaries
J	Norwegian Consumer Council Report on Google Location Tracking, "Every Step You Take-How deceptive design lets Google track users 24/7"
K	"Unique in the Crowd: The privacy bounds of human mobility," Scientific Reports, Published March 25, 2013.
L	*SEALED* Geofence Follow-Up Warrant Application for Further Subscriber Information; Filed 03/26/21
M	*SEALED* Rhine Search Warrant Application; Filed 11/05/21
N	*SEALED* Rhine Issued Search Warrant; Issued 11/05/21
O	*SEALED* Review of Triage Toolkit Videos Report; Dated 06/23/21
P	*SEALED* Review of Videos Report; Dated 07/27/21
Q	*SEALED* Warrant Return for Rhine Warrant; Executed: 11/09/21

But the MTS provides a bunch of the details of how the FBI used a series of warrants to GeoFence the crime scene.

First, as Step 1, it got a list of devices at the Capitol during the breach, either as recorded in current records, or as recorded just after the attack. At this stage, FBI got just identifiers used for this purpose, not subscriber numbers.

> The geofence warrant requested and authorized here collected an alarming breadth of personal data. In Step 1, the warrant directed Google to use its location data to "identify those devices that it calculated were or could have been (based on the associated margin of

> error for the estimated latitude/longitude point) within the TARGET LOCATION" during a four-and-a-half hour period, from 2:00 p.m. until 6:30 p.m. Ex. A at 6. The target location—the geofence—included the Capitol Building and the area immediately surrounding it, id. at 5, which covers approximately 4 acres of land, id. at 13. Indeed, the warrant acknowledges that "[t]o identify this data, Google runs a computation against all stored Location History coordinates for all Google account holders to determine which records match the parameters specified by the warrant." Ex. A at 26 (emphasis added). Though not spelled out with clarity in the warrant itself, the warrant ordered that the list provided in step 1 not include subscriber information, but that such information may be ordered at a later step. See id. at 6; see also id. at 25 ("This process will initially collect a limited data set that includes only anonymous account identifiers, dates, times, and locations.").

This yielded 5,723 unique devices (note, the MTS points to Google filings from the Chatrie case to argue that only a third of Google's users turn on this location service).

> Google ultimately identified 5,653 unique Device IDs that "were or could have been" within the geofence, responsive to the first step of the warrant. Ex. B (step 2 warrant and application) at 6. However, Google ***additionally*** searched location history data that Google preserved the evening of January 6. When searching this data, as opposed to the current data for active users at the time of the search, Google produced a list of 5,716 devices that were or could have been within the

> geofence during the relevant time period. Id. Google ***additionally*** searched location history data that Google preserved on January 7. When searching this data, Google produced a list of 5,721 devices that were or could have been within the geofence during the relevant time period. Id. The three lists combined yielded a total of 5,723 unique devices that Google estimated were or could have been in the geofence during the four-and-a-half hour period requested. Id. at 7.

In Step 2, the FBI asked Google to identify devices that had been present at the Capitol before or after the attack – an attempt to find those who were there legally. That weeded the list of potentially suspect devices to 5,518.

> In this case, the second step of the geofence warrant was also done in bulk, given the lack of specificity as to the people sought. In the initial warrant, the Court ordered Google to make additional lists to eliminate some people who were presumptively within the geofence and committed no crimes. First, the warrant ordered Google to make a list of devices within the geofence from 12:00 p.m. to 12:15 p.m. on January 6. And second, the warrant ordered Google to make a list of devices within the geofence from 9:00 p.m. to 9:15 p.m. Ex. A at 6.
>
> [snip]
>
> Google provided these lists to the government in addition to the lists detailed above. Google identified 176 devices that were or could have been within the geofence between 12:00 p.m. and 12:15 p.m., and 159 devices that were or could have been within the geofence between 9:00 p.m. and 9:15 p.m. Ex. B at 6. The government ultimately

> subtracted these devices from those that they deemed suspect. Id. at 7. However, this still left 5,518 unique devices under the government's suspicion. See id. The original warrant contemplated the removal of devices that were present at the window before and after the primary geofence time because the government asserted that the early and late windows were times when no suspects were in the Capitol Building, but legislators and staff were lawfully present. Ex. A at 27. However, the original warrant also indicated that "The government [would] review these lists in order to identify information, if any, that is not evidence of crime (for example, information pertaining to devices moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case)." Ex. A at 6.
>
> Aside from comparing the primary list with the lists for the early and late windows, the government appeared to do no culling of the device list based on movement. Rather, the government used other criteria to decide which devices to target for a request for subscriber information. 3.

The government then asked for the subscriber information of anyone who showed up at least once inside the Capitol (as the MTS notes, Google's confidence levels on this identification is 68%). That identified 1,498 devices.

> In step 3, as relevant to this case,4 the government sought subscriber information—meaning the phone number, google account, or other identifying information associated with the device—for two different categories of people. First, the government sought subscriber information for any device

> for which there was a single data point that had a display ratio entirely within the geofence. Ex. B at 7. In other words, the government sought identifying information for any device for which Google was 68 percent confident the device was somewhere within the geofence at a single moment during the four-and-a-half hour geofence period. Again, the government equated presence to criminality. The government sought and the warrant ordered Google to provide identifying information on 1,498 devices (and likely people) based on this theory. See id.

It also asked for subscriber information from anyone who had *deleted* location history in the week after the attack, which yielded another 37 devices.

> Second, the government sought identifying subscriber information for any device where location history appeared to have been deleted between January 6 or 7 and January 13, and had at least one data point where even part of the display radius was within the geofence. See Ex. B at 7–8. The government agent asserted that such devices likely had evidence of criminality because: "Based on my knowledge, training, and experience, I know that criminals will delete their Google accounts and/or their Google location data after they commit criminal acts to protect themselves from law enforcement." Id. at 8.
>
> [snip]
>
> The theory that potentially changed privacy settings or a deleted account as indicative of criminality led the government to request identifying information for 37 additional devices (and likely people). Ex. B at 8.

The MTS notes that at a later time, the FBI expanded the scope of the GeoFence for which they were seeking subscriber information, but that's not applicable to Rhine.

> 4 Discovery indicates that the government later sought substantially more data from geofences in areas next to, but wholly outside of, the Capitol Building. However, Mr. Rhine addresses here the warrants and searches most relevant to his case.

The GeoFence was one of a number of things used to get the warrant to search Rhine's house and digital devices.

I'll hold off on assessing the legal merit of this MTS (though I do plan to share it with a bunch of Fourth Amendment lawyers).

For now, what is the best summary I know of how the known Google GeoFence reveals how the FBI used it: first obtaining non-subscriber identifiers for everyone in the Capitol, removing those who were by logic legally present before the attack, and then obtaining subscriber information that was used for further investigation.

And that GeoFence yielded 1,500 potential investigative subjects, which may be only be a third of Google users present (though would also by definition include a lot of people — victims and first responders — who were legally present). Which would suggest 4,500 people were inside the Google GeoFence that day, and (using the larger numbers) 15,000 were in the vicinity.

As I keep saying, the legal application here is very different in the Chatrie case, because everyone inside the Capitol was generally trespassing, a victim, a journalist, or a first responder.

To make things more interesting, Rudolph Contreras, who is the FISA Court presiding judge, is the judge in this case. He undoubtedly

knows of similar legal challenges that are not public from his time on FISC.

Which may make this legal challenge of potentially significant import.