Manohar Raju
Public Defender
San Francisco Public Defenders Office
Matt Gonzalez
Chief Attorney
Sierra Villaran, SBN 306949
Deputy Public Defender
555 Seventh Street
San Francisco, CA 94103
(415) 575-88199, Sierra.Villaran@sfgov.org

Michael Price (*pro hac vice*)
Litigation Director, Fourth Amendment Center
National Association of Criminal Defense Lawyers
1660 L Street, NW, 12th Floor
Washington, DC 20036
(202) 465-7615, mprice@nacdl.org

Attorneys for LaQuan Dawes

Superior Court of the State of California
County of San Francisco

People of the State of California,

Plaintiff,

vs.

LaQuan Dawes,

Defendant.

Court No: 19002022

Post-Hearing Brief in Support of Defendant's Motion to Quash and Suppress Evidence

Date: July 15, 2022
Time: 9:00 AM
Dept: 23

LaQuan Dawes, through counsel, submits this post-hearing brief in support of his motion to quash and suppress a "geofence" warrant issued on December 4, 2018. *See* Mot. to Quash and Suppress Evidence under Penal Code 1538.5 and 1546 ("Mot. to Quash") at 1 (filed June 9, 2020).

The Electronic Frontier Foundation ("EFF"), a civil liberties organization that works to protect free speech and privacy in the digital world, filed an amicus brief in support of Mr. Dawes on June 10, 2020. *See* Def. Exhibit A, Brief of Amicus Curiae Electronic Frontier Foundation in Support of Def. Mot. to Quash and Suppress Evidence ("EFF Amicus"). EFF agreed with Mr. Dawes that the warrant was an unconstitutional general warrant in violation of the Fourth Amendment to the

United States Constitution as well as Article I, Section 13 of the California Constitution, and the California Electronic Communications Privacy Act ("CalECPA"), Cal. Penal Code § 1546, *et seq*.

The government filed its response on September 8, 2021. *See* People's Opp. to Def. Mot. to Quash and Suppress Evidence at 1. Mr. Dawes filed an initial reply brief on September 13, 2021, focused on whether he had a reasonable expectation of privacy in his Google Location History data. *See* Reply to People's Opp. to Def. Mot. to Quash & Suppress Evidence at 1 ("Reply"). Mr. Dawes included an expert report from Mr. Spencer McInvaille of Envista Forensics, dated September 10, 2021, establishing that Location History was enabled automatically during the initial setup of Mr. Dawes's phone without his consent. *See* Reply, Def. Exhibit B ("McInvaille 9/10/21 Report") at 6. Following a hearing on October 4, 2021, this Court determined that that Mr. Dawes did have an expectation of privacy in his Location History data under CalECPA. The Court held that Location History is protected location information under Penal Code sections 1546.1—specifically 1546.1(a)(1), (a)(2), and (g).

On October 18, 2021, Mr. Dawes filed a supplemental reply brief addressing the warrant's lack of probable cause and particularity in violation of CalECPA, the California Constitution, and the Fourth Amendment to the United States Constitution. *See* Supplemental Reply to People's Opp. to Def. Mot. to Quash and Suppress Evidence ("Supplemental Reply") at 1. Mr. Dawes also included a supplemental report from Mr. McInvaille showing that the method of executing the warrant was (1) prone to reporting "false positives" and (2) increased the effective range of the geofence to include "portions of 30 homes and 16 other fenced areas behind homes, the street and sidewalk." *See* Supplemental Reply, Def. Exhibit A ("McInvaille 10/18/21 Report") at 6.

The Court held a hearing on May 26, 2022, and received testimony from Sgt. Jesse Farrell of the San Francisco Police Department ("SFPD") as well as defense expert Spencer McInvaille of Envista Forensics. *See* Def. Exhibit B, 5/26/2022 Hearing Transcript ("5/26/2022 Hearing Tr."). Mr. Dawes introduced a second supplemental report from Mr. McInvaille (his third in this case), dated May 12, 2022, attesting that the true scope of a geofence search has no bearing on the shape or size of the geofence drawn in the warrant. *See* Supplemental Exhibits for Def. Mot. to Quash and Suppress Evidence, Def. Exhibit B ("McInvaille 5/12/22 Report"); 5/26/2022 Hearing Tr. at

17:21–18:5; Exhibit F at 4. Following the hearing, the Court ordered the parties submit post-hearing briefing in lieu of oral argument.

Finally, Mr. Dawes issued two subpoenas to Google during the course of this litigation. The first, dated November 10, 2020, sought information about how Google conducts and processes geofence warrants. The second, dated December 22, 2020, sought information about when and how Location History became enabled on Mr. Dawes's Google account. Google moved to quash both subpoenas, and after much discussion, Google produced a written declaration from Google Policy Specialist Emily Moseley showing that Google searched approximately 592 million people to execute the geofence warrant here. *See* Supplemental Exhibits for Def. Mot. to Quash and Suppress Evidence, Def. Exhibit A ("Declaration of Emily Moseley") at 2. Additionally, the government agreed to stipulate to certain evidence and testimony concerning the operation of geofence warrants, as provided in another case, *United States v. Chatrie*, No. 3:19-CR-130, 2022 WL 628905, at *3–4 (E.D. Va. Mar. 3, 2022) (finding a geofence warrant unconstitutional). This material was lodged in the docket at the May 26, 2021 hearing.

Introduction

As this Court has already ruled, Mr. Dawes had an expectation of privacy in his Location History data. Likewise, so did the other 592 million people that the SFPD searched with the geofence warrant in this case. It was an incomprehensively broad warrant, unsupportable by probable cause, and so lacking in particularity that it can only be described as a digital version of the reviled general warrants of old. The law has been clear for centuries: probable cause must be particularized, and there is no such thing as relying on a general warrant in good faith. Mr. McInvaille's third report and live testimony on May 26 reinforced the impossibility of a reasonable geofence warrant. And Sgt. Farrell's testimony revealed that even the SFPD no longer submits warrants like the one in this case, following concerns expressed by Judge Michael Begert and consultation with the City Attorney of San Francisco. *See* 5/26/22 Tr. at 49:8–51:22. Any reasonable officer knows that a valid warrant cannot authorize the search of every home in a neighborhood, city, or state. A digital dragnet is no different, and it should have been apparent that this geofence search was likewise unconstitutional. As a result, Mr. Dawes asks this Court to suppress the evidence obtained from the geofence warrant as well as all of its fruits.

Argument

1. The Geofence Warrant Was Overbroad

Mr. Dawes renews his argument that the geofence warrant violated both CalECPA and the Fourth Amendment for lack of probable cause. This issue has been briefed extensively, *see* Supplemental Reply at 2–16; Mot. to Quash at 10-21, so Mr. Dawes focuses here on facts elicited during the May 26 hearing and Mr. McInvaille's third report. *See* 5/26/22 Tr., Def. Exhibit B; McInvaille 5/12/22 Report. The Court and the government both accepted Mr. McInvaille as an expert in mobile device forensics, digital forensics, and location analysis, and his third report was introduced without objection. *See* 5/26/22 Tr. at 7:4–18, 18:17–19:4.

According to Mr. McInvaille's testimony and report, the size of the geofence does affect the scope of the initial search. 5/26/22 Tr. at 18:8–12, 20:10–27; McInvaille 5/12/22 Report at 3–4. The geofence could have been the size of a parking space or a mile wide, but the shape would not have changed the fact that Google had to search everyone with Location History enabled to execute the warrant. As the Court put it, "no matter how big or small, it's the same number that gets searched." 5/26/22 Tr. at 21:24–27. Critically, Google estimates that number was 592 million in 2018. *See* Declaration of Emily Moseley at 2; 5/26/22 Tr. at 20:6–8; McInvaille 5/12/22 Report at 2. The government did not object to or question this figure in any way. *See* 5/26/22 Tr. at 17:3. Thus, to conduct the geofence warrant in this case, Google did indeed search at least 592 million Google user accounts. *See* 5/26/22 Tr. at 20:6–8; McInvaille 5/12/22 Report at 3–4.

On the opposite side of the scale, there were no facts to support a search of this scope. Indeed, there were no specific facts showing that any of the suspects on video had cell phones with them, let alone had Google devices with Location History enabled. *See* 5/26/22 Tr. at 57:23–58:11; Mot. to Quash & Suppress Evidence, Exhibit B at 10 ("Warrant & Affidavit"); *see also* Supplemental Reply at 5-6. Instead, Sgt. Farrell relied solely on a series of assumptions that could apply in any case. 5/26/22 Tr. at 58:6–11 (agreeing that "essentially [his] logic was that suspects are people and people tend to have cells phones"). It is well-established that assumptions are no substitute for individualized probable cause. *See People v. Pressey*, 102 Cal. App. 4th 1178, 1190 (Ct. App. 2002) ("broad generalizations do not alone establish probable cause."); *People v. Garcia*, 111 Cal. App. 4th 715, 721 (Ct. App. 2003) ("[A]n affidavit based on mere suspicion or belief, or stating a

conclusion with no supporting facts, is wholly insufficient."); *Fenwick & West v. Superior Ct.*, 43 Cal. App. 4th 1272, 1279–80 (Ct. App. 1996) (finding that a misguided "assumption" was insufficient to support an "inference of probable cause"). But even if taken at face value, these assumptions do not yield a "fair probability" of identifying evidence among these 592 million accounts. *See* 5/26/22 Tr. at 31:17–23. In fact, they show only a 12.5% probability that a random American would have a device with Location History enabled.[1] *Id.* This is hardly a "fair probability" under the Fourth Amendment. *See Pressey*, 102 Cal. App. 4th at 1182; *Garcia*, 111 Cal. App. 4th at 720; *Fenwick & West*, 43 Cal. App. 4th at 1182.

Finally, it is important to emphasize that a Google geofence search does not function like a so-called "tower dump." 5/26/22 Tr. at 37:4–38:15. A tower dump compels a cell phone service provider to identify everyone who connected to a given tower during a specified time period. A tower dump is still an extremely broad search that can affect hundreds or thousands of people, but unlike in a geofence warrant, the service provider still does not have to search all of its users to produce this information. *Id.* at 39:18–21. That is because they store this information in a way that is searchable by tower, each of which has a known geographic location. Cell phone providers keep this information for service and maintenance purposes. *Id.* at 39:8–11. But Google, by contrast, attributes Location History data to individual accounts and has no cell phone towers to service or maintain. As a result, the nature of the search is fundamentally different. A tower dump searches thousands of people in one area; a geofence searches everyone to figure out who was in an area. That difference is consequential because it renders the shape of the geofence irrelevant. Even if someone were out-of-state when the crime occurred, a geofence searches them whereas a tower dump would not. *Id.* at 37:25–38:15.

[1] Indeed, many geofence warrants do not yield fruitful investigative results. *See, e.g., Scene of a Crime? Raleigh Police Searched Google Accounts as Part of Downtown Fire Probe*, WRAL (Feb. 14, 2018), https://perma.cc/XKP2-YNHQ; Jacob Ryan, *To Solve Murders, Louisville Police Turn To 'Geofence' Warrants – But Net Few Arrests*, WFPL (Oct. 19, 2021), https://perma.cc/KS6G-92WQ; *see also* Zach Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of all US Demands*, TechCrunch (Aug. 19, 2021), https://perma.cc/VV4Z-TBPR.

2. The Geofence Warrant Lacked Particularity

The warrant also failed to limit investigators' discretion regarding what to search and seize. At each step, it left critical questions up to the government and Google to hash out, rather than a judge. As a result, it was unconstitutional under the Fourth Amendment and unlawful under CalECPA.

At "step one," the warrant failed to indicate the type of location data to search (Location History, as opposed to "Google Location Accuracy" or "Web & App Activity"), 5/26/22 Tr. at 11:16–17, 13:25–14:27, omitting that only a third of Google accounts have Location History enabled. *Id.* at 17:14–15. The warrant also failed to specify how to count which devices were inside the geofence. *Id.* at 28:2–7. Instead, Google returned data on every device with a center point inside the geofence, regardless of whether the "display radius" extended outside the geofence. *Id.* at 28:6. Counting this way, however, increases the likelihood of "false positives," *i.e.* the possibility that a device was within its display radius but actually located outside the geofence. *Id.* at 27:17–19. It also increases the effective search area. *See* McInvaille 10/18/21 Report at 6. Indeed, the largest display radius was seven times larger than the geofence, covering approximately 30 homes instead of six. *Id.* at 25. Finally, the warrant did not adequately specify the time period for the step one search. One appendix authorized a 30–minute search (1630 hours through 1700 hours) while the other authorized a two-hour search (1630 hours through 1830 hours). *Id.* at 26. Despite this discrepancy, the government obtained data for the full two hours. *Id.*

At "step two" and "step three," the warrant explicitly granted the government discretion to decide which accounts to search further and which accounts to unmask. *Id.* at 28–29. After receiving information about nine devices in step one, the warrant left it up to investigators to decide which accounts were relevant, with the government identifying six for an expanded search in this instance. *Id.* Likewise, after reviewing this additional Location History data, the warrant left it to investigators to decide which accounts would be unmasked and have their subscriber information disclosed by Google. *Id.* at 29. Here, the government selected one account to be unmasked. *Id.* Even the government, however, now recognizes that placing such discretion in the hands of investigators was impermissible. As Sgt. Farrell recounted, the SFPD has changed the way it drafts geofence warrants in response to concerns expressed by Judge Begert, who believed it was necessary to write a second warrant to unmask an account. *Id.* at 50. And following consultation

with the City Attorney of San Francisco, the SFPD created a new warrant that no longer gives officers the discretion over who to unmask, requiring a second warrant instead. *Id.* at 51–52; *see also id.* at 49 ("We now have more steps as far as the initial warrants. We used to ask for all the information in one warrant and then just go back to Google for the information to unmask the tag ID and just ask them for it. Now we have to write a second warrant for that information.").

On all fronts, the geofence warrant was woefully unparticularized under the Fourth Amendment. It also failed to meet the heightened particularity requirements of CalECPA with respect to (1) the "time periods covered" by the warrant; (2) the "target individuals or accounts"; (3) the "applications or services covered"; *and* (4) and the "types of information sought." *See* Pen. Code §1546.1(d)(1). It gave conflicting time periods to search; it did not identify a single individual or account to search; it did not state the type of Google location data to search; and it did not indicate how to identify responsive information.

3. The Good Faith Exception Does Not Apply

There is no good faith exception to the exclusionary rule under CalECPA. Rather, CalECPA established suppression as the proper remedy for violation of its provisions or the Fourth Amendment. *See* Pen. Code § 1546.4(a). And as Mr. Dawes maintains, *see* Supplemental Reply at 16-17, such statutory suppression requirements do "'not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of [the statute]." *People v. Jackson* (2005) 129 Cal.App.4th 129, 153-160; Caskey, *California Search and Seizure* (2021) § 10:20.

Even under the Fourth Amendment, however, the warrant was "so lacking in indicia of probable cause" and "facially deficient" that the good faith doctrine should not apply. *See United States v. Leon*, 468 U.S. 897, 923 (1984); *see also* Supplemental Reply at 17-19. Sgt. Farrell's testimony on May 26 only confirms this.

Critically, Sgt. Farrell testified that he never explained to the issuing judge that a geofence warrant requires Google to search 592 million people, or that it requires a search of every person with Location History enabled. 5/26/22 Tr. at 57:5–10. He stated that he was unaware of these facts at the time because it was not a part of his training. *Id.* at 62:8–11. But this is no excuse. Instead, it highlights the fact that Sgt. Farrell had no formal training on geofence warrants, only a

45-minute office conversation with Officer Lieu and Lieutenant McGuire. *Id.* at 53. There was no formal training because, as Sgt. Farrell acknowledged, the SFPD had no policies or procedures for concerning geofence warrants. *Id.* at 52:18–21. There was no internal memo and no established technique vetted by the SFPD or the City Attorney's Office. *Id.* Indeed, despite the fact that he submitted a sworn affidavit to Judge Bolanos that cited his "training" and "experience" as foundations that the Court could rely upon, Sgt. Farrell testified that he did not actually understand the process Google goes through to execute a geofence warrant. *Id.* at 65:9–13. This is despite the fact that he agrees that he has an obligation to understand the nature of the search for which he is submitting an application. *Id.* at 64:6-16.

This lack of understanding is even more problematic, and underscores the lack of good faith, when considering that Sgt. Farrell was aware that a geofence warrant was "unique" and unlike other types of warrants he had dealt with in the past. *Id.* at 45:1–11. He recognized that it was different because it involves drawing a map around an area and capturing ID numbers from cell phones in that area. *See id.* at 45:4–11, 46:26–47:4. Nonetheless, he apparently did not think to ask how Google could possibly provide that information without searching everyone first. The reality is that Sgt. Farrell should have known how his warrant would operate when he applied for it. The lack of training and policies just underscores that he was acting outside the normal bounds for seeking search warrants. And by filing an unprecedented warrant application he did not fully understand, Sgt. Farrell assumed the risk it would be invalidated and that the evidence would be suppressed.

Furthermore, regardless of how Sgt. Farrell understood the process, it should have been apparent to any reasonable officer that a geofence search in a residential neighborhood would return many devices that have no connection to the crime. And thus it should have been apparent that there could be no probable cause to search or seize that data. Indeed, it is axiomatic that the scope of a search must be no broader than the probable cause on which it is based. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'"). Yet Sgt. Farrell proceeded, aware that they did not have a suspect and aware that there were no facts

showing that anyone involved had a cell phone. *See* 5/26/22 Tr. at 57:23–25. Sgt. Farrell knew this was not how warrants usually work, and he should have known it was completely backwards.

And any reasonable officer should have recognized the geofence warrant for what it is—a general warrant. It is plain that the Fourth Amendment forbids such general exploratory searches, with or without a warrant. *See Marron v. United States*, 275 U.S. 192, 195 (1927). Indeed, the British use of general warrants was the catalyst for the Fourth Amendment's warrant requirement. The Founders opposed them because of the discretion they gave to officials, placing "the liberty of every man in the hands of every petty officer" and were thus "the worst instrument of arbitrary power." *Stanford*, 379 U.S. at 481 (citations omitted). They allowed the government to target people without any evidence of criminal activity, "turn[ing] the concept of innocent until proven guilty on its head." *See* Donohue, 83 U. Chi. L. Rev. at 1317. Instead of having information that the person or place to be searched is engaged in illegal activity, general warrants presume guilt, establishing innocence only after a search. *Id.* Prohibiting such "promiscuous" searches therefore served to protect not only individual rights, but also establish a cornerstone criminal justice of America. *Id* at 1320.

Similarly, the unbridled discretion the warrant afforded Sgt. Farrell to determine which accounts to search in steps two and three should have been a red flag that it was facially deficient. Likewise in step one, the warrant left basic questions about what to search and seize up to the government and Google to work out—to play judge. It should have been obvious to Sgt. Farrell that valid warrants do not work this way. Thus, for example, no reasonable officer could rely on a warrant that authorized police to search any house in the neighborhood they deemed "relevant" to their investigation. Yet the warrant here did just that in digital form.

There is a lot that that is new about this case, but it is not new that warrants must be supported by probable case. And it is not new that warrants must be particularized. Rather, it should have been clear to Sgt. Farrell that the warrant here was so profoundly overbroad and lacking particularity that it was nothing short of a general warrant. And there is no such thing as relying on a general warrant in good faith. *See United States v. Winn*, 79 F. Supp. 3d 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions."). Rather, courts have recognized that "[t]he cost to society of sanctioning the use of general warrants—abhorrence for

which gave birth to the Fourth Amendment—is intolerable by any measure. No criminal case exists even suggesting the contrary." *United States v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982); *see also United States v. Wecht*, 619 F. Supp. 2d 213, 236–37 (W.D. Pa. 2009). Thus, the "the only remedy for a general warrant is to suppress all evidence obtained thereby." *United States v. Yusuf*, 461 F.3d 374, 393 n.19 (3d Cir. 2006).

Conclusion

For the foregoing reasons, Mr. Dawes submits that the geofence warrant was an impermissible general warrant, devoid of probable cause and particularity, the very type of warrant that the law and the Constitution was designed prohibit. Mr. Dawes therefore asks this Court to find that the good faith doctrine does not apply and suppress all evidence obtained from the geofence warrant, as well as all fruits thereof.

Dated: July 6, 2022

Respectfully submitted,

Sierra Villaran
Deputy Public Defender

Michael Price
NACDL

Counsel for LaQuan Dawes

EXHIBIT A

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT'S MOTION TO QUASH AND SUPPRESS EVIDENCE

Jennifer Lynch (SBN 240701)
jlynch@eff.org
Andrew Crocker (SBN 291596)
andrew@eff.org
Mark Rumold (SBN 279060)
mark@eff.org
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel: 415-463-9333
Fax: 415-436-9993

Attorneys for Electronic Frontier Foundation

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

PEOPLE OF THE STATE OF CALIFORNIA

Plaintiff,

vs.

LAQUAN DAWES,

Defendant.

Case No.: 19002022

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT'S MOTION TO QUASH AND SUPPRESS EVIDENCE

Date: 07/07/2020
Time: 9:00 AM
Dept.: 11 (to set)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

CONSTITUTIONAL PROVISIONS

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

I. INTRODUCTION

The warrant at issue here—a so-called "geofence" or "reverse location" warrant—is a modern version of an old problem: the general warrant.

The Fourth Amendment, and its familiar demands of particularity and probable cause, were designed to prevent warrants precisely like the one here—warrants that give law enforcement license to rummage through individuals' private spaces. At the Nation's founding, general warrants were used by customs officials to go house by house, searching for smuggled goods; *this* general warrant allows law enforcement to go Google account by Google account, searching each user's private location data for evidence of an alleged crime. Neither the Fourth Amendment, nor Article 1, Section 13 of the California constitution, tolerate a warrant of this breadth.

Compounding matters, the warrant also violates California's Electronic Communications Privacy Act ("CalECPA"), Cal. Penal Code § 1546, *et seq*. CalECPA provides Californians with the nation's strongest statutory protections for private electronic information. Unsurprisingly, a warrant that violates the Fourth Amendment and California's Constitution likewise runs afoul of CalECPA's stringent requirements.

Because the warrant here lacks particularity, is unconstitutionally overbroad, and violates CalECPA, the warrant must be quashed.

II. BACKGROUND

Geofence warrants are unlike typical warrants for electronic information in a key way: they are not targeted to specific individuals or accounts. Instead, they require a provider to search its entire reserve of user location data and identify any and all users or devices located in a geographic area during a time period specified by law enforcement.

With a geofence warrant, the police generally have no suspects. Instead, the sole basis for the warrant are three pieces of information: (1) that a crime occurred at a specific location around a given time; (2) that people carry cell phones that can create a detailed history of everywhere they have been in the past, and (3) that many companies collect and retain this private information.

The only public reports of geofence warrants involve Google, which has a particularly robust collection of location data. As Google has explained in another case involving geofence warrants, it tracks users who have a feature called "Location History" enabled on their mobile devices as they move through the world. *See* Br. of Amicus Curiae Google LLC at 6-8, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 20, 2019), ECF No. 59-1 [hereinafter "Google Amicus"]. Google collects location data from its own Android devices as well as from Apple devices that use Google apps. According to the *New York Times*, Google's Location History database contains information about hundreds of millions of devices around the world, going back almost a decade.[1] Although Google emphasizes that users must opt-in to Location History, that feature represents only one of the many ways that Google collects location data about its users. Google also collects location data through users' other interactions with its products, including web searching and even simply using a mobile device running Google's Android operating system.[2] Google's vast trove of location data draws on a variety of sensors, including GPS and Bluetooth, as well as methods for locating a device in relation to nearby cell towers and WiFi networks. Google Amicus at 10. As a result, individual location data points held by Google are often highly precise,

---

[1] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

[2] *See* Decl. of Marlo McGriff at ¶ 16-17, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-1 [hereinafter "Google Decl."]; Ryan Nakashima, *Google tracks your movements, like it or not*, AP (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb.

In *Chatrie*, Google asserted that only data from its Location History product is "sufficiently granular to be responsive to and searchable for" a reverse location request. Google Decl. ¶ 20. However, the warrant in this case is not limited to location history collected by Google's Location History feature, but includes any and all location information in the company's possession that fits the warrant's parameters. State of CA, City of San Francisco, Search Warrant and Aff. at 4 (Jan. 22, 2019) [hereinafter "Geofence Warrant" and "Geofence Affidavit"].

(footnote continued on following page)

determining where a user was at a given date and time, sometimes to within twenty meters or less. *Id.*; Google Decl. ¶ 12.

The geofence warrant in this case, like others reported on by the press, required Google to engage in a multi-step process.[3] For the first stage, law enforcement identified a "Target Location"—a geographical area identified by a series of latitudinal and longitudinal coordinates and time periods relevant to where and when the crime took place. Geofence Warrant at 3; Geofence Affidavit at 11. The warrant required Google to search for "all location information" corresponding to the Target Location and to provide information about any corresponding device, identified by a numerical identifier. As Google notes, "[t]he volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another." Google Amicus at 13. For the second stage, the police demanded Google provide additional location history outside of the initially defined geographic area and time frame for accounts that the officers, at their own discretion, determined were "relevant" to their investigation. Finally, officers demanded that Google provide identifying information for a subset of devices, including the user's name, email address, device identifier, phone number and other account information. Again, officers relied solely on their own finding of relevancy to determine this second subset. *See* Geofence Warrant at 4.

In order to comply with a geofence warrant, Google has explained that it must search its *entire store* of Location History for all Google users to identify responsive data. Google Amicus at 12-13. This is precisely because the warrant does not specify a particular account or device but

[3] Google explains that it developed this process to respond to geofence warrants to avoid having to fully identifying every user present in the government's area of interest in a given timeframe. *See* Google Amicus at 12-13.

instead demands the data corresponding to all devices present in the government's "Target Location." *Id.*

Although Google's Location History is relatively precise for its intended use as a "record" of users' "movements and travels," Google Decl. ¶ 5, the data Google produces in response to geofence warrants may actually be *imprecise and nonresponsive* in a highly significant respect. The company has explained that it cannot be sure that users whose data is produced were actually present within the geographic area specific in the request. *Id.* ¶ 25. This is because Location History "estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated L[ocation] H[istory] data point." *Id.* ¶ 24. Relying on GPS, WiFi and other methodology described above, Google's goal is to accurately infer a user's location within a certain radius 68% of the time. *Id.* In responding to a geofence warrant, Google will produce a user's data if a user's location is recorded as falling within the parameters of the requests, even if the radius corresponding to Google's 68% confidence interval lies partially outside those parameters. *Id.* ¶ 25. In other words, "it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius." *Id.* Hence, the request will frequently entail searching individuals who are not authorized in the warrant, and the data produced will frequently be inaccurate.

The use of geofence warrants is relatively new, reportedly dating to 2016, but they have quickly become a popular surveillance tool for the police. Google reports that it received 1500% more geofence warrants in 2018 than 2017 and 500% more in 2019 than in 2018. Google Amicus

at 3. According to the *New York Times*, the company received as many as 180 requests in a single week in 2019.[4]

Not only are the numbers of geofence warrants issued to Google increasing dramatically, but reports indicate that law enforcement frequently receives large sets of data in response to these warrants. In one case, the ATF was investigating a series of arsons in Milwaukee and served Google with two warrants that "demanded to know which specific Google customers were located in areas covering 29,387 square meters (or 3 hectares) during a total of nine hours for the four separate incidents."[5] In response, Google provided the government with identifying information for nearly 1,500 devices that happened to be within this vast geographic area during those nine hours. Even in cases with more limited search windows, geofence warrants routinely produce information belonging to tens or even hundreds of devices, depending on the size and population density of the area.[6]

Most of the information provided to law enforcement in response to geofence warrants does not pertain to individuals suspected of a crime. Yet law enforcement agents view location history

---

[4] Valentino-DeVries, *supra* note 1. Google does not report absolute numbers of geofence warrants, but it received over 20,000 total warrants in 2019 alone. *Global Requests for User Information*, Google Transparency Report, https://transparencyreport.google.com/user-data/overview?hl=en&user_data_produced=authority:US;series:compliance&lu=legal_process_breakdown&user_requests_report_period=series:requests,accounts;authority:US;time:Y2019H2&legal_process_breakdown=expanded:0,1 (limited to US legal process and expanded for the year 2019)

[5] Thomas Brewster, *Google Hands Feds 1,500 Phone Locations In Unprecedented 'Geofence' Search*, Forbes (Dec. 11, 2019), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/

[6] *See, e.g.*, Mot. to Suppress Evidence from a "Geofence" General Warrant, at 6, *filed in United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Oct. 29, 2019), ECF No. 29, (warrant produced identifiers belonging to 19 devices); Tyler Dukes & Lena Tillet, *In quest to solve murders, Raleigh community targeted twice by Google warrants*, WRAL (July 25, 2019) (geofence warrant produced information on 39 devices) https://www.wral.com/scene-of-a-crime-raleigh-police-search-google-accounts-as-part-of-downtown-fire-probe/17340984/; Brewster, *supra* note 5, (reporting a case in which Google pushed back on investigators to limit their search area to a 50 meter radius from 400 meters).

(footnote continued on following page)

belonging to devices identified in their search area and choose, at their own discretion, which to target for further investigation. Unsurprisingly, this has led to investigations that ensnare innocent individuals. In one case, police sought detailed information about a man in connection with a burglary after seeing his travel history in the first step of a geofence warrant. However, the man's travel history was part of an exercise tracking app he used to log months of bike rides that happened to take him past the site of the burglary. Investigators eventually acknowledged he should not have been a suspect.[7]

III. ARGUMENT

A. The Geofence Warrant is an Unconstitutional General Warrant in Violation of the Fourth Amendment and Article I, Section 13.

The SFPD's request to Google to search for "all location data" for the mobile devices of everyone who was in the "Target Location" around the time a crime occurred in the past is an unconstitutional general warrant.

Like other "papers" and "effects," a person's location information can only be seized and searched with a warrant. *Carpenter v. United States* (2018) 138 S. Ct. 2206, 2217. That warrant must satisfy all the Fourth Amendment's familiar requirements—that it be issued by a neutral and detached judicial officer, supported by probable cause and describing with particularity the place to be searched and the items to be seized. *See Ex parte Jackson* (1878) 96 U.S. 727, 733; *United States v. Van Leeuwen* (1970) 397 U.S. 249, 251. It is axiomatic that "a warrant may not authorize

[7] Jon Schuppe, *Google tracked his bike ride past a burglarized home. That made him a suspect*, NBC News (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.
(footnote continued on following page)

a search broader than the facts supporting its issuance." *People v. Frank* (1985) 38 Cal. 3d 711, 728.[8]

The geofence warrant in this case fails each of these requirements. It is overbroad because it encompasses data and accounts that are in no way connected to the crime being investigated. *See id.* at 727. In some instances, data produced is outside the boundaries of the warrant itself. Google Decl. ¶ 25. It fails to meet the Fourth Amendment's particularity requirement because it does not identify any particular person, device, or account to be searched. *See Stanford v. Texas* (1965) 379 U.S. 476, 485-86. And it is not supported by probable cause because the mere fact that many, or even most, people use devices that record and share location information with Google is insufficient to show the perpetrator used such a device, much less to justify a search of the location history of *all* Google's users. *See Ybarra v. Illinois* (1979) 444 U.S. 85, 91-92 ("mere propinquity" to criminal activity insufficient to establish probable cause).

In effect, this warrant gave SFPD license to search through the location information of millions of Google users around the globe; and it gave the police the authority to require Google to produce more information about particular devices that, at SFPD's own discretion, it deemed of interest. The California Supreme Court has recognized that "[t]he vice of an overbroad warrant" such as this one "is that it invites the police to treat it merely as an excuse to conduct an unconstitutional general search." *Frank*, 38 Cal. 3d at 726.

1. The Fourth Amendment was drafted to preclude general warrants.

In the American colonies, British agents used general warrants, known as "writs of assistance," to conduct broad searches for smuggled goods, limited only by the agents' own

[8] In most cases, the protections afforded Californians under Article 1, Section 13 are coextensive with the Fourth Amendment to the United States Constitution. *See People v. Crowson* (1983) 33 Cal. 3d 623, 629.
(footnote continued on following page)

discretion. *See Stanford*, 379 U.S. at 481-82 (describing writs of assistance and their influence on the drafters of the Fourth Amendment).[9] "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States* (1981) 451 U.S. 204, 220. "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley v. California* (2014) 573 U.S. 373, 403.

In addition to the experience of the American colonists, two English cases—*Wilkes v. Wood* (C.B. 1763) 98 Eng. Rep. 489, 490, and *Entick v. Carrington* (1769)19 Howell's St. Tr. col. 1029 —directly inspired the Fourth Amendment. In *Wilkes*, Lord Halifax issued a general warrant authorizing the seizure of papers from people suspected of libel without specifying which houses or business to search and "without nam[ing] of the person charged." *Wilkes,* 98 Eng. Rep. at 490. Nearly fifty people were arrested, their houses were ransacked, and all their papers were seized. In *Entick*, the King's agents were authorized to search for the author and anyone related to a publication deemed seditious. At the agents' discretion, they raided, searched through, and carted away papers from many homes and businesses, including Entick's.

The Fourth Amendment was drafted against this backdrop. Its text "reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford*, 379 U.S. at 481-82.

2. Geofence warrants have direct parallels to the general warrants that inspired the Fourth Amendment.

A warrant purporting to authorize a reverse location search is a digital analogue to an arrest warrant that authorizes officers to search every house in an area of a town—simply on the chance

[9] *See also* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning, 602–1791* p. 363 (2009).

that someone connected with a crime might be located inside one. Like the general warrants and writs of assistance used in England and Colonial America, this warrant's lack of particularity and overbreadth invites the police to treat it as an excuse to conduct an unconstitutional general search. *See Frank*, 38 Cal. 3d at 726.

Here, like the general warrants discussed in *Wilkes* and *Entick*, the geofence "warrant specified only an offense" and left to the SFPD's discretion "the decision as to which persons" should be pursued. *Steagald*, 451 U.S. at 220. The warrant did not name particular suspects or even particular accounts. Instead, it sought information on *all* accounts associated with devices that happened to be in the general area where a crime occurred. And as described above, it may have resulted in the search and production of data corresponding to devices that were never even in that general area. The warrant gave the police unrestricted license to search each of these accounts and then, *at SFPD's own discretion*, to conduct a broader search of a subset of those devices, based on no clear, limiting criteria other than that certain accounts would be "identified [by SFPD] as relevant." Geofence Warrant at 4. But, with a proper search warrant, "[n]othing should be left to the discretion of the officer." *People v. Dumas* (1973) 9 Cal.3d 871, 880. The geofence warrant is precisely the sort of "general, exploratory rummaging" the Fourth Amendment was intended to forestall. *Coolidge v. New Hampshire* (1971) 403 U.S. 443, 467; *Andresen v. Maryland* (1976) 427 U.S. 463, 479-480.

The California Supreme Court has held that "[t]he requirement of particularity is designed to prevent general exploratory searches which unreasonably interfere with a person's right to privacy." *Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249. When a warrant is unduly broad, the warrant is more likely to reach information that is "ordinarily innocuous and [] not necessarily connected with a crime." *Aday v. Superior Court of Alameda Cty.* (1961) 55 Cal.2d 789, 796. Where, as here, the categories of records sought are "so sweeping" as to include every device in a

given area, the warrant places "no meaningful restriction on the things to be seized. Such a warrant is similar to the general warrant permitting unlimited search, which has long been condemned." *Id.*[10]

The warrant here is arguably broader than those "long…condemned" general warrants. *Id.* As Google notes, because it does not retain location data in discrete groups labeled by date, time, or particular geographic areas, reverse location warrants require it to search through *all* of its users' data—*tens of millions* of user accounts—just to extract the subset of location information responsive to the warrant. Google Decl. ¶ 13. And a warrant like this was not conceivable, much less possible, at the nation's founding. Historical location data held by Google "gives police access to a category of information otherwise unknowable." *Carpenter*, 138 S. Ct. at 2218. Like cell site location information, it allows the police to "travel back in time to retrace a person's whereabouts." *Id.*

Search warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet" of information "to be seized at the discretion of the State." *United States v. Bridges* (9th Cir. 2003) 344 F.3d 1010, 1016. Searches like these—where the only information the police have is that a crime has occurred—are just that: a "dragnet" that inevitably implicates innocent people who happen to be in the wrong place at the wrong time. *See* Sec. II, *supra*. Google releases data to the police that includes location history for people with no

---

[10] The same concerns that underlie the reasoning in cases involving searches and seizures of papers like *Aday*, *Burrows*, and *Frank*, apply equally to searches and seizures of location data. Like personal and business writings, information about where a person was at some time in the past can reveal protected expressive and associational activities— it can reflect "a wealth of detail about her familial, political, professional, religious, and sexual associations." *Riley*, 573 U.S. at 396 (quoting *United States v. Jones* (2012) 565 U.S. 400, 415 (Sotomayor, J., concurring)). Information about multiple peoples' locations only increases the privacy harm by showing associations between and among individuals. *See id.*

(footnote continued on following page)

connection to the crime under investigation. And even though the initial release purportedly only includes accounts identified by "a numerical identifier,"[11] the warrant requires Google to later release, at SFPD's discretion, data on a subset of those accounts that includes the "subscriber's name, email address, IMEI and phone numbers, services subscribed to, recovery SMS phone number and recovery email address." Geofence Warrant at 4. The second disclosure is not based on the determination of a neutral and detached magistrate: it is based solely on law enforcement's own determination of "relevancy." *Id.* This kind of search turns every device owner in the area—and some even outside the area—during the time at issue into a suspect, for no other reason than that they own a device that shares location information with Google.[12]

The breadth of the warrant here, coupled with the absence of specific information about the accounts or devices to be searched, renders it invalid under the Fourth Amendment.

B. The Geofence Warrant Violates CalECPA.

In addition to the protections provided by the Fourth Amendment and Article 1, Section 13, CalECPA, Penal Code § 1546 - § 1546.6, regulates law enforcement access to private electronic information by California law enforcement officials. The geofence warrant likewise violates CalECPA's stringent requirements.

---

[11] The fact that the initial data is deidentified, and that the time period and geographic scope of the search are limited, is of no import to the Fourth Amendment analysis, because the warrant still allows the police to obtain information that they would otherwise not have in order to build their case and to select individuals to narrow in on—the very thing the Fourth Amendment prohibits.

[12] Neither the convenience of gathering location information on all individuals in the area nor the fact that the broad warrant might return information relevant to the investigation—and might therefore be "particular" as to that information—can justify the warrant after the fact or in any event allow the introduction of that particular or particularly helpful information. As the California Supreme Court has recognized, "[s]uch an abuse of the warrant procedure, of course, could not be tolerated." *Aday,* 55 Cal. 2d at 797.

1. CalECPA guarantees individuals' privacy in electronic information, including location information, by placing strict limits on law enforcement access to that information.

The legislature drafted CalECPA with two goals: first, to provide a clear statutory framework for the application of existing state and federal constitutional and statutory protections for private electronic information—protections that had been unevenly applied in the digital age; second, to provide *additional* guarantees for that private electronic information, above and beyond existing statutory and constitutional protections. Assemb. Comm. on Privacy and Consumer Protection Rep. at 5 (Ca. Jun. 23, 2015) ("This bill is intended to both codify and expand on existing" protections for electronic information).[13] For these reasons, CalECPA provides the strongest digital privacy protections in the nation. *See* Susan Freiwald, *CalECPA: At the Privacy Vanguard*, 33 Berkeley Tech. L.J. 131, 133 (2018).[14]

CalECPA requires law enforcement agencies to obtain a probable-cause warrant for almost all electronic information, including location information, § 1546.1. It also imposes a heightened specificity standard and stringent particularity requirements on those warrants, § 1546.1(d)(1). The

---

[13] *Available at* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178#; *see also* S. Pub. Safety Rep. No. SB 178 at 8 (Ca. Mar. 23, 2015) ("[CalECPA] updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information."), *available at* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178#;

[14] Professor Freiwald was intimately involved in CalECPA's passage. She served as "an issue expert for CalECPA's authors, State Senators Mark Leno and Joel Anderson, and as a member of the bill's policy and language teams. In that capacity, [she] helped answer questions about the bill's language, testified at legislative committee hearings about its legal impact, and coordinated dozens of academic colleagues to send a scholarly support letter to California Governor Jerry Brown." Freiwald, *supra*, 131 n. d1.

Professor Freiwald's account is thus more than an academic treatment of the subject: it is reliable "indicia of legislative intent." *Highland Ranch v. Agric. Labor Relations Bd.* (1981) 29 Cal.3d 848, 860 (relying on a law review article written by a law professor who assisted in drafting statute).

statute also specifies explicit minimization rules for data unrelated to law enforcement's investigation, § 1546.1(d)(2); imposes clear notice requirements, § 1546.2; and provides a robust suppression remedy, § 1546.4(a).

CalECPA's proponents recognized the special risks to individual privacy posed by digital searches of electronic information. *See, e.g.*, Assem. Comm. on Privacy and Consumer Protection Report at 8 (noting bill's requirements "explicitly limit the searches to necessary information"). As Professor Freiwald explains, CalECPA's specific warrant requirements work to prevent the type of expansive digital "fishing expeditions that violate the spirit, if not the letter, of the Fourth Amendment." Freiwald, *supra*, at 154.

In addition to cabining wide-ranging searches of digital information, CalECPA's proponents had a special concern for the protection of location information. *See, e.g.*, Assemb. Floor Analysis No. SB 178 at 5 (Ca. Sep. 4, 2015);[15] Freiwald, *supra*, at 140 ("location data [was] an area of great concern to CalECPA's proponents"). Prior to CalECPA, federal and state court decisions had left location data "ambiguously or completely unprotected." *Id.* CalECPA changed that by applying its robust warrant standard to the compelled production of location information. *Id.*

2. The geofence warrant violates CalECPA's particularity requirement.

CalECPA requires that all warrants satisfy stringent particularity requirements. These requirements work to limit the scope of electronic information law enforcement can obtain through a warrant. Penal Code § 1546.1(d)(1). Thus, a warrant must specify, as "reasonable and appropriate:" "the time periods covered" by the warrant, the "target individuals or accounts, the applications or services covered, and the types of information sought." *Id.*

[15] *Available at* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178#

The warrant here wholly failed to describe the "target individuals or accounts." *Id.* No individual's name was included in the warrant; nor was any specific cell phone number, email address, or account information. At best, the warrant can be understood to target all "mobile devices" located at a certain place, over the course of multiple hours, on a specific day. Geofence Warrant at 1.

But that level of generality is irreconcilable with CalECPA's *heightened* particularity requirements. As explained above, this type of generalized warrant violates the Fourth Amendment. *See* Sec. III(A), *supra*. But *even assuming* a warrant like this violates only the "spirit of the Fourth Amendment," Freiwald, *supra*, at 154, CalECPA places additional specificity requirements on warrants for electronic information—beyond those already required by the Fourth Amendment. Those additional requirements work to prohibit unspecific "fishing expeditions" like the warrant here. *Id.*

A warrant that fails to identify any target individual or account is neither reasonable nor appropriate under CalECPA.

II. CONCLUSION

The warrant violates the Fourth Amendment, Article 1, Section 13, and CalECPA. The Court should grant Mr. Dawes motion to quash.

Respectfully submitted,

Dated: June 10, 2020

By_____
Jennifer Lynch

Attorney for Amicus Curiae Electronic Frontier Foundation

PROOF OF SERVICE

I, Madeleine Mulkern, do hereby affirm I am employed in the County of San Francisco, State of California. I am over the age of 18 years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109. I am employed in the office of a member of the bar of this court at whose direction the service was made.

On June 10, 2020, I served the following documents:

Application to File Brief of Amicus Curiae Electronic Frontier Foundation

Brief of Amicus Curiae Electronic Frontier Foundation

[proposed] Order Granting Application to File Brief of Amicus Curiae Electronic Frontier Foundation

☒ United States Mail. I enclosed the documents in a sealed envelope addressed to the person below and deposited the sealed envelope with the United States Postal Service, with postage fully paid. I am a resident employed in the county where the mailing occurred. The envelope or package was placed in the mail at San Francisco, California.

Manohar Raju, Public Defender
City and County of San Francisco
Matt Gonzalez, Chief Attorney
Sierra Villaran, Deputy Public Defender
Brett Diehl, Certified Law Student
555 Seventh Street
San Francisco, CA 94103

Attorneys for Laquan Dawes

Anthony Lombardo
Assistant District Attorney
Office of the District Attorney
350 Rhode Island
North Building, Suite 400N
San Francisco CA 94103

Attorneys for the State of California

I declare under penalty of perjury of the laws of the State of California and the United States that the foregoing is true and correct. Executed this 10th day of June, 2020 in San Francisco, California.

_____
Madeleine Mulkern

EXHIBIT B

REPORTER'S TRANSCRIPT OF HEARRING

THURSDAY, MAY 26, 2022

SUPERIOR COURT OF CALIFORNIA

IN AND FOR THE COUNTY OF SAN FRANCISCO

DEPARTMENT 23

---oOo---

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. LAQUAN DAWES and ALPHONSO ODOM, Defendant.	Court No. 19002022, 19002037 Pages 1-69

Reporter's Transcript of

HEARING

Thursday, May 26, 2022

BEFORE: THE HONORABLE LINDA COLFAX, JUDGE

---oOo---

APPEARANCES OF COUNSEL:

For the People:

CHESA BOUDIN
District Attorney
District Attorney's Office
County of San Francisco
350 Rhode Island Street
North Building, Suite 400n
San Francisco, CA 94103
BY: JACK SHANNON
Deputy District Attorney

For the Defendant:

MANOHAR RAJU
Public Defender
Public Defender's Office
County of San Francisco
555 7th Street
San Francisco, CA 94103
BY: SIERRA VILLARAN
Deputy Public Defender

Also Appearing: Michael Price and Silas Geneson

REPORTED BY: DIANA PAQUETTE, CSR NO. 14192

INDEX OF WITNESSES

INDEX OF EXHIBITS

DEFENSE EXHIBIT	ID	EVD
D. Search warrant affidavit.	13	13
E. Declaration from Google.	16	17
F. Report May 12, 2022.	18	19
G. Report October 24, 2021.	18	24

THURSDAY MAY 26, 2022

BEFORE: THE HONORABLE LINDA COLFAX, JUDGE

--oOo-

THE COURT: Let's then call the matters at lines six and eight. People vs. Laquan Dawes. As well as line seven, Alphonso Odom.

MR. SHANNON: Good afternoon, Your Honor. Jack Shannon for the People.

THE DEFENDANT: Good afternoon, Your Honor.

THE COURT: Good afternoon.

MS. VILLARAN: Good afternoon.

THE COURT: Good afternoon. I hope you're feeling okay, sir.

THE DEFENDANT: I feel a little better than I was the other day.

THE COURT: That's good. Will you mute yourself again, please?

THE DEFENDANT: Okay. Thank you.

MS. VILLARAN: Sierra Villaran.

MR. GENESON: Silas Geneson for Mr. Odom.

MR. PRICE: Mike Price also for Mr. Dawes.

THE COURT: We are on today for a long awaited hearing on defense's motion to quash two of the search warrants. I was thinking I should say for purposes of the record which one was December 4th, 2018, was when that warrant was issued and a motion to then suppress. Are both sides ready for this hearing?

MR. SHANNON: Yes, your Honor.

MS. VILLARAN: Yes, your Honor.

THE COURT: Have you all -- I know there are witnesses. There's issues related to witnesses who have come here. Possible availability. Are you simply wanting to proceed in the normal course of a affairs or have you all discussed taking any witnesses out of turn?

MR. SHANNON: I spoke with Ms. Villaran about those issues. I think that even with her -- my witness has availability issues as he's not -- he's leaving town this afternoon, but I spoke with Ms. Villaran about the anticipated time frame for her witness, and I don't think it's be a problem to proceed in the normal order. My witness should be able to leave when he needs to.

THE COURT: Just so you all know it's about 1:40. We will take one 15 minute recess in the afternoon and do our very best to get all the testimony in today. Then you may call your first witness.

MR. SHANNON: Thank you, your Honor. We would call -- but prior to doing so I would like to lodge stipulated materials that both parties have agreed to with the Court. I have two copies. One for the Court and for the -- for the record if I may approach.

THE COURT: You may.

MR. SHANNON: Your Honor, is the docket in court for this case?

THE COURT: Ish. Yes. Is there something in particular you're seeking from it?

MR. SHANNON: No. Not particularly. The affidavit. It's fine. We'll talk about it later.

THE CLERK: Do you solemnly state under penalty of perjury that the testimony you are about to give in the matter pending before this court shall be the truth and nothing but the truth?

THE WITNESS: Yes.

SPENCER MCINVALLE,

called as a witness by the People, having been duly sworn, was examined and testified as follows:

THE COURT: Please state and spell your name name for the record.

THE WITNESS: S-P-E-N-C-E-R. Last, M-C-I-N-V-A-L-L-E.

THE COURT: You may proceed.

DIRECT EXAMINATION

BY MR. PRICE:

Q Good afternoon, Mr. McInvalle.

A Good afternoon.

Q Can you state your occupation and relationship to the case for us?

THE COURT: Counsel, I have to stop you from the very beginning. Are you hoping the Court's going to be able to read the things you're putting on the screen?

MR. PRICE: The things on the screen are just meant to be demonstrative. Everything I'm putting on the screen is pretty --

THE COURT: Demonstrative for whom?

MR. PRICE: For the Court so that it's easier which section or which slide we're talking about rather than going through different pages. You will get a hard copy of everything.

THE COURT: Give me a brief moment to log in on my computer

and that way -- and I will at least be able to follow a little better. Okay. Thank you. You may continue.

MR. PRICE: Thank you, your Honor.

Q Mr. McInvalle, can you please remind us your occupation and relationship to this case?

A I'm a technical investigator in forensics in the digital forensics division.

Q And you've been retained by the defense?

A I have.

Q You previously qualified as an expert in this case?

A I was. Yes.

Q In what field were you qualified?

A I believe mobile device forensics, digital forensics, and location analysis I believe.

MR. PRICE: So based off of the previous hearing I believe the People will stipulate that Mr. McInvalle is qualified still unless you would like an opportunity to voir dire.

MR. SHANNON: Stipulated.

THE COURT: All right. You may continue to question your witness based upon that proffer.

MR. PRICE: Thank you, your Honor.

Q So I want to just start with a few basics and ask you about the sources of location data that Google uses to identify and locate phones generally.

A Sure. Within location history you commonly see the use of wifi networks, GPS, the cellular network, and sometimes bluetooth.

Q I think a lot of us are familiar with some of those, but could

you explain a little bit more, especially about wifi?
A We use GPS very commonly in our day-to-day activities. It uses satellites to locate us, but wifi's a little different. It is using the wifi networks around us that have been mapped out by Google so that using signal strength values you can determine the approximate location of the device by measuring essentially its distance based on signal stream values from each of those wifi routers. You don't need to connect to all of these routers, but it's simply it's those that your device sees at any given time.
Q When Google is determining location from these inputs, how do they do that? Do they just take the GPS data and show it to you?
A In terms of what they produce?
Q Yeah.
A So what they will produce is -- you will see the device identifiers with an estimated latitude and longitude with a margin of error or a display radius that they also produce.
Q So this is an estimate?
A It is. So this is Google's estimate. This is appropriate to Google.
Q Is it different than GPS data?
A Especially with wifi because clearly it's not GPS. Just because you see latitudes and longitudes it is not GPS data.
Q Do you know how Google comes up with this sort of estimate?
A No, I do not.
Q Do you know if they run an algorithm of some kind?
A I assume they do. Yes.

Q Is that algorithm public in any way?
A Not that I'm aware of.
Q We have these different inputs --
THE COURT: I'm going to stop you. The question was asked what will they produce, as you will see, and then you go onto explain it. When you say this is what they produce, at what time frame in this process are you talking about.
THE WITNESS: So for that information where device IDs and their approximate locations and other information, it can be produced several times within the warrant. It's one of the first things produced in the request as well as a subsequent request there is further information just expanding upon that data that you're seeing.
THE COURT: Okay. Go on.
MR. PRICE: Maybe I can clarify.
Q When I meant they I was referring to Google. So how Google produces your location and information to you.
A Right. So it's those spreadsheets with that same data that I've explained.
Q When we have this location data, it's based off of these different inputs. What happens to the accuracy of that data with different types of inputs?
A The different methods of locating a device do a better job than others at locating the device. So GPS we all know can be very accurate. It has its inherent issues when you put it inside of buildings and things, but most for parts it can accurately locate devices. What you will kind of see next in the process of really kinda keeps up with GPS is the wifi

location because those generally have smaller -- can have smaller estimates as well than the cellular network you start to get really large estimates. It's just because you're using a cellular network which isn't great at precising to make an estimation.

Q Is there just one margin of error for all these points or does it change based on the data available?

A I have seen it vary from 3 meters to 3,000 meters. It's anywhere in between.

Q Thank you. So based on your research are there different repositories of locations data that Google keeps?

A Yes. So, well, we have been talking about is what is called location history. There are other functions that they have which are Google location accuracy. That is a repository of those wifi locations and other inputs they are using to measure from, and then there's web and app activity so Google can track your relative location based on the internet usage IP addresses and other information that is gathered to determine the approximate location of the user.

Q So we've got location history, web and app activity, and Google location accuracy?

A Correct.

Q What does Google do generally with all of this location data?

A Google besides their search function that everybody's familiar with Google's an advertising company. That's how they make their money. The gathering of data is how they are able to monetize the information.

Q Does Google ever give that information to an advertiser?

A No. So the type of data that we see in return of warrants is nothing that is produced other than in this instance.
Q All right. I want to -- you reviewed the warrant in this case?
A I have.
Q And what kind of warrant was it?
A It's a Google geofence warrant.
Q Can you explain to us just generally how a geofence warrant is?
A They're typically broken down into separate stages. Each stage of the warrant requests a different portion or different parameters of data, but generally what is produced is some form of location history for a given time and for a space or geofence that is indicated in the warrant.
Q And then step two?
A That is step one. Step one is which devices are supposed to be located within the geofence for a given time. If stage two is in the warrant, which it is in this case, you will then remove the geofence, expand the time frame, and then watch the selected users for an extended period of time. You now see those devices travel from prior to the geofence, into the geofence, and then outside of the geofence. So you see travel or you see a larger time frame.
Q What's the difference between stage two and stage three?
A So stage three is not so much a request for location information but stage three is once the subscriber identity information is provided.
Q Thank you. It's fairly unusual to see a warrant follow this

sort of process. Are you aware of where this process came from?
A Yes. From previous cases and testimony that I've witnessed from Google employees. This is a process developed by a governmental agency and Google to produce this information.
Q Do you happen to remember the name of that governmental agency?
A The acronym is CCIPS.
Q Would it sound correct to you if it's the Computer Crimes and Intellectual Property Sections?
A I believe that's correct.
Q How do you know this?
A Again, I witnessed this testimony from Google employees. The location history manager themselves.
Q Are you aware of any discussions that Google had with CCIPS about crafting the process for this warrant?
A Not the specific conversations but yes there were conversations. Both the FBI as well as Google had confirmed that those were a negotiated or crafted boilerplate.
Q To your knowledge did this collaboration between CCIPS and Google produce any sample language?
A There are boilerplate templates to make these requests.
Q Let's turn now to what type of location data this warrant authorized. I want to have you take a look now at what I believe has been previously been introduced as evidence, although we're not exactly sure, Your Honor.
MR. PRICE: It's the search warrant and affidavit in this case. I can reintroduce as defense exhibit, although it may have been introduced as a government exhibit at the previous

hearing.

THE COURT: You may. My recollection from the bifurcated hearing is there were Exhibits A through C only marked. So why don't you just move beyond A through C so that we can try to have as clean a record of as possible.

MR. PRICE: We will with start exhibit --

Q I'd like you to take a look at this document.

MR. PRICE: May I approach, Your Honor?

THE COURT: You may. Are you wanting a copy marked for identification?

MR. PRICE: Yes. It'll be Exhibit D.

THE COURT: Exhibit D for identification is search warrant affidavit stamped -- court stamped -- January 22nd, 2019.

(Defendant's Exhibit D marked for identification.)

MR. SHANNON: No objection to being admitted.

THE COURT: Exhibit D will be admitted.

(Defendant's Exhibit D received in evidence.)

Q Mr. McInvalle, I'd like to turn your attention to page three of what is now Exhibit D.

A Okay.

Q Page four. Subsection A where it says location information?

A Yes. I see that.

Q We have that snippet up on the screen that we're discussing at the moment. Can you take a look at this warrant and tell us what kind of location data the warrant specifies?

A There are location information that specifies all location

data.
Q Does it specify web and app activity?
A No, it does not.
Q Does it specify Google location accuracy?
A No, sir.
Q Does it specify Google location history?
A No, sir.
Q Do you know what type of data was searched as a result of the warrant here?
A Based on my review of the data this is location history data that was produced in the steps of this warrant.
Q Was that only location history data or did they search other kinds?
A I'm not aware of any other searches, but I know data was produced from location history.
Q Based on your understanding who decided to just search location history?
THE COURT: That seems to assume facts based upon the last answer. Did you say that only location history data was produced but you don't know how much location -- what data was actually searched?
MR. PRICE: Well, we're saying that the warrant didn't specify one way or the other, but we do know that Google only searched location history data.
THE COURT: Was that your answer?
THE WITNESS: Only produced location history data. I'm not aware if they searched anything else.
THE COURT: Okay. Your next question.

Q Who made that decision to search location history or produce location history?
A I don't know.
Q Did it specify in the warrant?
A Not -- no. I didn't see it specified in the warrant.
Q Based on your experiences in previous cases do you know whose decision that has been?
A I've not known whose decision it is.
MR. SHANNON: Do you mind if I interrupt briefly with a question?
THE COURT: A question for who?
MR. SHANNON: The Court.
THE COURT: You may.
MR. SHANNON: The exhibits that we've stipulated to, has the Court reviewed any of those yet or are you just receiving them for the first time at the start of this hearing?
THE COURT: Can you be a little more specific because I have received so much? So if you're talking about transcripts from prior testimony.
MR. SHANNON: I'm talking about the declarations from the Google witnesses.
THE COURT: From Ms. Rodriguez and Mr. McGriff? I've reviewed those.
MR. SHANNON: Okay. Sorry. Thank you.
Q Mr. McInvalle, do all Google users have location history data?
A No, they do not.
MR. SHANNON: I'm going to interrupt. Just 352. I'm trying to allow for a little bit of review, but a lot of what we've

gone over is in the stipulated exhibits.

THE COURT: At this time the objection's overruled.

Q On average do you know what percentage of Google users have location history enabled?

A Based on Google about 33 percent of their users.

Q You know that how?

A Again, testimony from Google.

Q What was the search date specified for the geofence warrant in this case?

A This was October 24th of 2018.

Q Do you know how many users had location history enabled in 2018?

A Again, from Google's declaration approximately 592 million users.

Q 592 million?

A Yes.

Q You reviewed a declaration from Google that was prepared in this case?

A Yes. I believe Emily Mosely.

MR. PRICE: I'm going to approach one more time and show you that.

THE COURT: Are you asking this that be marked as an exhibit?

MR. PRICE: I will. Yes, your Honor.

(Defendant's Exhibit E marked for identification.)

Q Do you recognize the document that I just handed you?

A Yes. This is the declaration that I was referencing.

MR. PRICE: At this time I would like to move this into evidence as Defense Exhibit E.

MR. SHANNON: No objection.

THE COURT: Exhibit E will be admitted.

(Defendant's Exhibit E received in evidence.)

Q Can you please turn to page two?

THE COURT: Of the declaration, Exhibit E?

MR. PRICE: Of the declaration, Exhibit E.

Q Page two of Exhibit E -- and, Mr. McInvalle, I ask to read the highlighted portion for us?

A Under number three it is in October 2018 there were approximately 592 million daily active users of location history worldwide. Roughly one-third of all active Google users had location history enabled on their accounts.

THE COURT: Thank you. Counsel, we do have limited time today. I will be entertaining 352 objections for questions that are simply redundant.

MR. PRICE: I think we've covered the basics so moving on specifically to this set of facts.

Q In fact, Mr. McInvalle, did you prepare a second supplemental report dated May 12th?

A Yes, I did.

Q That concerned a significance of this 592 million number?

A That's right.

MR. PRICE: I'd like to mark this, Your Honor, as Defense Exhibit F.

THE COURT: It may be so marked. It's been previously

provided to the district attorney as part of the filing on May 13th?

(Defendant's Exhibit F marked for identification.)

MR. PRICE: That's correct.

Q Can you tell us what that number 592 million tells you about any geofence search in October of 2018?

A In any geofence within a warrant, no matter how many there are or how large or small they are each one requires a search of that number of users.

Q 592 million?

A Yes.

Q Let's focus on the warrant specifically in this case. Can you take a look at the search warrant, Appendix A? It's on page three.

A Yes.

Q Can you tell us what stage one requested in this warrant?

A So stage one requested a search on October 24th, 2018, for three separate time periods. They are listed here for each of the time periods as well as underneath you get the coordinates of the geofence. The line would be drawn in between these points to form the geofence.

Q I know that you've drawn this out in another report, which I'd like to introduce as the last item. It's going to be Exhibit G.

(Defendant's Exhibit G marked for identification.)

MR. PRICE: Your Honor, if I did not move Exhibit F into evidence, I'd like to do that at this time.

THE COURT: Any objection?

MR. SHANNON: No.

(Defendant's Exhibit F received in evidence.)

THE COURT: My only thing is Exhibit G -- I need some way to distinguish between Exhibit F and Exhibit G for the record as they are both reports.

MR. PRICE: Exhibit F is dated May 12th although I think the date might be at the end.

THE COURT: That's why I need the record -- so Exhibit F on the last page has a May 12, 2022, and Exhibit G is dated October 18th, 2021. Thank you. Off the record.

(Off the record.)

(Back on the record.)

THE COURT: Exhibit G for the record is a report prepared by Mr. McInvalle with the date already dated October 18th, 2021. Thank you.

MR. PRICE: Thank you for the clarification.

Q Mr. McInvalle, did you create a map of the geofence in the supplemental report?

A Yes. It would be page four.

Q That's what we're looking at here. I'd like you to turn your attention to figure three and can you tell us what we're looking at?

A So the red lines indicate the geofence based on the points referenced in Appendix A of the geofence warrant.

Q What did Google have to do in order to determine which devices were inside of that geofence?

A Sure. Because Google doesn't store this information in a way that is searchable by location -- it's organized by the device IDs and they have to run a query across the coordinates for each of those entries to determine which of those entries purport to fall within this geofence.

Q They have to serve 592 million people to figure out what was in that trapezoid?

A Right. To figure out which one of those points would have fallen in this area.

Q As you discussed in your second report, which would be Exhibit F, what would happen in step one if the size or shape of that geofence was changed?

A So the size and shape does not affect the scope of what Google has to do to the data to determine who may or may not be within this area.

Q What would happen if we made the geofence just the size of a parking space only covered for five minutes?

MR. SHANNON: I'm going to object as 352. I think this is covered in Exhibit F, which has already been admitted.

THE COURT: The objection is sustained. The point's also been made.

MR. PRICE: I don't believe we've previously presented these reports to the court, Your Honor.

THE COURT: You haven't, but isn't your point no matter how big or small it's the same number that gets searched, that 500 something?

MR. PRICE: Yes, it is.

THE COURT: So move on.

MR. PRICE: We may move on.
Q Can you tell us -- we can skip ahead to slide nine -- how many time frames are specified in this warrant?
A Yes. Looking at Appendix A there are three separate time frames.
Q How many sets of step one returns did you review in this case?
A Three.
Q So how many times did Google have to search 592 million people?
A It would have been three separate searches.
Q And after conducting a search of 592 million three separate times, how many individuals had their information sent back to the police?
A Across the returns I believe it was a nine total device IDs were returned in the first stage, first stages.
Q In the first stage. So to identify those nine people Google had to search 592 times 3?
A Right.
Q I want to keep talking about step one but switch gears a little bit. Could you turn to page three of your first supplemental report which is Exhibit G and look at figure one?
A Yes.
Q Can you tell us the different types of information included there?
A What was the question? I'm sorry.
Q The different types of data included in the return.
A Oh, yes. That is the device ID is there on the far left. That indicates which device is being indicated and its location.

The date, the time, the latitude, longitude. That's that estimated point as well as the source, what was used to create this estimate, and then finally that maps display radius.

Q That display radius is what I'm interested in. This is a figure two in that same report. Can you tell us what this is?

A This is just an illustration of how the map display radius gets used. When Google reports the estimated location, that is the center point for the map's radius to be drawn around so it's a radius drawn out from that point so in that instance it would be a 58 meter radius, 58 meters out from the center point, and you have the blue shaded area.

MS. VILLARAN: It looks like on Zoom -- that the meeting has been ended by the host so.

THE COURT: The hearing's over. Let's pause for a moment and see if we can get back on Zoom. We'll go off the record.

(Off the record.)

(Back on the record.)

THE COURT: We are back on the record. Because I don't know when we lost the people on Zoom if you would just ask that last question regarding the radius.

MR. PRICE: Yes.

Q I asked you to take a look at figure two, which is a picture of that radius and explain to us what it is?

A Yes. So the radius again is the center point which is -- you see that estimated latitude and longitude and the radius is drawn from that point outwards to create the map's display radius.

Q Google sometimes talks about a confidence interval or

confidence rating. Can you tell us what that means in this particular context?
A Sure. So it's their confidence as to how well they estimated this location of this device; so it would be the point in the center is the estimation and then that radius or confidence factor is this blue circle that is drawn around it.
Q What is the significance of 68 percent in this context?
A Google provided that it was their goal 68 percent of the time for the device to be located somewhere within this circle. After the estimated latitude and longitude used to locate the position and the display radius around it essentially what you're doing is just looking at the blue shaded area as the area where that falls within. You can kind of the forget that the center point is even there at that point.
Q So 68 percent confident that you're somewhere in that blue circle?
A Yes.
Q But not necessarily where that dot is right in the middle?
A You can remove that dot as you use the referent point to draw a display radius.
Q It's equally likely someone is off to the side as opposed to at the center?
A Absolutely. Anywhere within that circle. Center, outside, inner.
Q So 68 percent anywhere in that circle. What about outside of the circle?
A There would also be a chance.
Q 32 percent?

A Yes.
Q Let's take another look at the geofence. Here your report on page four -- hopefully we can get the visuals back up at some point, but we can use this for the moment. This is the red trapezoid is the geofence here. Can you tell us how many houses are within that geofence?
MR. SHANNON: I'll object. Just 352.
THE COURT: Sustained.
MR. SHANNON: Is the intention to move G into evidence?
MR. PRICE: I believe it has been moved into evidence.
MR. SHANNON: Has it already -- then yeah. 352.
THE COURT: Has G been moved in? Any objection to the admission of Exhibit G?
MR. SHANNON: None.
THE COURT: Exhibit G will be admitted, and that last objection is sustained.
(Defendant's Exhibit G received in evidence.)
Q The blue circle -- this is figure four in your report. Can you explain to us what that blue circle is?
A That's one of the data points from the location history information returned in stage one and you see the center point -- the estimated latitude and longitude with its 58 meters confidence interval or max display radius around it.
Q Do you know approximately how many homes are covered by that radius?
A I believe there were about 30.
Q Do you know about how many times larger that radius is than

the geofence?
A As far as the area that it covers it's about seven times larger than the geofence.
Q So seven times larger and 30 homes. We see that -- is it possible that that device would generate that radius was never within that geofence?
A That's possible. Yes.
Q What would you call that?
A It's a false positive.
Q Are you aware of false positives occurring in other cases?
A Very often.
Q So you'd say how often do they occur?
A You can generally find them in any set of data I'm provided.
Q Okay. I want to talk to you about the three stage one searches and specifically the time periods identified in the warrant.
THE COURT: Before you do, what specifically would be characterized as a false positive using the geofence and the radius? Something falling outside the geofence but something within the radius circle?
THE WITNESS: Right. If this device was located within that maps display radius but never entering the geofence, if Google estimates that its center point falls within that geofence, it will be returned responsive to the geofence even though it never entered.
THE COURT: Understood. Thank you. Understood.
Q We're back looking at the warrant here. We can go to page two of the warrant, Appendix A. Can you tell us the three time

areas.
A You've got 14:24 through 15:15. The second is 16:30 hours through 18:30 hours as well as 17:20 hours and 18:30 hours.
Q I want to go to the next page and look at Appendix B and tell me what the times are there?
A Period one is the same as well as period three, but period two has a different time frame.
Q How many minutes is period two in Appendix B?
A Thirty minutes.
Q How many minutes is in Appendix A?
A It would be two hours.
Q Two hours in appendix A. 30 minutes in appendix B. Can you tell from this warrant which time period the Court authorized?
A I guess both since they're both in the warrant.
Q Is it clear to you which time frame Google should follow?
A No.
Q Can you imagine a need to search time period three, which is completely encompassed by time three in Appendix B?
A Not as described in A. No.
Q Do you know what Google actually did here, what they produced?
A They produced periods one, two, and three as prescribed in Appendix A.
Q So they went for the two hours instead of the 30 minutes?
A Correct.
Q How do you know that?
A It's just based on the data. You can see the times and you see how long the data covers. They start at just after 16:30 and end right at 18:30.

Q Thank you. I want to talk about how to determine who's inside the geofence. That seems like a straightforward thing but not perhaps always. Could the police have requested data where the display radiuses were completely within the geofence. This is just a demonstrative?
A That can be.
Q Would that have likely reduced the number of false positives?
A Yes.
Q Would it have been reduced, the number of people who were --
A Many of those extended outside of the fence.
Q Did the police do that here?
A No.
Q Could the police have requested all the data where display radiuses just touch that geofence?
A I've seen that happen but yes. That can be requested, but it was not requested here.
Q Would that increase or decrease the number of false positives?
A That would definitely increase when you start merging the geofence with just the edges touching.
Q Would it increase or decrease the number of people, the step one?
A It would decrease.
Q The government did not do that here?
A They did not.
Q There's a third option here and that would be just returning data where the center point is inside that geofence?
A That's right.
Q Is that what the government did here?

A That's what was returned. Yes.
Q Where in the warrant does it specify how to count which devices are in the geofence?
A It doesn't.
Q And the warrant doesn't say one way or another between the points in the middle or the display radius being inside?
A No. It does not.
Q What happened after Google sent the step one data to law enforcement?
A So once step one is received law enforcement has to look at that day and begin to map this out so that you can see where the device IDs were located, what times showed up. Once that's done they look through that data and try to determine what's relevant to the investigation so that they can make the stage two request.
Q How many devices did the police say were relevant here?
A I believe there were six that made it to stage two.
Q Who got to decide what was relevant?
A The law enforcement officers who received that data would make that decision.
Q What happened after step two?
A So after step two again, now you receive that step two data which is now removing that geofence and expanding the time frame to where you can see these devices move about. So there's another decision made based on those movements or what they believe about the case to make the stage three request.
Q How many --
THE COURT: I'm going to interrupt you again. So just so

I'm clear you said that responsive to step one were nine devices, but law enforcement only followed up with six?

THE WITNESS: That's right. So nine were returned in step one. They asked for more information about six of those devices in step two.

THE COURT: That's one of my questions. The other question -- I want to go back to the geofence and the geometric area around it, and you said that it's possible to request data where the display radiuses are completely within the geofence. How does that happen?

THE WITNESS: So in the warrant it would need to be specified to only return to those users who the legally fell within that, but also their mass display radius does not exceed the geofence.

THE COURT: Okay. You can continue.

Q How many devices were unmasked in step three?

A Step three I believe one device was requested for subscriber information.

Q Who got to decide which device or devices would be unmasked in step three?

A Again, law enforcement's going to receive that step two data and make that decision as to how many devices they would like to get subscriber information for.

Q There's one more topic cover here. I want to come back to that 592 and the probable cause and the affidavit used to get it. There's generalizations about cell phone use that I want to ask you about. So could you turn to page 12 of the warrant and affidavit?

A Okay.
Q So after saying the people -- there's a claim about smart phone usage. Can you read the highlighted portion of what it says there? Can you read what's on the screen?
A Under the most common types of cell phones by the vast majority of people in the United States are smart phones.
Q Do you happen to know the percentage of people in America who own smart phones in October of 2018?
A For research with the census bureau about 84 percent of the nation.
Q 84 percent?
MR. PRICE: Your Honor, could I use that chalkboard for one second?
THE COURT: That one?
MR. PRICE: Just the bottom.
THE COURT: Sure.
MR. PRICE: We've got 84 percent of a smart phone, and now we move on in the warrant here.
Q Could you read the next highlighted line?
A Based on my training and experience I know the two most commonly use smart phone operating systems are ISO which are run on Apple phones and android which run on the mobile devices of various manufacturers.
Q Do you happen to know the percentage who owned android devices in 2018?
A For the statistics were about 46 percent were android users.
Q 46 percent. All right. And then can you read the next highlight line there?

A Therefore, it is nearly certain that a person using an android device has an associated Google account.
Q Do you agree with that?
A Yes. For the most part. Yes.
Q Is it necessary for an iPhone to have a Google account associated with it?
A No, it does not.
Q Remind us. Google only searches their data?
A Their location history of data.
Q What's the location of history?
A That would be 33 percent of their users use that service.
Q All right. If I ask you now what the probability is that a random American has a smart phone, that's an android with location history enabled in 2018, what's the probability?
A So obviously I'm not doing the math in my head now, but it's about 12 and a half percent.
Q There's a 12 and a half percent probability that a random person, perhaps the suspect in this case, would have all three things together?
A That's right.
Q The search of 592 million people was based off of a 12 and a half percent likelihood?
A Essentially yes.
MR. PRICE: Thank you. I don't have any further questions.
THE COURT: Cross-examination.

CROSS-EXAMINATION

BY MR. SHANNON:
Q Good afternoon. The search process that Google uses for the

592 million users to comply with requests like this, that process is automated; is that correct?
A The search of it.
Q Yeah.
A I would assume so. Yes.
Q Essentially there's no Google intern poring through all 600 million?
A They would still be there if that were the case.
Q Exactly. Once Google runs that computer algorithm against all 600 million people, it identifies which items are potentially within the geofence of those 600 million using this case as an example?
A That's right.
Q What that algorithm -- that all all having checked all those accounts it just then provides those nine anonymized accounts to the Google employee who's running the search?
A I believe that's correct. Yes.
Q Sort of the other side of that coin being when the Google employee runs that search they don't get -- the information that get back is -- anonymizes it in some way?
A Currently yes. They are anonymizing that information. As it stood in 2018 that device identifier that you're seeing is that user's device identification number for their account. They reference it as anonymized, but it is actually that device's real identifier. It would be simply to say the -- you know, it belongs to you. They came and tracked that specific device whereas now they have changed that very recently. They do assign a randomized number to each of those devices.

Q Understood. That number by itself can be -- that number is connected with some account, but there's no connection between the number that's provided and the account without doing an additional research?

A Right. Like you could either have Google go through and look at that day to determine who it belongs to or you can use the locations that it produces to then identify it.

Q Sure. And so those -- again keeping nine as an example that Google employee running the search would get those nine device identifiers back but wouldn't get any information about the other 590 whatever million devices that the algorithm checked against the geofence.

A Right. They're returning just those devices.

Q Okay. Then my other question was for the example about the radiuses that are all within the geofence that is going to be changing the radius of the device location. That's changing it from within 58 meters is also going to change the confidence interval associated with that device being within that now modified radius; correct?

A Yeah. I think actually what was being referred to there is instead of the way it was counted in this case was just kind of forget the radius but just where the dot lands. If the dot lands within the geofence, then it's responsive. That example was going towards if you only return those whose dot and radius were encompassed only within the geofence. That would reduce the number of users.

Q I understand, but that radius as you said was 58 meters; correct?

A You actually would be reducing any of the radius, but you would be telling Google to only respond with those radiuses that stayed within the geofence.

Q Sure. But if there was a geofence who by its shape and size, etc. a 58-meter radius circle could not fit entirely within that geofence then that's an impossible request; correct?

A It's not impossible. It just wouldn't be returned as responsive.

Q Sure.

A If that makes sense.

Q It does.

MR. SHANNON: That's all I have. Thanks.

THE COURT: It didn't make sense to me. Can you explain it again?

THE WITNESS: If we look at the geofence itself and we say if any dot falls within here, that's what happened, and now if we went with a step further, if the dot falls within here, we'll take it by itself -- map distance within the fence cannot break the boundaries. So, for example, that 58-meter that you see, that one would not be returned as responsive because obviously it exceeds the geofence even though its point falls within it's display radius exceeds that fence.

MR. SHANNON: May I ask a follow up question?

THE COURT: In a moment. The it you're referring to in the sense, the one that exceeds the geofence, wouldn't that be the false positive anyway?

THE WITNESS: It could be. Yes.

THE COURT: But it might not be.

THE WITNESS: It might not be.

THE COURT: All right. Explain further.

THE WITNESS: If you just look at that one single point, there's no way to fell if that one single point is a false positive. Through other vantage you will see -- for example I've had cases where you will see in step one the devices squarely within the geofence, but then when you receive the step two data you see this device travel, travel down the street passing by this location. It jumps in, jumps back out, and continues on, and when you look at the time period there you can tell there's no way that device stopped; but because of the way this estimation was made if it was an area was made that it fell inside, then it was returned as responsive.

THE COURT: Okay. Thank you.

BY MR. SHANNON:

Q So essentially if Google using a 58-meter radius with a 60 whatever -- 68 percent confidence interval -- for example, if you kept that 58-meter radius for the 68 percent confidence interval, if you were to ask -- if you were to send Google a geofence that was a 57-meter circle, it would return no hits whatsoever if you were specifying the entire radius had to be within the geofence?

A It may not. No.

MR. SHANNON: That's all.

THE COURT: Any redirect?

MS. VILLARAN: Just very briefly, Your Honor.

THE COURT: You may.

REDIRECT EXAMINATION

Q We've established that nine device IDs were returned, but still 592 million people were searched; correct?
A That's right.
Q And it would be the equivalent of every home in San Francisco was searched but only nine addresses were given to San Francisco Police Department still the case that every home in San Francisco was searched; right?
A I mean obviously the people are -- probably not 592 million homes here but yes. It would be that equivalent of searches, this broad search to get a smaller number.
Q Using the device IDs that were returned here could you issue a subpoena to Google with that device ID and get responsive information?
A Yes. I have seen where the further steps that are prescribed are skipped with subpoenas straight to Google for those device identifiers that they received.

MS. VILLARAN: Nothing further, Your Honor.

THE COURT: This is back when it was the -- before they made the change and now have completely random IDs?

THE WITNESS: Even with the completely random IDs, since Google can't identify obviously who the random ID is, this subpoena process still works. I believe it's used in times when more information is sought than what Google will say is reasonable on their end; so that is a work around to get that information. So instead of following the steps it kind of bypasses that and directly asks for the identifiers for the subscriber information for each one of those identifiers.

THE COURT: Didn't happen in this case, though?

THE WITNESS: It did not.

THE COURT: Any recross?

MR. SHANNON: No.

THE COURT: Let me just confirm I don't have any other questions. I believe -- I have another question that I think is a fairly basic question, but I would like it in the record. That is, you've explained how these searches work related to geofence and location history. How are they similar -- going to be a compound question and I'm going to overrule on the objection. How are they similar to and different from the cell tower dots?

THE WITNESS: I guess it is similar in terms of it is a request for unknown users by simply expecting that people use cell phones. The scope of that warrant is far smaller than the scope of a geofence warrant just because of the number of users that can be searched because obviously if you guys do a geofence or a cell tower dump in San Francisco and I'm back in Raleigh, you're not going to find me. I'm not here. It's confined to users in that specific area that have to be using those specific towers.

THE COURT: In that moment?

THE WITNESS: In that moment as well.

THE COURT: Would you also not be here for a geofence if you're back in wherever you said you were?

THE WITNESS: That's where the difference comes in here. Let's take for example -- let's say I do have an android phone with an account and Google location history. If I go home and you guys complete a search here, yes you do search my

information. That's the difference or if I take the trip to Europe and you guys do a search here in San Francisco, you're going to have to search my information to see who was responsive to your geofence here in San Francisco.

THE COURT: To state it a little differently the search is not based upon your location. Rather, if you have anything in your device that makes you part of the location history data.

THE WITNESS: Right, so if you were going to take that tower dump information and try to compare it to Google information, the opposite of what actually happens in a tower dump is who's in proximity to that tower using that tower. This would be hey, Verizon search all of your users to determine which of those users were using it instead of just those who actually use the tower. So it's you see where it would be. A much broader search then.

THE COURT: I understand.

MR. PRICE: If I may ask a follow up question.

THE COURT: You may. Just one moment. Any direct based on the Court's questions?

MR. PRICE: Yes. Just a couple of questions, Your Honor.

REDIRECT EXAMINATION

BY MR. PRICE:

Q To your knowledge when a cell phone company keeps records about phones connecting to towers, those are their business records; correct?

A They are business records; so those are used for billing their clients as well as there's many different reasons they retain.

Q Network optimization in particular. They need to know which

tower is doing what?
A They need to know -- yes. Generally how many people are using these towers as well as how that process is working. If calls are dropping, they're dropping, lose subscribers so keeping up with that information allows them to optimize that network.
Q So they have to be able to tell what each tower is doing and how many devices are connected to it; correct?
A That's again part of their business model is keeping up how well their network is doing.
Q Those business records about individual towers that get searched when a tower dump occurs; correct?
A That's correct.
Q To your knowledge does Google treat location history data like a business record?
A No. They have described it as your journal or journal entries for your data.
Q And do they store it the same way by general location?
A So no. In a -- consider for example in a tower dump record they are querying a specific tower for a specific time period to see which users are using it whereas Google is having to search all their users to determine who was there.
Q So Google can't do what the cell company does in terms of --
A Right. It's just not the same thing.
Q Thank you.
THE COURT: Mr. Shannon, any further questions?
MR. SHANNON: No.
THE COURT: Thank you for your time. You may step down. Any further witnesses?

MS. VILLARAN: Not from the defense, Your Honor.

THE COURT: Anything from the People?

MR. SHANNON: We do have a witness, Your Honor. Here he is. I told him we might be talking a break before we start.

THE COURT: I wanted to check in. How long do you anticipate the testimony to take?

MR. SHANNON: Direct will be 10, maybe 15 minutes.

(Off the record.)

(Back on the record.)

THE COURT: We are back on the record. Mr. Dawes is still present over Zoom and counsel are all present and Mr. Shannon you have a witness.

MR. SHANNON: I do. Sergeant fair.

THE COURT: Good afternoon. If you would come up to the witness stand, remain standing, and raise your right hand, please.

THE CLERK: Do you solemnly state under penalty of perjury that the testimony you are about to give in the matter now before this court to be the truth and nothing but the truth?

THE WITNESS: I do.

JESSE FARRELL,

called as a witness by the People, having been duly sworn, was examined and testified as follows:

THE CLERK: Please have a seat and state and spell your name for the record.

THE WITNESS: Jesse Farrel. J-E-S-S-E, F-A-R-R-E-L-L.

THE COURT: You may proceed.

MR. SHANNON: Thank you, your Honor.

DIRECT EXAMINATION

BY MR. SHANNON:

Q Good afternoon, Sergeant Farrell.

A Good afternoon.

Q Can you please tell the Court who you work for and what your position there is?

A San Francisco Police Department sergeant.

Q How long have you been a sworn peace officer?

A Twenty years.

Q Is all of that with the SFPD?

A Yes.

Q Can you describe -- let me start with this. In your current assignment you said sergeant of police in the burglary unit?

A Correct.

Q How long have you been in the burglary unit?

A Coming up on five years.

Q Safe to say that was your assignment back in 2018?

A Yes.

Q Up to 2018 -- well, at the time in 2018 did some of your job duties involve drafting and filing and executing search warrants?

A Yes.

Q Can you describe for the Court up until until 2018 what, if any, training and experience you had in drafting, filing, and executing search warrants?

A Up until 2018 I had a 40 hour course through the ICI -- I'm sorry. An 80 course in ICI which covered at least 10 hours of search warrant courses. I had a four hour search warrant prep

class. I believe at that time I had already taken a robbery and several other courses with the ICI that encompassed search warrants.

Q To clarify for the record can you explain what ICI is?

A It's the Institute of Criminal Investigation put on by the state as a post certified course. They have various investigation courses that cover the bases, which is an 80 hours from robbery to internal affairs to burglary.

Q Is it possible for you to estimate how many search warrants you had filed in the course of your various informations up until 2018?

A Maybe 300 to 400. Between that.

Q Now, you were assigned to investigate an alleged burglary in 2018 associated with case number 180808982; is that correct?

A Correct.

Q That's an alleged residential burglary at 1447 42nd Avenue?

A Correct.

Q As part of that investigation did you draft what's referred to as a geofence warrant?

A Correct.

Q Can you please tell the Court what that is?

A A geofence warrant --

Q Actually let me clarify the question. What you understood that to be at the time of the investigation in 2018.

A What I understood it to be during that time was a warrant drafted to a company and in this case Google which captures their ID numbers from cell phones in a particular area that you're requesting, and you can then research that data and find

out which cell phones were in that area.
Q Can you describe for the Court what sort of training and/or experience you had up to 2018 that informed your understanding of what a geofence warrant was and how it worked?
A So our geofence warrant was developed by our special investigations technical services unit. Lieutenant Tom McGuire and Officer *alameda lieu -- they developed the warrant with the help of Google. They then provided the training to the burglary unit and then during that time -- I don't know the specific date -- an employee of Google came out and gave further training.
Q Was there any -- just in a general way rather than related to this warrant, do you recall if there was any training or collaboration with either SFPD's legal team or the district attorney's office or any other body like that?
A Not to my knowledge.
Q Up until the point you drafted the geofence warrants in this case had you drafted any geofence warrants previously?
A Yes. I believe that was my third or fourth.
Q You don't happen to remember the date range of the ones that preceded this one, do you?
A I don't.
Q At the time the procedure you went through for preparing the search warrant in this case, did it defer in any substantial way from the ones you had done previously?
A No.
Q Had you prepared any geofence warrants prior to this one you took to a judge or magistrate that were not signed?

MS. VILLARAN: I'll object as to relevance.
THE COURT: Overruled.
THE WITNESS: Can you ask the question again?
Q Sure. Prior to the warrant at issue in this case any of the your geofence -- you had said you drafted three or four of them; is that right?
A Yes.
Q And they were not signed?
A No.
Q Bad question. Were any of your previous geofence warrants -- were all of your previous geofence warrants signed that you attempted to have filed prior to this one?
A Yes.
Q Were are all of those in San Francisco or other jurisdictions?
A All in San Francisco.
Q Back in 2018 at the time you prepared this one, what was the process for preparing your affidavit specifically related to a geofence warrant you wanted to have signed?
A You want to go through the process of me drafting the warrant?
Q Well, strike that. Is it safe to say that the features which make a geofence warrant unique are you have to select a geofence that is a physical area bounded by latitude and longitude and also a time frame for the warrant?
MS. VILLARAN: I'll object as to leading.
THE COURT: It is.
MS. VILLARAN: Move to strike.
THE COURT: I'm not going to strike the question. The question will stand, but there's no answer yet.

Q As far as your understanding of a geofence warrant, what are the features that would make it unique or distinguish it from other types of warrants?
A You would use map. So you take -- the short answer is you would take an area where the crime occurred and you would compile the information that you have using video, time frame, witness statements if you have any, and then you would compile that to an area where you believe the suspects are at and you would use the tools or Google maps and Google Earth and as the location we believe the suspects were and create the map from there, the geofence.
Q Is that map something you would include with that affidavit or with your warrant that you would bring to the judge?
A Yes.
Q I'm going to show you what's already been admitted as Exhibit D. Do you recognize what that is?
A I do.
Q What is that?
A That is the warrant I drafted for Google in relation to this case.
Q And the time and location boundaries that you were asking for, those in that warrant somewhere; is that right?
A Yes.
Q Where are they in Exhibit D?
A They're found in the actual search warrant and in the affidavit at the end.
Q I know that there are a couple of appendices, Appendix A, Appendix B which appear on pages three and four of Exhibit D.

Are those related to the time and location boundaries for the geofence warrant at all?
A Yes. Those are the maps I was referring to.
Q Understood. I'll take that back. And then once you're assuming that you got -- we can stick with this one actually. The geofence warrant in Exhibit D, this one was signed; correct?
A Correct.
Q So what was -- how did -- what was the process for these geofence warrants as you understood them once the warrant was signed? What was your next step?
A I provided it Officer Lieu. I explained their function earlier. He sent it to the Google portal.
Q You get the warrant signed and then Officer Lieu would serve it on the subject of the warrant?
A Yes.
Q What happened happen from there?
A Then it would be a specific time period. Google gets back. Officer Lieu gets the results. He then researches the results, provides results, his data. I then do my own research and go from there.
Q Are you aware the -- as part of the process that was developed between Google and the officers you described earlier, are you familiar with the process having a series of steps to it?
A Yes.
Q Can you describe those steps as they existed in 2018?
A So in 2018 you would get the information back. An officer would go through it. He would then ring me up, and we would go through it together. We would ask for further information based

on the information he got from Google as far as he would get a certain amount of ID numbers, and then he would look at the ID numbers. Ask for additional. Back then it was 45 minutes, and then Google would return that with the additional 45 minutes.
Q That would be a back and forth between you and Officer Lieu and Google; correct?
A Correct.
Q What would happen after that?
A And then Google would give the additional information that was requested, the 45 minutes of movement; then we determine if we see that one is likely to one or two or three or however many are likely to be the suspect or suspects.
Q Assuming there were one or more of the initial returns that you felt were the suspect, what would you do?
A Then you'd ask for that ID tag, ID number which is very specific to Google be unmasked.
Q In this case the one I guess ID tag was unmasked; is that correct?
A Yes.
Q How if it at all did you use that now unmasked ID tag in your investigation from that?
MS. VILLARAN: Objection. Relevance.
THE COURT: Overruled. You may answer.
THE WITNESS: So they provided me with email. It's been a while. I believe it's lacquandawes22@gmail.com was the owner of that ID tag, and then I did research on that.
Q When you say you did research did that involve any additional warrants?

A Yes.

MS. VILLARAN: Objection. Relevance.

THE COURT: It is moving beyond relevance of this hearing, but I will allow the last question and answer to stand unless you have an offer of proof.

MR. SHANNON: Well, Your Honor, I don't think it's any secret that the issue in this case is at which point in the process the 4th Amendment would require law enforcement to rather than on their own collecting additional information from Google go back to a judge or a magistrate for an additional warrant, and I believe this answer is relevant to that issue.

THE COURT: You may continue. You have that question and answer.

Q You did eventually seek another warrant based on the information that was unmasked in step three of the initial warrant?

A Yes.

Q Can you tell us about that, please?

A They provided me with --

MS. VILLARAN: Objection. Relevance it sounds like that satisfied Mr. Shannon was seeking. Additional warrants were sought that showed it is irrelevant to this hearing -- what they produced.

MR. SHANNON: Maybe I can rephrase.

THE COURT: You may.

Q Was there any information related to the unmasked ID tag, the lacquandawes@gmail.com -- was there any Google information you collected about that account without a second search warrant or

was all of the rest of the information you collected about that account subject or the result of an additional search warrant?
A So all from the geofence warrant I got was that email and then I wrote a second warrant to Google because that was the email they had and gmail is -- Google is the owner of gmail. In order to get any other information I had to write a warrant to Google for the gmail. If that makes sense.
Q I think that's sufficient. Since the time of this geofence warrant in 2018, has the process that SFPD uses to do these geofence warrants with Google -- has it changed in any way?
MS. VILLARAN: Objection. Relevance.
THE COURT: I'll allow it. You may answer.
THE WITNESS: Yes.
Q How?
A We now have more steps as far as the initial warrants. We used to ask for all the information in one warrant and then just go back to Google for the information to unmask the tag ID and just ask them for it. Now we we have to write a second warrant for that information.
Q Do you know why that change was made?
A Yes --
MS. VILLARAN: Objection. Speculation. Hearsay. Relevance.
THE COURT: Sustained on foundation at this point.
Q Were you -- do you know why that change was made?
A Yes.
Q Why was that change made?
MS. VILLARAN: Same objections, Your Honor.

THE COURT: At this point the objection's sustained.
Q How did you learn about why that change was made?
A I can't remember the exact date, but I believe it was a year later I had a geofence that I had to author. I brought it to Judge Begert. Judge Begert said he was okay with the warrant. However, he believed that the legality needed to write a second warrant to unmask the ID tag so we got together with the district attorney's office. They agreed; so as far as right now we have to write two warrants. The beginning warrant which we have there and then if we want more information we can get the 15 minutes of ID tags, but if we want ID tags or multiple ID tags to be unmasked, we have to seek a second warrant for that information.
Q When you said -- you said I had a warrant. Are you talking about a SFPD like the royal I?
A It was actually my case. I brought a geofence warrant to Judge Begert who then said he would not sign it unless it was a two step process, and so from that we just redeveloped our warrants. Because of that SID created a new warrant. We agreed on it and now we had a two step process.
Q Two step process to get to the unmasking?
A Correct.
Q Then if you wanted to get additional information -- well, actually strike that. Withdrawn.
MR. SHANNON: I think that's it, Your Honor. Let me just check one thing. Thanks, Sergeant Farrell. That's all.
THE COURT: Cross-examination.
MS. VILLARAN: Yes. Thank you.

CROSS-EXAMINATION

BY MS. VILLARAN:

Q I'm going to start on that last point that we just talked about, the warrant you brought to Judge Begert. He told you that the process you were using when you brought it to him was not legal in his opinion; is that correct?

A I don't know if he said it was not legal. He didn't like -- I don't know if he said it was illegal, but he did not like how we would just ask for the unmasking instead of getting a second warrant.

Q He didn't like SFPD interfacing with Google instead of involving a judicial officer again?

A Correct.

Q Based on that response the San Francisco Police Department counseled with the city attorney's; correct?

A I think we brought it to the city attorney's office. They wouldn't provide a definitive answer. We didn't go the DA's office; so we decided to go with Judge Begert's opinion.

Q So based off of that entire situation you decided to change -- you the San Francisco Police Department decided to change the entire way in which they executed geofence warrants; correct?

A I wouldn't say the entire way. It's just that one section; so if we wanted unmasking of an ID number, we'd have to get the second warrant.

Q The San Francisco Police Department no longer had discretion who to unmask; is that correct?

A We still asked for time frames. We don't ask for the unmasking. We get a second warrant.

Q So in the step one, two, and three process you now have to get a second warrant before step three or before step two?
A Step three.
Q But that was not the case in 2018 when you executed this warrant; correct?
A That's correct.
Q After the initial warrant there was no additional interaction with the judicial officer until after step three; correct?
A Correct.
Q When you prepared this warrant in October of 2018, San Francisco Police Department had no policies outside of their normal warrant policies for geofence warrants; is that correct?
A That's correct.
Q Meaning there was no written policy for how to properly secure a geofence warrant; correct?
A Correct.
Q And no internal memo for how to do this; correct?
A Yes.
Q Even no real established technique that had been vetted by the department or the city attorney's office or legal counsel on how to do this; correct?
A Correct.
Q And that's still the case today four years later; correct?
A Correct. There is no policy for geofence.
Q And prior to authoring this warrant you had received no official training put on by the San Francisco Police Department on geofence warrants; is that correct?
A Correct.

Q So nothing like the ICI training that you were telling us about before; correct?
A Correct.
Q So the 14 hours that you had said were dedicated to search warrant trainings, that 14 hours did not include geofence warrants; correct?
A That's correct. That was way before geofence warrants were around.
Q You mentioned that Lieutenant McGuire and Officer Lieu worked with the burglary unit to provide some information about geofence warrants; is that correct?
A They work -- well, Lieutenant McGuire but they work for the special informations technical unit and they provide training to people in the burglary unit.
Q For you that training comprised of about 45 minutes conversation in Officer Lieu's office; correct?
A Correct.
Q So it wasn't official training put on where multiple officers attended and several hours. It was just going to Officer Lieu's office for 45 minutes?
A That's correct.
Q The only people present were yourself, Officer lieu, and Lieutenant McGuire; correct?
A Correct.
Q This is when Officer Lieu gave you a warrant template for the geofence warrants; correct?
A Correct.
Q And that is the template that you used in this particular

case; correct?
A That's correct.
Q So the language that we see in the search warrant and the appendix and the affidavit is not language that you drafted yourself; correct?
A That's correct.
Q You plugged in the coordinates for this time frame in this case, but otherwise it was preprepared; is that right?
A Along with my actual affidavit. That is correct.
Q You also tell us on direct Google came and trained you at some point, but that was after you had executed this warrant; correct?
A Like I said, I don't remember the time frame when Google came out. It was years ago. I don't know if it was before or after this.
Q Do you recall having a conversation with the district attorney Biana Calderon-Penaloza back in October of last year?
A No.
Q Would it refresh your recollection if I showed you a proposed affidavit that she had worked with you on that was potentially going to be submitted to this court?
A Sure.
MS. VILLARAN: May I approach, Your Honor?
THE COURT: You may. Have you seen this?
MR. SHANNON: No.
THE COURT: Why don't you show it to the district attorney first.
Q Sergeant, would you mind looking at just the top of this page

here, items 1 through 13?
A Okay.
Q Does this look like an affidavit you would have worked on with a district attorney in terms of your training and experience?
A It does.
Q Do you see item number seven there?
A Yes.
Q Does that refresh your recollection on when you received the training from a Google employee?
A Yes.
Q Was that before or after the execution of this warrant?
A This says after.
Q So prior to this warrant the only sort of unofficial information or conversation you had about geofence warrants was that 45 minutes in Officer Lieu's office?
A Correct.
Q Now, as you were using this template to prepare the warrant you did not have any known suspects, correct, in this particular case?
A Correct.
Q There were two people that you had seen on surveillance footage; correct?
A Yes.
Q You had a general physical and clothing description of those people that you believe were involved; correct?
A Correct.
Q But you had no information on who those two people were at the time you authored this warrant; correct?

A Correct. Yes.
Q You had sent crime bulletins and information to not only the San Francisco Police Department, but nine Bay Area law enforcement agencies; correct?
A Correct.
Q At the time you authored this warrant you had not received any response back about the potential identity of those two people; correct?
A I believe so. Yes.
Q And similarly using video there were two different cars you suspected were involved in this burglary; correct?
A Correct.
Q But beyond general make and model you had no identifying information about the cars; correct?
A Correct.
Q No license plate numbers for example?
A That's correct.
Q And no person associated with either car; correct?
A Correct.
Q So the only way you ever associated Mr. Laquan Dawes with this case was through this geofence warrant?
A That's correct.
Q You presented this warrant to the Honorable Judge Bolanos; is that correct?
A Correct.
Q And the materials that you presented her with were just what has been marked as I believe Defense D; correct? Let me present you with a copy of what's been marked as Defense D. You want to

take a moment to just scan those?

THE COURT: You may continue.

Q So Defense D is what you presented Judge Bolanos; correct?

A Correct.

Q In this affidavit you never explain that when Google executes a geofence warrant it searches 592 million people; correct?

A Correct.

Q You didn't tell her that it requires conducting a search of every single person who has location history enabled; correct?

A Correct.

Q You knew that the geofence area that you were requesting was for a residential area; correct?

A Correct.

Q You also did not inform Judge Bolanos that because of margin of error the geofence radius is actually much larger than what you drew in your attached map; is that correct?

A Correct. I did not inform her of that.

Q I think we've established this, but to make clear the initial representation of this warrant on December 4th of 2018 to Judge Bolanos was the last time you interacted with her over this particular warrant; correct?

A That's correct.

Q In the affidavit for this warrant there's no indication that any of the suspects had a cell phone; correct?

A Correct.

Q Nothing in the warrant mentions that the suspect --

MR. SHANNON: I sense we're getting maybe near the end, but I think I'll object as 352 because the warrant is what the

warrant is.

THE COURT: Overruled.

Q Nothing in the warrant indicates that the suspect had a Google account; correct?

A Correct.

Q Nothing in the warrant indicates that the suspects had location history enabled; correct?

A Correct.

Q Essentially your logic was that suspects are people and people tend to have cell phones; correct?

A Correct.

MS. VILLARAN: If I could have a moment, Your Honor.

THE COURT: You may.

MS. VILLARAN: I don't have any further questions at this time. Thank you.

THE COURT: Any redirect?

MR. SHANNON: No.

THE COURT: Court has some questions. Do you still have Exhibit D in front of you?

THE WITNESS: I do.

THE COURT: Exhibit D has two appendixes. Appendix A and Appendix B. Do you see that?

THE WITNESS: I do.

THE COURT: Why is the time period in Appendix A, time period two, different from the time period in Appendix B?

THE WITNESS: Let me see. I don't know. I've never seen that. I didn't know notice that. I'd have to look back through my CHRON, go through the time periods specifically. Could be an

error because they should be -- I'd have to exact time. This is like three years, four years old so I'd have to look into it. Could be an error.

THE COURT: Okay. Another question I have is in terms of Appendix A, the location. You decided upon a particular geometric shape.

THE WITNESS: Correct.

THE COURT: How did you decide on that geometric shape?

THE WITNESS: When we talked with Officer Lieu and we talked about the best way to narrow it down, we went through where we see the cars parked at intervals and through the house. It's hard to tell on this warrant. The house goes through here so we captured the house.

THE COURT: When you say the house goes through here.

THE WITNESS: When you see 1447 42nd Avenue the triangle goes through that house and then you can see where the initial car pulled up, where the two locations of the car if I remember remember the warrant correctly from the two different time periods. The car parked here are suspect vehicles so we made a triangle. Does that make sense?

THE COURT: It does. It's somewhat trapezoidal?

THE WITNESS: Yes.

THE COURT: Would it have been possible to have narrowed the trapezoid to encompass only the house that had been burglarized?

THE WITNESS: Yes. That would have been possible, but based on my training and experience and time now, the drivers of the get away vehicles rarely get out of the car; so we wouldn't capture the driver. If I just put the suspects that went into

the house.

THE COURT: I guess my question's different. Would it have been possible to create a geofence that encompasses the entirety of the street area but only in terms of residences, the burglarized house?

THE WITNESS: Yeah. I can make -- Officer Lieu and I can make that included in the warrant. We can narrow that down.

THE COURT: I was just curious. Just so this is clear when you were talking about the residence, this is in the Sunset District?

THE WITNESS: Correct.

THE COURT: The residential.

THE WITNESS: The Terraval. It's weird to say this now, but it's pre-pandemic 2018.

THE COURT: Yes. I think I know the answer to this, but why did you request the times that you chose?

THE WITNESS: Those were based off surveillance video and times of the report.

THE COURT: When the first set of data information comes in from Google and you said that you and I think it was Officer Lieu do research on it, how was that research conducted?

THE WITNESS: It comes in raw data and we have a mapping system called CellHawk which we use to map out suspect's phone numbers and locations. It will also take the Google data. Instead of us sitting there with a pen and paper it will completely upload into the system and put it on a map for us.

THE COURT: And from the nine you originally received, how did you narrow down to six for further information?

THE WITNESS: We ask for 15 minutes before and after and then from there you narrow it down and then Officer Lieu was able to identify one tag that matched the suspect's movements.

THE COURT: You identified that one tag because of the movement?

THE WITNESS: Correct.

THE COURT: You indicated three different times. Were any of the six in the geofence area more than one of the three times? Do you understand what I'm asking?

THE WITNESS: You're asking if I could just restate it were any of those tags in there all three times.

THE COURT: Yes.

THE WITNESS: I don't believe so. I'm not a hundred percent. It's been years, but I don't believe so. It's why we eliminated those. I have to look at the raw data.

THE COURT: You were able to determine the path of travel from the data?

THE WITNESS: Correct.

THE COURT: And what did the path of travel allow you to conclude, if anything?

THE WITNESS: Well --

MS. VILLARAN: I'll object as to relevance.

THE COURT: I'll sustain it. Let me look if I have any others. Ms. Villaran asked you a number of questions about what you included in your affidavit. One of them was you didn't tell Judge Bolanos that it required conducting a search of every single person who has location history enabled, and you said that's correct. Your affidavit didn't contain that information.

Were you aware of that information?

THE WITNESS: My training up to that point only talked about what we were asking for in the specific area; so I wouldn't have told her they collected everybody's data. Does that make sense?

THE COURT: No. Say it again.

THE WITNESS: When I ask for a geofence it will collect everybody's cell phone from that area.

THE COURT: Did you know at the time of the affidavit that because of the margin of error the geofence radius was actually much larger than what you drew in the attached map?

THE WITNESS: No.

THE COURT: I think that's all of my questions. We will return to Mr. Shannon to see if you have any questions based on the Court's questions.

MR. SHANNON: I do not.

THE COURT: Ms. Villaran, do you have any questions based upon the Court's questions?

MS. VILLARAN: I may. Just one moment, please.

THE COURT: Of course.

RECROSS-EXAMINATION

BY MS. VILLARAN:

Q Start with a quick clarifying question. You said when the Court asked how you narrowed it down from nine devices to six, you said you asked for an additional 15 minutes, but in this warrant you asked for 45 minutes, correct?

A I made a mistake. The new warrants are 15. The old warrants are 45. I apologize.

Q In addition to requiring a second warrant for step three, the

new warrant process also limits the additional amount of time you can ask from 45 to 15 minutes; correct?
A Correct.
Q And the judge also asked you whether any of the six devices were in the geofence area at all three times. Do you recall that?
A Yes.
Q You recall that the device ID associated later allegedly with Mr. Dawes was also not in the geofence at all three of those time periods; correct?
A I'm sorry. Could you ask that again?
Q Do you recall that the raw data showed that the device ID associated allegedly with Mr. Dawes was not in the geofence area at all three of the time periods listed in either Appendix A or Appendix B; correct?
A Yes, that's correct.
Q That device ID was only in the final time frame listed in Appendix A?
A Yes. When Mr. Dawes pulled up to the scene.
Q That's when you you believe that device ID was in that area; correct?
A That ID was in that area.
Q The Court asked you whether you knew that all devices with location history enabled were going to be searched for this type of warrant, and you said at the time your training had not told you that; correct?
A Correct.
Q That's just the 45 minute conversation you had with Officer

Lieu in his office?
A That's right.
Q You told us on direct that you've done about 300 to 400 search warrants prior to 2018?
A Yes.
Q You would agree that it's your obligation to understand the nature of the search that you're asking to conduct; correct?
A That is correct.
Q Is it your routine and practice to file warrants you don't understand?
MR. SHANNON: Objection. Argumentative.
THE COURT: Rephrase.
Q Would you agree it's your responsibility when you ask a judicial officer to authorize a warrant that you understand what it is exactly that you're asking for?
A Yes.
Q In this case you did not understand what you were asking for; correct?
MR. SHANNON: Well, objection. Misstates the evidence and assumes facts not in evidence.
THE COURT: Objection's overruled. You may answer.
THE WITNESS: Ask the question again.
Q In this case you did not understand that what you were asking for was to search 592 million people; correct?
A Correct.
Q You did not understand what you were asking for was to search radius or area much larger than the actual geofence that you drew with Officer Lieu; correct?

A Correct.
Q Because at that time you didn't understand how the geofence warrant process actually worked; correct?
MR. SHANNON: Objection. Misstates the evidence and assumes facts not in evidence.
THE COURT: Overruled. You may answer the question.
THE WITNESS: I had training for that Google warrant. Is that what you're asking?
Q At the time you authored this warrant in 2018 before you got the training from the Google employee, you didn't actually understand the process that Google goes through to execute a warrant of this nature; correct?
A I would say that's correct. Yes.
ATTORNEY2: Nothing further.
THE COURT: Re-redirect.
MR. SHANNON: No.
THE COURT: Thank you for your time. You may step down. Do you have any further witnesses?
MR. SHANNON: No.
THE COURT: Both sides then rest?
MR. SHANNON: Yes.
MS. VILLARAN: Yes, your Honor.
THE COURT: We discussed the other day when we were having a conversation as to whether this hearing could actually occur given Mr. Dawes's current condition and given Mr. Shannon may be being in trial as to whether or not I said to you that I was going to offer up to you the opportunity to write a closing brief if you were seeking such an opportunity. That's still my

intention if you are seeking to have that opportunity. I was not intending on ruling from the bench today. There's a lot to pore over. Not in terms of case law. That's for sure but in terms of this case. I am likely going to write a written opinion/order.

What I would like to know from you all is do you want an opportunity to make simply an argument or would you like to have an opportunity instead and it's one or the other -- I'm not going to do both -- have a closing brief? Or submit a closing brief I should say.

MR. SHANNON: I think we'd like the chance to make a closing either argument or brief. My understanding of Your Honor was kind of enough to indicate your intention to us before we went on the record today. Based on that conversation my understanding was that we would not be doing an oral argument today so I don't necessarily have a preference one way or the other about oral argument or written just as long as I'm not prepared to give oral argument today.

THE COURT: Do you have a preference?

MS. VILLARAN: Would the Court permit -- since it's our motion would the Court permit us to respond to the People's brief? Because I think if it's an oral argument where we would have the opportunity to after the People's oral argument.

THE COURT: That's a reasonable request.

MS. VILLARAN: Then I would want to do it orally.

THE COURT: I would permit that yes.

MR. SHANNON: I would like it reverse since it's their motion. It's fine. Whatever.

THE COURT: In which case simply -- I would simply do oral argument.

MS. VILLARAN: Then you can tell us to stop.

MR. SHANNON: Written's probably best.

THE COURT: Let's go off the record.

(Off the record.)

(Back on the record.)

THE COURT: After discussions off the record it's my understanding that counsel have agreed to a few things. One, there's going to be a request for a transcript, and it's expected the transcript will be made available by June 10th. Counsel will submit any closing briefs you seek to have filed and served no later than June 24th. And then, Ms. Villaran, if you want to file any response brief to the People's, that needs to be filed and served no later than July 1st.

MS. VILLARAN: Understood and agreed.

MR. SHANNON: Understood and agreed.

THE COURT: At that point the Court will be taking the matter under submission as of July 1irst close of business. We still need a control date.

MR. SHANNON: Mr. Geneson is on Zoom. Is that when we ask him to join us again?

THE COURT: Let's go off the record again.

(Off the record.)

(Back on the record.)

THE COURT: The matter will be continued to July 15th in this department at 9:00 a. M. both matters for status of the Court's ruling and Mr. Dawes and Mr. Odom's appearance be waived

so long as you remain in good contact with your clients. Thank you.

MR. SHANNON: Thank you.

THE COURT: Anything further then?

THE CLERK: Exhibits.

THE COURT: Oh, the exhibits. I just want to for housekeeping purposes every exhibit that was marked was admitted.

MR. SHANNON: Correct.

MS. VILLARAN: That's my understanding. Yes.

THE COURT: The Court has a courtesy copy of the set of exhibits so I think that's -- off the record.

(Off the record.)

(Back on the record.)

THE COURT: That completes the matter.

(Whereupon proceedings concluded.)

State of California)
)
County of San Francisco)

I, DIANA PAQUETTE, Official Reporter for the Superior Court of California, County of San Francisco, do hereby certify:

That I was present at the time of the above proceedings;

That I took down in machine shorthand notes all proceedings had and testimony given;

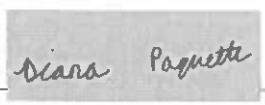
That I thereafter transcribed said shorthand notes with the aid of a computer;

That the above and foregoing is a full, true, and correct transcription of said shorthand notes, and a full, true and correct transcript of all proceedings had and testimony taken;

That I am not a party to the action or related to a party or counsel;

That I have no financial or other interest in the outcome of the action.

Dated: June 14, 2022



DIANA PAQUETTE, CSR No. 14192

Proof of Service

I say:

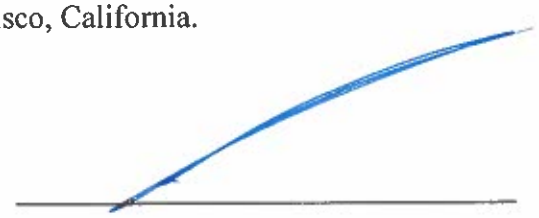
I am over eighteen and not a party to the above action. My business address is 555 Seventh Street, San Francisco, California 94103.

I caused to be served copies of the attached Opposition to Motion to Quash, by transmitting via my electronic service address (sierra.villaran@sfgov.org), to the persons at the email addresses set forth below:

Lawrence DeSouza
San Francisco District Attorney
350 Rhode Island Street
North Building, Suite 400N
San Francisco, CA 94103

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 6, 2022, at San Francisco, California.



Sierra Villaran