MORE ON THE GOVERNMENT'S JANUARY 6 GOOGLE GEOFENCE

In October, I wrote a piece on a reasonably framed challenge to the Google GeoFence used to investigate January 6, in the trespassing case of David Rhine. In recent days, Wired picked up my story, but didn't situate the GeoFence in the context of prior rulings overturning their use, including the EDVA ruling in March on which this challenge most directly relies. Nor did it show how this information worked with other evidence against Rhine (including two tips), that led to his arrest. That led to a lot of alarmism that, if the January 6 GeoFence is upheld, it'll set some kind of precedent.

Yesterday, the government submitted its response to the challenge, which better explains how the GeoFence was used and why it is highly unlikely the conditions present with this GeoFence will be replicated in the future. That description is here.

As described this was a three step process:

- Provide an anonymized list of the phones using Google Location Services that were present in the Capitol between 2 and 6:30PM on January 6 (whether in Google records preserved on the evening of January 6, the morning of January 7, or still on January 13). In addition, provide anonymized lists of phones using Google Location Services present in

the Capitol between 12:00 and 12:15 and/or 9:00 and 9:15 PM on January 6.

- Eliminate devices believed to be legally present in the Capitol (because they were in the earlier and/or later lists, so there before and/or after the riot), and identify those that evinced likely criminal behavior, either because the location data showed at least one hit entirely within the margin of error, or because there device showed presence in the Capitol (but not entirely within the margin of error) but also showed evidence of account deletion.

> 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.

- For the resulting ~1,500 devices, DOJ obtained a second warrant for Google to obtain the account identifier.

As the government explains this Google GeoFence differs from ones that have been overturned in several ways. Most importantly, in addition to the claim that the use of Location Services is voluntary (as distinct from location services associated with using cell phones), which was rejected in other GeoFences, here, the government *also* argues that, even on a normal day, anyone entering the Capitol would have no reasonable expectation of privacy, but all the more so here, where it was closed to the public.

So whereas the government argued that with Google and Facebook, users had no Reasonable Expectation of Privacy regarding information voluntarily shared with the tech company, they appear to have pursued individualized warrants with cell companies because sharing that information (under Carpenter) does involve REP. For all three, though, I *think* the government would argue there was no REP for people who entered the Capitol without authorization.

Service	REP entering Capitol	REP for location data	Warrant
Google	No	No	GeoFence
Facebook (livestream)	No	No	GeoFence
Cell	No	Yes	Individualized

The government is also relying on the short timespan — 4.5 hours — to justify its GeoFence.

Relatedly, in contrast to other GeoFences that encompassed public spaces and in some cases, private residences, here, most people captured by the Google GeoFence would be people who

committed a crime by being in the Capitol, or who were witnesses, victims, or first responders.

> 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.

In the past, I've noted that the others captured by the GeoFence would be victims (employees of Congress, whether Members, staff, or service staff) or First Responders. The most serious privacy exposure here might be journalists, particularly those carrying burner phones or similar.

I asked Igor Bobic, as a test of whether a credentialed journalist would be included in those deemed legally present(recall that Bobic took the iconic footage of Doug Jensen chasing Officer Eugene Goodman up the steps). He told me he was inside the Capitol for both the control periods, at noon and at 9PM. That makes sense: those present to report on the vote certification would have had cause to show up

before it started and to stay — often until the wee hours of the morning — to witness its completion.

In other words, journalists who were covering events outside, but followed rioters in (and there were substantial teams from multiple media outlets as well as a number of documentary teams), would be those whose privacy was most affected.

I said in my last post that this is a well-argued motion to suppress. But the government's response explains why Rhine is not the best situated defendant to bring this challenge. Generally, the FBI has used this GeoFence in three ways: To confirm already identified defendants were present in the Capitol or entered the Capitol, to help identify a suspect in surveillance footage, or (more recently) as leads sent out to the field to run down.

As I suspected, Rhine is in the second category: DOJ opened the investigation and advanced it based off several tips and even had confirmed Rhine's presence via a particularized warrant to Verizon. Only later did it use the GeoFence to identify where in the existing surveillance footage to look for images of Rhine (who obscured his face with a mask).

> 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.
>
> [snip]
>
> [T]he 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.

There are other arrest affidavits that, at least as described, *start* with the identification in the Google GeoFence (here's one example). Some even suggest that leads based off GeoFence hits were sent to field offices to chase down. While there are no arrests based entirely on the GeoFence, defendants arrested after an investigation that started from a GeoFence lead would seem to be better situated to challenge the GeoFence.

In any case, the unique conditions at the Capitol on January 6, based on the fact that any unauthorized person who entered the Capitol was likely breaking the law, are unlikely to be replicated anytime in the future.

So whether or not this is sustained (and the warrants based on it would be sustained on good faith grounds), it’s unlikely to be a precedent for other GeoFences.