

ENDORSED
FILED
Superior Court of California
County of San Francisco

SEP 30 2022

CLERK OF THE COURT
BY: MOHAMMED ASHRAF
Deputy Clerk

SUPERIOR COURT OF CALIFORNIA
COUNTY OF SAN FRANCISCO
Dept. 23

THE PEOPLE OF THE)
STATE OF CALIFORNIA)
)
Plaintiff)
)
v.)
)
LAQUAN DAWES)
)
Defendant)

Court No. 19002022
SW# 42739

ORDER GRANTING MOTION TO
QUASH GEOFENCE SEARCH
WARRANT

INTRODUCTION

The Fourth Amendment to the United States Constitution guarantees to the people the right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” (U.S. Const. 4th Amend.) To that end, the Framers prohibited the issuance of a warrant, unless that warrant was based “upon probable cause” and unless it “particularly describ[ed] the place to be searched, and the persons or things to be seized.” (*Ibid.*) The Supreme Court of the United States has since applied the principles embodied in this language to rapidly evolving technology—from recording devices in public telephone booths (*Katz v. United States* (1967) 389 U.S. 347)—to thermal-imaging equipment (*Kyllo v. United States* (2001) 533 U.S. 27)—and, most recently, to cell-site location data (*Carpenter v. United States* (2018) 138 S. Ct. 2206).

Law enforcement is increasingly relying on a novel technological technique—geofence warrants—to investigate crimes with no readily identifiable suspect. These geofence warrants,

1 also referred to as “reverse-location” warrants, aid law enforcement in identifying an unknown
2 suspect by obtaining geolocation data of all electronic devices at the location, on the date and at
3 the time of the criminal activity. A geofence is a virtually bound geographic area and a geofence
4 warrant captures all the users located within that area during the time period specified.

5 In the instant case, Laquan Dawes (“Defendant”) asks this Court to quash the geofence
6 search warrant issued that authorized law enforcement to search and seize his geolocation data
7 that ultimately implicated him in a crime.¹ (Pen. Code, § 1538.5.) He contends that under the
8 Fourth Amendment to the Federal Constitution, he has a reasonable expectation of privacy in
9 geolocation data, thereby requiring a search warrant for law enforcement to obtain such data. He
10 further argues that under the California Electronic Communications Privacy Act (hereinafter,
11 referred to as “CalECPA”), state law requires a search warrant for this particular data.

12 At the same time, Defendant challenges the *validity* of the geofence search warrant
13 obtained in this case that ultimately implicated Defendant as a suspect of a residential burglary.
14 Specifically, Defendant argues that the geofence search warrant issued in this case lacked
15 particularity, was overbroad, and divested too much discretion to law enforcement rendering it
16 akin to a general warrant and in violation of Fourth Amendment principles.

17 Defendant also argues that the geofence search warrant, as drafted, violated California
18 statutory authority as prescribed under CalECPA. Defendant asserts that CalECPA requires law
19 enforcement to specify, among other things, the targeted individual or account.

20 Defendant finally argues against the application of the good faith doctrine in this case.
21 Defendant argues that because there is a statutory violation under CalECPA, the Court is barred
22 from extending the good faith doctrine to a violation of CalECPA.

23 The Court has reviewed all the moving papers, exhibits, and documents filed in this
24 matter. The Court has also considered the testimony provided by witnesses at two evidentiary
25 hearings before this Court, and the stipulated testimony from witnesses who testified in *United*

26
27 ¹ A “presumption of validity” exists “with respect to the affidavit supporting the search warrant. (*Franks v Delaware*
28 (1978) 438 U.S. 154, 171.) Defendant Dawes moves only to quash and not traverse the search warrant, as he has not
challenged the statements made by the affiant officer in support of the search warrant; rather the challenge avers that
such statements, even if true, do not provide sufficient information to support a search warrant. Therefore, the Court
relies, in part, on those statements in the affidavit and in addition to the testimony offered at the evidentiary hearing.

1 *States v. Chatrie* (E.D. Va., Mar. 3, 2022, No. 3:19CR130) 2022 WL 628905 (hereinafter,
2 “*Chatrie*”), a federal district court case addressing the constitutionality of a geofence search
3 warrant.

4 The Court issues this written order not only to address the warrant challenged in this case,
5 but also to provide a framework for analyzing future search warrant applications involving
6 geofence technology. For the reasons set forth below, the motion to quash the search warrant and
7 motion to suppress the evidence are **GRANTED**.

8 9 **PROCEDURAL HISTORY AND FINDINGS OF FACT**

10 11 **I. PROCEDURAL HISTORY**

12 The People charged Defendant in a two-count felony complaint of first-degree burglary
13 (Pen. Code, § 459; Count I); and (2) grand theft of personal property (Pen. Code, § 487, subd.
14 (a); Count II). Arraignment occurred on February 13, 2019, at which time Defendant pleaded not
15 guilty to all the charges and allegations. On or about June 9, 2020, Defendant filed the
16 underlying Motion to Quash and Suppress pursuant to Penal Code sections 1538.5 and 1546.²

17 On October 4, 2021, the Court conducted an evidentiary hearing, limited in scope as to
18 whether Defendant had a reasonable expectation of privacy in his geolocation data and, thus,
19 whether a search warrant was required. (Volume 1, Reporter’s Transcript (hereinafter “Vol. 1,
20 R.T.”) 6:6-18; 86:26-87:2.) At the conclusion of the limited hearing, the Court found no need to
21 address the Fourth Amendment issue because the State Legislature already determined that this
22 type of data required a search warrant, pursuant to the CalECPA (Pen. Code, §§ 1546-1546.4).
23 (Vol. 1, R.T. 87:19-89:15.) Further, law enforcement had, in fact, proceeded by way of search
24 warrant.

25 On May 26, 2022, the Court conducted a second evidentiary hearing as to whether the
26 geofence search warrant in this case was sufficiently particular and not overly broad under the
27 Fourth Amendment to the Federal Constitution and under CalECPA. (Volume 2, Reporter’s

28 ² Although Defendant Dawes has a co-defendant in this case, Alphonso Odom in Case No. 19002037, only
Defendant Dawes moves to challenge the geofence search warrant.

1 Transcript (hereinafter “Vol. 2, R.T.”) 4:4-26.) The parties were invited to file additional
2 briefing. Defendant filed an additional brief; the People declined. The Court also received in its
3 filings an amicus brief from the Electronic Frontier Foundation, and a copy of Google’s amicus
4 brief filed in *Chatrie*. The Court took the matter under submission on July 15, 2022, to issue a
5 written order.³

6 In each hearing, the Court heard testimony from the defense expert witness, Spencer
7 McInville. The parties stipulated to McInville’s expertise as a digital forensics examiner,
8 which included “the education and methods of extracting information from mobile devices.”
9 (Vol. 1, R.T. 9:5-19.). By the second evidentiary hearing, the parties stipulated to the admission
10 of certain declarations and prior testimony offered in *Chatrie, supra*, 2022 WL 628905 by two
11 Google employees, Sarah Rodriguez and Marlo McGriff, as well as Spencer McInville. The
12 Court also received into evidence an additional declaration by Emily Moseley, a Google
13 employee.

14 15 16 **II. FINDINGS OF FACT**

17 **A. The Underlying Crime and Initial Investigation**

18 **1. The Residential Burglary**

19 The following facts are derived from the search warrant and attached documents in
20 Exhibit D. On October 24, 2018, at approximately 11:46 pm, San Francisco Police Department
21 (“SFPD”) officers responded to a report of a burglary at a residential home.⁴ Officer Ramirez
22 met with the victim, Lai Pham, who was the resident of an in-law suite at that location.

23 Pham told police that his unit had been broken into by three unknown suspects. He stated
24 that he left his unit at approximately 9:00 am (900 hours) on October 24, 2018, from the ground-
25 level side front door. When leaving, he locked his unit and left for work. Pham later returned

26 ³ Any citations to the exhibits admitted into evidence in this Order are in the same sequence as admitted during the
27 evidentiary hearings and as reflected in the reporter’s transcripts. To avoid confusion, the Court does not rely on the
28 exhibit identification sequence as presented in the briefs, as some exhibits may have been submitted there with a
different exhibit identification.

⁴ The Court notes that there was a specific address identified in the warrant that law enforcement responded to, but
for purposes of this Order to protect the privacy of the victim, the specific address is omitted.

1 home at around 3:30 pm (1530 hours). At that time, “he observed a black male adult,
2 approximately 25 years old, wearing a white T-shirt and red/black sweatpants in the vicinity of
3 his residence.” Pham did not notice anything out of the ordinary and went into his home.

4 About five minutes later, around 3:35 pm (1535 hours), Pham locked his unit and left his
5 home again. Pham returned home at around 6:45 pm (1845 hours) and saw that his front door
6 had been kicked in. Fearing someone may still be inside, Pham contacted the police. While
7 waiting for them to arrive, Pham spoke with his neighbors and obtained surveillance footage of
8 the suspects who broke into his unit.

9 When law enforcement officers arrived, Pham conducted a walk-through of his home and
10 discovered that his MacBook Pro laptop and a black digital combination safe had been stolen
11 from his bedroom. The combination safe, which contained \$9,000 in cash and two vehicle keys,
12 was pried from the wall inside his bedroom closet. Pham showed the police the video he had
13 obtained from his neighbor.

14 15 2. The Surveillance Video Footage

16 Sergeant Jesse Farrell, who at the time had been employed with San Francisco Police
17 Department for 16 years, was the investigating officer who drafted the search warrant at issue in
18 this case. During the investigation, he personally reviewed the surveillance footage that was
19 collected. From one neighbor, police received a total of seven video clips.

20 Sergeant Farrell described his observations of the surveillance footage as follows: On
21 October 24, 2018, at 2:59 pm (1459 hours), a black male suspect exited out of the rear passenger
22 seat of an Acura TL, 4 door, dark color vehicle. This suspect is identified in the affidavit as
23 Suspect #1, and is described as a tall, thin, Black male with short hair and a beard wearing a
24 white T-shirt, red and black pants, with the shin and ankles covered in white. The suspect walked
25 toward the front door of Pham’s residence. A minute later, at 3:00 pm (1500 hours), Suspect #1
26 walked away from Pham’s residence, returned to the Acura TL and entered it.

27 Later, at 4:42 pm (1642 hours), another suspect walked on the sidewalk toward Pham’s
28 residence. This suspect is identified in the affidavit as Suspect #2, and is described as shorter

1 than Suspect #1, heavysset, wearing black and red pants, with shin and ankle covers in black
2 material, and a white and gray striped sweatshirt with a hood over his head. Later, at 5:43 pm
3 (1743 hours), Suspect #2 is again observed on video, exiting from the rear passenger door of a
4 dark colored Honda vehicle. A third suspect, who remained undescribed, could be seen at 5:53
5 pm (1753 hours).

6 At 6:06 pm (1806 hours), Suspects #1 and #2 exit from the back seat of the Honda and
7 walked toward Pham's residence. Suspect #1 is described in the affidavit as wearing the same
8 pants as before, but now also wearing a dark colored jacket with the hood pulled over his head.
9 At 6:09 pm (1809 hours), both suspects can be seen in the video walking back and forth from
10 Pham's house to the parked Honda while carrying items and putting them into the car. The
11 Honda was recorded leaving the scene at 6:11 pm (1811 hours).

12 Sergeant Farrell could not recognize the suspects from the surveillance footage, and the
13 vehicles in the footage did not display any identifying information, such as a license plate
14 number. (Vol. 2, R.T. 55:21-56:19.) Sergeant Farrell sent a crime bulletin to nine Bay Area law
15 enforcement agencies but had not heard back by the time he authored the geofence warrant
16 affidavit. (Vol. 2, R.T. 56:2-9.) Sergeant Farrell applied for a geofence search warrant in an
17 effort to identify the burglary suspects through Google's location history tracking services.

18
19 **B. Testimony Regarding Google's Collection of Geolocation Data Through Its**
20 **Location History Feature.**

21 The geofence search warrant sought by Sergeant Farrell ultimately requested Google to
22 turn over responsive geolocation data. Our record reflects that Google collects detailed location
23 data on numerous tens of millions of its users and stores this data through the following services:
24 (1) Location History, (2) Web and App Activity, and (3) Google Location Accuracy. (*Chatrie*,
25 *supra*, 2022 WL 628905, at p. 3.) In responding to a geofence search warrant, Google only
26 reviews and provides law enforcement with geolocation data from Google users' Location
27 History service. (*Ibid.*) Additionally, the return to the geofence search warrant in this case
28 yielded data corresponding only to Google's Location History feature.

1
2 1. Google's Location History Feature Collects Users' Geolocation Data.

3 Google's Location History feature is a service provided to Google users that allows them
4 to access, maintain, and view their historical locations.⁵ (*Chatrie, supra*, at p. 3; Vol. 2, R.T.
5 10:20-28.) Google users access this data through the Timeline feature, which depicts a user's
6 Location History data points over time so that users can "keep track of locations they have
7 visited while in possession of their mobile device."⁶ (*Chatrie, supra*, at p. 3 [internal quotes
8 omitted]; Vol. 1, R.T. 14:24-15:3.) For example, a user can observe their visit to a ski resort and
9 their travel to that ski resort from their hotel. (McGriff Dec. p. 2, ¶ 5.) Google users can access
10 and review their Google Timeline through certain applications ("apps"), such as a Google Maps
11 app. (Vol. 1, R.T. 10:19-24; 48:16-28.)

12 To collect Location History data, Google uses several sensors in an electronic device to
13 locate and track it, such as the Global Positioning System ("GPS"), cellular location information
14 from nearby cellular towers, Wi-Fi networks, and Bluetooth beacons. (Vol. 1, R.T. 10:14-18;
15 *Chatrie, supra*, at p. 3.) Google's geolocation data gathered through the Location History feature
16 is the locating of a device user's location through those sensors. (Vol. 1, R.T. 11:13-17; 14:6-23.)
17 Because a user's device is "out and about" during travel, the device determines its locations
18 based on the services and features that are enabled and reports it back over the cellular network
19 to Google who then stores the data in the user's Google account. (Vol. 1, R.T. 11:18-23; 14:20-
20 23.) In some instances, Google's estimation of a device's location may include an estimate of
21 where a device is in terms of elevation. (*Chatrie, supra*, at p. 3.) For example, Location History
22 has the capability to determine if a user is on the second floor of a mall. (*Ibid.*)

23 According to McInville, geolocation data is routinely collected from those sensors at
24 certain intervals, about every two minutes, but the intervals can fluctuate. (Vol. 1, R.T. 12:2-11;

25 ⁵ While a service for users, Google also uses Location History for advertisement purposes. (*Chatrie, supra*, at p. 3.)
26 Without identifying a specific user, this feature can be used to identify the number of users exposed to a specific
27 business advertisement who then visited that business' establishment. (*Chatrie, supra*, at p. 3; Vol. 2, R.T. 10:28-
28 11:2.) These advertisements may be shown to a user across different apps; for example, a user who traveled to a ski
resort may see an ad for ski equipment while watching YouTube videos. (McGriff Dec., p. 4, ¶14.)

⁶ Google's Location History feature also provides other benefits to users. For example, those who opt in can "obtain
personalized maps or recommendations based on places they have visited, get help finding their phones, and receive
real-time traffic updates about their commutes." (McGriff Dec., p. 2, ¶ 5.)

1 16:9-15.) Geolocation data is collected by Google in both Android and iOS iPhones but only if
2 the Location History service is enabled.⁷ (Vol. 1, R.T. 12:2-5; 17:3-8.) If the device is powered
3 off or if Location History is disabled, Google does not collect Location History data. (Vol. 1,
4 R.T. 17:11-13.) Even when the feature is enabled, a user need not actively use a Maps-based
5 application to collect Location History data, as the data is collected passively and routinely. (Vol.
6 1, R.T. 16:20-17:10.) As Location History is tied to a Google account, Location History can be
7 enabled on a single account and can collect data across multiple devices. (McGriff Dec., p. 3, ¶
8 9.)

10 2. Enabling Location History on an Electronic Device.

11 There are several ways for Google's Location History feature to be enabled. (Vol. 1, R.T.
12 10:25-11:6.) One method occurs during a new device setup, when a prompt pops onto the device
13 screen asking the user whether they would like to turn on the Location History feature. (Vol. 1,
14 R.T. 11:2-6.) Another method is for the user to manually turn it on through a Google-based app,
15 such as Google Maps. (*Chatrie, supra*, at p. 6.) The last method is referred to as "migrating,"
16 which occurs when Location History had been previously activated on an old device causing the
17 new device to automatically enable Location History. (Vol. 1, R.T. 18:26-19:7; 43:9-44:12.) In
18 those cases, Location History was activated by default and users might have been unaware the
19 feature was enabled.⁸ (Vol. 1, R.T. 20:8-23.)

20 For Location History to be fully enabled, a Google user must first turn on the location
21 feature on the mobile device itself. (McGriff Dec., p. 2, ¶ 7.) This allows the device to detect its
22 own location based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks.
23 (*Ibid.*) Turning on a mobile device's location feature alone, however, does not automatically
24 enable Google's Location History feature, as Location History is an entirely separate feature that
25 is enabled through a Google account. (*Id.* at p. 3, ¶ 8.) On the other hand, other Google services
26

27 ⁷ McInville indicated that, according to the census bureau, 84% of Americans owned smartphones in 2018. (Vol. 2,
28 R.T. 30:2-10.) In 2018, 46% of cell phone users were Android users. (Vol. 2, R.T. 30:19-26.)

⁸ Around 2018, Google set up what they refer to as "supported consent flows" to stop Google users from being
unaware the feature is turned on and to allow users to opt-in. (Vol. 1, R.T. 20:24-28.)

1 do not require having a user account to use the service, such as Google Maps and Search. (*Id.* at
2 p. 1, ¶3.)

3 Emily Moseley, in the declaration she authored for the hearing, indicated that “[i]n
4 October 2018, there were approximately 592 million daily active users of Location History
5 worldwide. Roughly one-third of all active Google users had Location History enabled on their
6 accounts.” (Exhibit E; see also Vol. 2, R.T. 16:3-7.) McGriff similarly declared that in 2019,
7 roughly one-third of active Google users had Location History enabled on their Google accounts.
8 (McGriff Dec., p. 4, ¶13.)

9 10 3. Pausing and Deleting Location History Data.

11 In addition to turning on the Location History feature, a user may pause the feature. (Vol.
12 1, R.T. 18:4-8.) Although there is no official “off” option, the “pause” option allows a user to
13 stop Google from collecting future Location History data while maintaining the already collected
14 data. (Vol. 1, R.T. 18:4-13.) A user can manually pause or stop Location History from collecting
15 their geolocation data and continue to use their device. (Vol. 1, R.T. 49:22-50:3.)

16 Location History also allows a user to manually delete geolocation data that has been
17 collected. (Vol. 1, R.T. 17:21-18:25.) A user can manually delete a day’s worth of data, or all of
18 it. (Vol. 1, R.T. 50:4-9.) Deleting some past data, however, does not stop Google from
19 continuing to collect future data, unless the user employs the pause option. (Vol. 1, R.T. 17:21-
20 24.) When a user deletes data from their Location History settings, that data is also removed
21 from Google’s Sensorvault servers within a few days. (Vol. 1, R.T. 19:14-19.) While a user can
22 manually delete data, a user cannot manually add data and create a fictional trip. (Vol. 1, R.T.
23 50:10-15.)

1 4. Google Stores Location History Data in its Sensorvault Database.

2 Google stores all of its users' Location History geolocation data in its Sensorvault
3 servers.⁹ (Vol. 1, R.T. 11-24-27; McGriff Dec., p. 3, ¶ 11.) Sensorvault stores only Location
4 History information. (*Ibid.*) Other location data, such as Google Location Accuracy and Web &
5 App Activity, are stored separately outside of the Sensorvault. (*Id.* at p. 5, ¶16; p. 6, ¶17.) Google
6 has determined that the data held in the Sensorvault is the only data that is responsive to a
7 geofence search warrant, as it is the only location data that is associated with a Google account
8 with sufficient precision. (*Id.* at pp. 7-8, ¶20.)

9 Google's Sensorvault stores each Location History data point associated with a unique
10 user account. (*Chatrie, supra*, at p. 4.) McGriff testified in *Chatrie* that the Sensorvault assigns
11 each device a unique device ID, distinct from a personally identifiable Google ID. (*Ibid.*) When
12 Google responds to a geofence search warrant and has "to identify users within the relevant
13 timeframe of a geofence, Google has to compare *all* the data in the Sensorvault in order to
14 identify users within the relevant timeframe of a geofence." (*Ibid.*)

15
16 **C. Google's Process in Responding to a Geofence Search Warrant Request for
17 Location History Data.**

18 Geofence search warrants, and Google's response to one, employ a multi-step procedure
19 developed by both Google employees and a government agency, Computer Crimes and
20 Intellectual Property Sections ("CCIPS")¹⁰. (Vol. 2, R.T. 12:1-13.) *Chatrie* details Google's
21 procedure through Sarah Rodriguez's testimony, a Google Team Lead for Legal Investigations
22 Specialists, which was testimony stipulated to in the instant case. The procedure Google
23 undertakes when a geofence search warrant is received follows:

24
25
26
27 ⁹ While some geolocation data may be stored on a physical device (i.e. in photographs taken by smartphones), the
geolocation data at issue here is the data stored in Google's Sensorvault servers. (Vol. 1, R.T. 12:12-13:2; 14:6-
14:23.)

28 ¹⁰ The Court takes judicial notice that CCIPS is a federal executive agency under the U.S. Department of Justice.
(Evid. Code, § 452, subd. (c), (h).)

1 1. Step One

2 In Step One, Google is asked to produce Location History data to law enforcement
3 responsive to the geofence parameters, which are the specific date(s), time(s), and place(s) as
4 indicated in the warrant and that correspond with the devices present at those times. (Vol. 2, R.T.
5 11:12-17; *Chatrie, supra*, at p. 9.) At this stage, Google produces the unique device IDs, the
6 latitude/longitude coordinates and timestamp of the stored Location History information, the
7 confidence interval, and the source of the Location History signal (i.e., GPS, Wi-Fi, etc.).
8 (*Chatrie, supra*, at p. 9.) The volume of data produced at this stage varies by the size and nature
9 of the geographic area and the length of time requested. (*Ibid.*)

10 For Google to produce Location History data that corresponds with the geofence search
11 warrant, Google must run a query across all of its worldwide users with Location History
12 enabled for the coordinates corresponding with each of those entries to determine what falls
13 within the geofence. (Vol. 2, R.T. 20:1-9.) Google must run its query against all of those users
14 because it does not store Location History information in a way that is searchable by location;
15 rather, it is organized by the anonymous device IDs. (Vol. 2, R.T. 20:1-3.) The query is
16 automated, and a computer algorithm generates the results, not a Google employee. (Vol. 2, R.T.
17 32: 1-13.)

18 In this first step, Google’s policy includes objecting to any geofence search warrant that
19 fails to require de-identification of the device IDs.¹¹ (*Chatrie, supra*, at pp. 8-9.) Google employs
20 Legal Investigations Specialists who process and review the geofence search warrant requests.
21 (*Id.* at p. 9.) If a specialist finds the warrant “needs further review,” because the geofence
22 parameters are too large (i.e., geographical area or time requested), the specialist may have
23 conversations with the requesting law enforcement officer about their investigation, and then
24 discuss it with Google’s legal counsel. (*Ibid.*) If Google’s legal counsel objects to the warrant,
25 Google may require law enforcement either to alleviate Google’s concerns or to seek an
26 amended or newly issued warrant to address the issue. (*Ibid.*)

27 ¹¹ Google uses the term “de-identified” which refers to the use of the Device ID with no specific identifying account
28 information. An example of a device ID, such as the one for Defendant Dawes, is 861462233. By contrast,
identifying account information would include subscriber information, such as the subscriber’s name, email address,
phone number, etc. (Pen. Code, § 1546, subd. (l).)

1 2. Step Two

2 In step two, law enforcement reviews the de-identified data from step one to determine
3 which device IDs are of further interest. (*Chatrie, supra*, at p. 10.) At this second step, law
4 enforcement can request from Google additional de-identified location data points for specific
5 device IDs present in the step one data that law enforcement has determined are relevant to its
6 investigation. (*Ibid.*) These additional data points can aid law enforcement in eliminating devices
7 not relevant to their investigation. (*Ibid.*) For example, the additional data may indicate that a
8 specific device was not in the target area for enough time to be of further interest, or that the
9 device moved through the area inconsistent with the other evidence (i.e., surveillance footage,
10 witness statements, etc.). (*Ibid.*)

11 Once the step two data for specific device IDs is requested, the geofence parameters are
12 entirely removed and the time frame is expanded for those specific device users to show the
13 devices' movement and travel prior to the geofence, into the geofence, and then outside the
14 geofence. (Vol. 2, R.T. 11:15-23.) In step two, there is no longer a geographical barrier of any
15 sort, as the focus is now device specific. (*Chatrie, supra*, at p. 10.) Google typically requires law
16 enforcement to narrow their request for step two data by requesting fewer devices than the
17 number of devices that were responsive in step one. (*Ibid.*) In other words, Google typically does
18 not permit law enforcement to request step two data from all devices present in step one. (*Ibid.*)
19 There is no clear policy as to when Google is satisfied that a step two data request is sufficiently
20 narrow. (*Ibid.*)

21 22 3. Step Three

23 In step three, law enforcement requests Google to reveal the subscriber information, or
24 account-identifying information, of specific device IDs. (Vol. 2, R.T. 11:24-27; *Chatrie, supra*,
25 at p. 10.) The account-identifying information includes the name and email address of the user.
26 (*Ibid.*) Google generally *prefers* law enforcement to ask for account-identifying information from
27 fewer users than in step two, but it is possible that Google may provide the information requested
28 even if it is not narrowed down. (*Ibid.*)

1
2 4. Location History Provides Law Enforcement an Estimation of a Device's
3 Location in Response to a Geofence Search Warrant Request.

4 Spencer McInville, a digital forensics examiner, provided testimony as to the accuracy
5 of Location History and the estimation of a device's geolocation. Specifically, geolocation data
6 produced by Google to law enforcement in response to a geofence search warrant is an estimated
7 location as opposed to an exact location. (Vol. 2, R.T. 8: 19-21; 9:4-13.) The geolocation data
8 will contain anonymous identifiers with an estimated latitude and longitude and a margin of error
9 or a display radius. (Vol. 2, R.T. 8:11-18.) Further, some of the different sensors for determining
10 a user's location are better than others. (Vol. 2, R.T. 9: 20-24.)

11 When Google reports the estimated location, that estimated location has a center point
12 and a specified radius is drawn around that point to create the map's display radius. (Vol. 2, R.T.
13 22:4-8, 22-27.) Google also reports a confidence interval, which is their confidence as to how
14 well they estimated the device's location. (Vol. 2, R.T. 22:28-23:4.) Google has a 68 percent
15 confidence interval that the device will be located within the specified radius of where the device
16 is estimated to be present; thus, there is a 32 percent chance that the device is actually located
17 outside the radius. (Vol. 2, R.T. 23:4-14; 23:25-24:1.) In other words, a device is not estimated to
18 be at the center point but somewhere in the specified radius of that center point; the device can
19 be at the edge of the radius and not necessarily close to the center. (Vol. 2, R.T. 23:10-24.)

20 The data produced by Google can include a false positive, which is a device that is
21 present inside the radius but falls outside the geofence drawn by law enforcement. (Vol. 2, R.T.
22 25:17-21.) This can occur, for example, if the center point estimated by Google is responsive
23 inside the geometric shape drawn by law enforcement, but the device was actually located
24 outside the shape and within the display radius. (Vol. 2, R.T. 25:17-25.) Usually, false positives
25 can be determined by looking at the overall data produced in step two, and it cannot be
26 determined by examining a single point. (Vol. 2, R.T. 35:2-14.) For example, in some cases, a
27 device's step one data may fall squarely inside the geofence's geometric shape. (Vol. 2, R.T.
28 35:2-14.) But in the device's step two data, it will show how the device traveled for the given

1 time stamps, and whether the device’s location “jumps in, [and] jumps back out.” (Vol. 2, R.T.
2 35:2-14.)

3 **D. The Instant Geofence Warrant and Its Justifications.**

4
5 1. SFPD’s Investigation into the Residential Burglary.

6 a. *The Affiant Officer’s Training, Background, and Experience*

7 Sergeant Farrell testified in the second evidentiary hearing on May 26, 2022, as to the
8 geofence search warrant he drafted. (Vol. 2, R.T. 40: 10-27; 42:13-20.) He estimated that he had
9 authored 300 to 400 search warrants prior to drafting the search warrant at issue in this case.
10 (Vol. 2, R.T. 42:9-12.) More specifically this was the third or fourth geofence search warrant
11 Sergeant Farrell had authored. (Vol. 2, R.T. 43: 17-19.) All of his prior geofence search warrants
12 had been signed by a San Francisco Superior Court judge. (Vol. 2, R.T. 44:10-15.)

13
14 b. *The Geofence Search Warrant and Affidavit*

15 The geofence search warrant at issue is a standardized search warrant and affidavit form,
16 and had attached to it an Appendix A, Appendix B, and a Probable Cause Statement. Page one of
17 the search warrant and affidavit checked off specific boxes that averred the geolocation data was
18 lawfully seizable because:

- 19 (A) [i]t was used as the means of committing a felony;
20 (B) [i]t [was] possessed by a person with the intent to use it as a means of
21 committing a public offense or [was] possessed by another to whom he or she may
22 have delivered it for the purpose of concealing it or preventing its discovery;
23 (C) [i]t tend[ed] to show that a felony has been committed or that a particular person
24 has committed a felony; and
25 (D) a provider of ‘electronic communication service’ or ‘remote computing service]
... ha[d] records or evidence regarding a subscriber or customer which (1) is of a
type specified in Penal Code section 1524.3.... and (2) which records or evidence
show[ed] that property was stolen or embezzled constituting a misdemeanor....

26 (Exhibit D.)

27 The geofence search warrant specifically authorized the search for “Reverse Geolocation
28 Data” and commanded that “Google Inc. SHALL provide Cellular, GPS and Wi-Fi sourced

1 location history for mobile devices that reported a location within the geographical region(s)
2 bounded by the listed latitude and longitude coordinates on the date and time as stated on
3 Appendix 'A'..." Additionally, the search warrant authorized the search for "Google Account
4 Information Associated to Reverse Geolocation Data." Specifically, the warrant commanded that
5 "Google Inc. SHALL adhere to the process as stated in Appendix 'B'... to obtain the
6 Subscriber/User information for mobile devices within the geographical region(s) as requested in
7 Appendix A."

8 The warrant further authorized a 90-day delay in notifying a subscriber, customer, or
9 owner of the existence or content of the search warrant pursuant to Penal Code section 1546.2.¹²
10 The search warrant was issued but was also sealed pursuant to *People v. Hobbs* (1994) 7 Cal.4th
11 948.

12
13 *c. Appendix A*

14 Appendix A identified the "target location" to be searched and provided Pham's complete
15 residential address. Appendix A included a map showing the residential neighborhood, with a
16 trapezoid drawn into the map. Each of the four corners of the trapezoid corresponded with a
17 specific longitude and latitude, as identified in Appendix A. The smallest end of the trapezoid
18 covered the back end of Pham's home, and the longest end covered the entire street in front of
19 Pham's home. The trapezoid shape cut through several other residences as it stretched out to the
20 far corners of the street.

21
22
23
24
25
26
27
28

¹² There is a separate order signed by the judge authorizing the sealing of the search warrant as well.



14 (Exhibit G, Fig. 3 [Same area as depicted in Appendix A, but in color and without victim's
15 address].)

16 Appendix A attached to the search warrant provided the date for the data to be searched
17 as October 24, 2018. It also provides three time periods as well:

- 18
- Time Period 1: 1445 hours through 1515 hours (or 2:45 pm to 3:15 pm)
 - Time Period 2: 1630 hours through 1830 hours (or 4:30 pm to 6:30 pm)
 - Time Period 3: 1720 hours through 1830 hours (or 5:20 pm to 6:30 pm)

19
20 (Exhibit D, Appendix A.)

21
22 *d. Appendix B*

23 Appendix B attached to the search warrant provided instructions, as a multi-step process
24 for Google to follow in responding to the search warrant. In its first step, Appendix B specified
25 the information sought as:

26 Location information: All location data, whether derived from Global Positioning
27 System (GPS) data, cell site/cell tower triangulation/trilateration, and precision
28 measurement information such as timing advance or per call measurement data, and

1 Wi-Fi locations, including GPS coordinates, estimated radius and the dates and
2 times of all location recordings....

3 (Exhibit D, Appendix B.) The warrant limited the order to produce this data for the date, time,
4 and locations specified, which was identical to Appendix A, with the notable exception of Time
5 Period 2. In Appendix A, Time Period 2 provided a different time period when compared against
6 Appendix B, which limited the end of Time Period 2 to 1700 hours (or 5:00 pm) instead.¹³

7 Appendix B further specified that in this first step, “[e]ach device corresponding to the
8 location data...will be identified only by a numerical identifier, without any further content or
9 information identifying the user of a particular device.” In other words, it required Google to
10 provide a unique device ID for each device to “mask” the users and keep them anonymous.

11 In its second step, Appendix B provided that:

12
13 For those accounts identified as relevant to the ongoing investigation through an
14 analysis of provided records, and upon demand, Google shall provide additional
15 location history outside of the predefined area for those relevant accounts to
16 determine path of travel. The additional location history shall not exceed 45 minutes
17 plus or minus the first and last timestamp associated with the account in the initial
18 dataset. The purpose of path of travel/contextual location points is to eliminate
19 outlier points where, from the surrounding data it becomes clear the reported
20 point(s) are not indicative of the device actually being within the scope of the
21 warrant.

19 (Exhibit D, Appendix B.) The Court notes that there was no requirement for the officer to return
20 to the duty judge or issuing judge to request additional judicial authorization for this Step Two
21 data.

22 Finally, in the third and final step, Appendix B provided that “[f]or those accounts
23 identified as relevant to the ongoing investigation through an analysis of provided records, and
24 upon demand of the investigative agents, Google shall provide the subscriber’s information for
25 those relevant accounts....” The subscriber information to be provided included the “subscriber’s
26 name, email address, IMEI and phone numbers, services subscribed to, recovery SMS phone
27

28 ¹³ At the second evidentiary hearing, Sergeant Jesse Farrell testified that he did not know why Appendix A’s Time
Period 2 (1630 hours through 1830 hours) was different than Appendix B’s Time Period 2 (1630 hours through 1700
hours); he indicated it could have been an error. (Vol. 2, R.T. 58:18-59:59:3.)

1 number and recovery email address.” Again, the text of the warrant provided no requirement for
2 the officer to obtain additional judicial authorization for this Step Three data. In other words,
3 once the warrant was signed, movement from Step One through to Step Three involved no
4 further judicial oversight or review.

5
6 *e. The Probable Cause Statement*

7 The “Probable Cause Statement” detailed much of the facts surrounding the crime and
8 the police’s investigation described above. Sergeant Farrell stated that based on his training,
9 experience, and consultations with other investigators that he knew “that subjects who commit
10 crimes, including residential burglaries, often use their cell phones as a means of communicating
11 during the commission of the crime” and specifically that suspects inside a home during a
12 residential burglary often communicate by cell phone with another who acts as a lookout.
13 Because the driver of the suspect vehicle remained outside during the residential burglary of
14 Pham’s home, Sergeant Farrell believed there was cell phone communications occurring between
15 those inside Pham’s home and the driver outside. More specifically, Sergeant Farrell believed the
16 nature of this communication was to alert the suspects inside the residence for the most optimal
17 time to flee and to know where to meet when the suspects fled.

18 Furthermore, Sergeant Farrell stated that based on his training, experience, and
19 consultations with other investigators that he knew most cell phones are smart phones and the
20 two most common types of smart phones are Androids and iOS Apple iPhones. Sergeant Farrell
21 explained that for Android devices, when a user turns on the Android device for the first time, it
22 prompts them to add a Google Account, which corresponds with a Google email address ending
23 in “gmail.com.” Sergeant Farrell believed, therefore, “it is nearly certain that a person using an
24 Android device has an associated Google account.”

25 Moreover, Sergeant Farrell stated that based on his training, experience, and
26 consultations with other investigators, that he knows Google collects and retains location data
27 from Android-enabled mobile devices, as well as non-Android devices if the device is registered
28 to a Google account and has location services enabled. Google collects this information from

1 Global Position System (“GPS”) data, cell site/cell tower information, and Wi-Fi access points.
2 The information collected from Google includes: “subscriber name, email address, IP address,
3 IMEI and phone numbers, services subscribed to, SMS recovery phone number and a recovery
4 email address.”

5 Finally, Sergeant Farrell indicated his reasons and beliefs for why there was probable
6 cause to search and seize the geolocation data in investigating the crime. Based on the evidence
7 collected in the investigation, including the surveillance footage and statements from witnesses
8 and officers, Sergeant Farrell knew the suspects were recorded on video at the location of the
9 crime, the date of the crime, and between 2:45 pm to 6:30 pm (1445 hours to 1830 hours).
10 Sergeant Farrell indicated he believed the suspects appeared to be surveilling, or casing, the
11 residence. And for those reasons, he sought judicial authorization to collect certain location
12 information related to Google accounts that were located near Pham’s home, at the date of the
13 crime, and during the time period the suspects appeared on the surveillance video footage.

14
15 **2. Duty Judge Authorizes the Geofence Search Warrant.**

16 On December 4, 2018, Sergeant Jesse Farrell presented to Judge Suzanne Bolanos the
17 geofence search warrant at issue here, which she signed and issued.¹⁴ The return to the geofence
18 search warrant, provided to law enforcement on January 10, 2019, implicated Defendant as one
19 of the burglary suspects because his cell phone was present during the commission of the crime.

20
21
22 **E. Google’s Return to the Geofence Search Warrant.**

23 McInville testified, in reviewing the return to the geofence search warrant, that he
24 identified three sets of Step One data that required three separate queries of all Google users.
25 (Vol. 2, R.T. 21:2-9.) He determined that the return to the geofence search warrant for Step One
26

27
28 ¹⁴ The Court notes that while motions to quash a search warrant are typically reviewed by the issuing judge, on March 24, 2021, Judge Bolanos granted a Code of Civil Procedure section 170.6 (hereinafter, “CCP 170.6”) challenge raised by Defendant. Upon granting the CCP 170.6, the motion to quash was assigned to this bench officer. This reviewing court approved and issued a subsequent search warrant in this investigation.

1 was consistent with the time periods as outlined in Appendix A, including the 20-minute overlap
2 between Time Periods 2 and 3. (Vol. 2, R.T. 26: 4:20-22.)

3 In the return for Step One, nine total device IDs were returned. (Vol. 2, R.T. 21:11-15.)
4 The results of the queries relating to those devices provided anonymized account IDs and were
5 anonymous even to the Google employee running the queries. (Vol. 2, R.T. 32:14-33:7.) The
6 results of the queries also yielded no information, pertaining to the remaining 590 million
7 Google users with Location History enabled, to the Google employee. (Vol. 2, R.T. 33:9-13.)

8 In Step Two, law enforcement identified six devices as relevant to their investigation and
9 requested corresponding Step Two data. (Vol. 2, R.T. 28:12-20.) In this second step, the
10 geofence was removed and the time frame was expanded to see the movement of the devices.
11 (Vol. 2, R.T. 28:21-26.) In the third and final step, only one device was “unmasked,” from which
12 law enforcement requested that user’s subscriber information. (Vol. 2, R.T. 29:16-23.)

14 **F. Defendant Dawes’ Location History Data.**

15 1. Defendant’s Location History was Enabled by Default in 2015.

16 McInville testified that he determined how Location History originally became enabled
17 on Defendant Dawes’s cell phone. (Vol. 1, R.T. 22:1-4.) He determined this by reviewing a
18 Google audit log for a “LaquanDawes22@gmail.com” account. (Vol. 1, R.T. 24:5-21; Exhibits
19 A and B.) That audit log reflects that Location History was a service added on March 9, 2015, at
20 12:53 am. (Vol. 1, R.T. 25:21-26:12; Exhibit A and B.) Within a few seconds after the Gmail
21 account for Mr. Dawes was created, Location History service was added and therefore enabled.¹⁵
22 (Vol. 1, R.T. 26:19-27:7; Exhibit A and B.) McInville testified these entries in the audit log are
23 “consistent with the setup of a brand-new device....” (Vol. 1, R.T. 27:8-25.) McInville opined
24 that from his experience in conducting new device setups, a user in 2015 would not have seen
25 any user prompts during the phone setup process pertaining to turning on Location History. (Vol.
26 1, R.T. 38:22-39:8.) McInville further opined that Defendant’s Location History was likely

27
28 ¹⁵ To be exact, the audit log reflects the following services were added at the specified times on March 9, 2015:
Gmail was added at 00:52:54, Location History was added at 00:53:05, Google Calendar was added at 00:53:56, and
Android was added at 00:53:06. (Exhibits A and B.)

1 activated by default in 2015 instead of being prompted to turn it on. (Vol. 1, R.T. 39:28-40:3;
2 42:21-43:8.)

3
4 2. Law Enforcement's Review of the Return to the Geofence Search Warrant.

5 In this case, after Google produced the return to the geofence search warrant, SFPD
6 received it as raw data that they entered into a mapping system called "CellHawk," which is used
7 to map out the suspects' phones and IDs. (Vol. 2, R.T. 60:19-26.) The software "will completely
8 upload [the raw data] into the system and put it on a map for [SFPD]." (Vol. 2, R.T. 60:19-26.)
9 After demanding the additional 45 minutes of Step 2 data, the officers narrowed down their
10 suspect to one device based on the device's movements. (Vol. 2, R.T. 61:1-6; 62:22-27.)
11 Sergeant Farrell did not remember, at the time of testifying, the exact results from the software,
12 but he did not believe that one device appeared in all three time periods. (Vol. 2, R.T. 61:7-15.)
13 The specific device for which law enforcement sought unmasking had geolocation data that
14 appeared only in the final time period, which was during the commission of the crime. (Vol. 2,
15 R.T. 63:8-22.)

16 Sergeant Farrell asked for only that one ID tag to be unmasked. (Vol. 2, R.T. 47:17-19.)
17 Google provided Sergeant Farrell with Defendant Dawes's subscriber information, email
18 "laquandawes22@gmail.com." (Vol. 2, R.T. 47:20-26.)

19
20 3. McInville's Review of Defendant Dawes' Location History Data Responsive
21 to the Geofence Search Warrant.

22 As to the data responsive to the geofence search warrant corresponding with Defendant
23 Dawes, three time-stamps were provided, which correspond with 1745 hours, 1747 hours, and
24 1749 hours (5:45 pm, 5:47 pm, and 5:49 pm), each with the sensor source as Wi-Fi. (Exhibit G,
25 Fig. 1.) McInville identified that the three time-stamps had a 58-meter radius with the center
26 points falling inside the trapezoid shape drawn by law enforcement. (Vol. 2, R.T. 21:19-22:11;
27 27:25-1; Exhibit G, Fig. 1.) Figure 4 in Exhibit G provides a demonstrative image of what the 8-
28

1 meter radius looks like in comparison with the trapezoid shape that law enforcement drew for the
2 geofence.



15 (Exhibit G, Fig. 4.) The 58-meter radius covers approximately 30 homes. (Vol. 2, R.T. 24:25-
16 27.) The radius is approximately seven times larger than the geofence drawn by law
17 enforcement. (Vol. 2, R.T. 24:28-25:3.)

18 McInville indicated that law enforcement could have requested geolocation data that
19 corresponded with either: (1) the display radius being completely inside the geometric shape, or
20 (2) the outer radius touching the points of the geometric shape (in other words, the shape would
21 be inside the display radius). (Vol. 2, R.T. 27:1-6, 17-19.) McInville testified that although both
22 of those options could have reduced the false positives, neither was requested by law
23 enforcement in the geofence warrant. (Vol. 2, R.T. 27:1-24.) However, on cross-examination,
24 McInville did indicate that if Google were instructed to produce data where the radius of
25 devices fell only inside the geofence's shape, then devices with the 58-meter radius would
26 simply not be included in the return. (Vol. 2, R.T. 34:1-22.)

1 **G. San Francisco Police Department's Geofence Search Warrant Practices.**

2 1. San Francisco Police Department's Geofence Search Warrant Drafting,
3 Processing, and Practices in 2018.

4 Sergeant Farrell testified that the geofence warrant template was developed by San
5 Francisco Police Department's Special Investigations Technical Services Unit by Lieutenant
6 McGuire and Officer Lieu.¹⁶ (Vol. 2, R.T. 43: 2-8.) Before the issuance of this search warrant,
7 Sergeant Farrell met with Lieutenant McGuire and Officer Lieu to discuss geofence search
8 warrants. (Vol. 2, R.T. 53:12-27; 55:13-16.)

9 In 2018, there was no official SFPD policy or internal memo specifically as to geofence
10 search warrants. (Vol. 2, R.T. 52:10-22.) This continues to be the case in 2022. (Vol. 2, R.T.
11 52:23-24.) Sergeant Farrell did not have any formal training specifically as to geofence search
12 warrants. (Vol. 2, R.T. 52:25-53:8.) At some unknown point in time *after* the issuance of this
13 geofence search warrant, a Google employee provided training to the burglary unit in
14 geofencing. (Vol. 2, R.T. 43:6-11; 55:8-12.)

15 Sergeant Farrell testified to what he understood about geofence search warrants at the
16 time of drafting this geofence warrant in 2018. Specifically, at that time, Sergeant Farrell
17 understood a geofence warrant to ask for data from Google that "captures [users'] ID numbers
18 from cell phones in a particular area that you're requesting, and you can then research that data
19 and find out which cell phones were in that area." (Vol. 2, R.T. 42:21-43:1.) At that time, he was
20 only aware he was asking for data for a specific area, not from a database with every user with
21 Location History enabled. (Vol. 2, R.T. 61:23-62:7; 63:23-27.)

22 In drafting a geofence search warrant, Sergeant Farrell indicated that in the course of an
23 investigation, he would compile the information that he possessed through video, time frames,
24 and witness statements, and then use Google maps or Google Earth to discern the area he
25 believed the suspects were located. (Vol. 2, R.T. 45:1-11.) In this case, based on the information
26 he had collected, Sergeant Farrell created a trapezoid shape. (Vol. 2, R.T. 59:8-22.) He explained

27 ¹⁶ The record is unclear as to whether Google was involved in drafting the original template of the geofence search
28 warrant at issue. In Sergeant Farrell's initial testimony, he indicated that SFPD's warrant was developed with the aid
 of Google, but in later testimony, he indicated that the training provided by Google came after this search warrant
 was issued. (Vol. 2, R.T. 43: 2-11; 55:8-12.) This ambiguity was never clarified by the People.

1 that he could have made the geometric shape smaller to encompass only Pham's residence and
2 the street. (Vol. 2, R.T. 59:8-60:7.) However, in 2018, he did not know that, because of the
3 margin of error, the geofence radius was actually much larger than the geometric shape he drew
4 on the map. (Vol. 2, R.T. 62:8-11.)

5 Sergeant Farrell described his general procedure in executing a geofence search warrant
6 in 2018. He testified that, after obtaining a judge's signature for a geofence search warrant, he
7 would transfer it to Officer Lieu to serve on Google. (Vol. 2, R.T. 46: 8-15.) Google would then
8 provide the search warrant return to Officer Lieu who would research the results and turn them
9 over to Sergeant Farrell, who would then conduct further research. (Vol. 2, R.T. 46:16-20.) After
10 meeting to discuss the results, Sergeant Farrell would request that Google provide an additional
11 45 minutes of data from select ID numbers to determine if any may be the likely suspect. (Vol. 2,
12 R.T. 47:1-17.) After selecting a device ID believed to belong to the suspect, Sergeant Farrell
13 would ask for Google to unmask that specific ID number and provide the unmasked information
14 to him. (Vol. 2, R.T. 47:8-16.)

15
16 2. Changes to SFPD's Geofence Search Warrant Procedure Subsequent to the
17 Signing of This Search Warrant in 2018.

18 Sergeant Farrell testified that SFPD's process for obtaining geofence search warrants has
19 changed since the issuance of this geofence warrant in 2018; SFPD now obtains a second
20 warrant to unmask a device ID. (Vol. 2, R.T. 49:8-19.) SFPD now only requests up to 15 minutes
21 of additional step two data as well. (Vol. 2, R.T. 50: 9-11.). This change came when Sergeant
22 Farrell drafted a geofence search warrant possibly a year later and brought it before Judge
23 Michael Begert. (Vol. 2, R.T. 50:2-5.) Judge Begert indicated to Sergeant Farrell that a second
24 warrant was required to unmask the device, which prompted Sergeant Farrell to consult with the
25 San Francisco District Attorney's Office. (Vol. 2, R.T. 50:5-8; 51:19-24.)

26 Sergeant Farrell provided some testimony as to SFPD's consultations with either the San
27 Francisco District Attorney's Office or with the City Attorney's Office *after* the issuance of this
28 geofence search warrant. Unfortunately, the record is unclear. During direct examination,

1 Sergeant Farrell testified that the District Attorney's Office agreed with Judge Begert's
2 requirement that law enforcement needed to draft two geofence search warrants and for the first
3 warrant to only request up to 15 minutes of additional data. (Vol. 2, R.T. 50:8-13; 62:22-63:3.)
4 On cross-examination, the transcript indicates the opposite: that the geofence warrant was
5 instead presented to the City Attorney's Office, who did not provide a definitive answer, and that
6 it was not presented to the District Attorney's Office. (Vol. 2, R.T. 51:14-18.) It is unclear from
7 which office, or both, SFPD sought advice from, as the attorneys never clarified this during their
8 examination.¹⁷

9 10 **H. The Subsequent Search Warrants Issued in This Investigation.**

11 After narrowing the geolocation data to Defendant's device and associated Google
12 account, Sergeant Farrell sought further search warrants. On January 15, 2019, a second search
13 warrant was signed and issued by Judge Richard Darwin. This second search warrant specifically
14 targeted Defendant Dawes and ordered all information pertaining to his Google Account under
15 the "laquandawes22@gmail.com" email, including: Subscriber information; Devices phone
16 numbers, IMEI ESN tablets, etc.; Login activity for all mobile devices; Location History from
17 10/22/18 to 10/26/18; Google Contacts; Google Drive; Google Gmail; Google Photos; Google
18 Search; and Google Voice. It also provided for a 90-day delay in notifying Defendant of this
19 search. The next day, on January 16, 2019, a return to the search warrant was provided. At the
20 same time, law enforcement performed a records check and confirmed Defendant Dawes owned
21 a Honda Accord, which matched one of the two vehicles in the burglary.

22 On January 21, 2019, Judge Brendan Conroy signed and issued a search warrant targeting
23 Defendant's telephone number. The return was presented to the judge the next day. On January
24 28, 2019, the final two warrants were issued by Judge Linda Colfax-- another search warrant for
25 Defendant's Google Account and a *Ramey* arrest warrant. Defendant was ultimately arrested on
26 February 6, 2019.

27
28 ¹⁷ The Court points out the ambiguity in the record to explain why these facts are not relied upon for a showing of good faith.

1 DISCUSSION

2 I. STANDARD OF REVIEW.

3 The Fourth Amendment to the Federal Constitution directs that no warrant shall issue, but
4 upon probable cause, supported by oath or affirmation, and particularly describing the place to be
5 searched, and the persons or things to be seized. (U.S. Const. 4th Amend.) Search warrants must
6 be supported by probable cause and signed by a neutral and detached magistrate. (U.S. Const.
7 4th Amend.; *Johnson v. U.S.* (1948) 333 U.S. 10, 14.). A defendant may move to quash a search
8 warrant pursuant to Penal Code section 1538.5, on the ground that the warrant was obtained
9 without sufficient probable cause. Probable cause determinations are assessed by the totality-of-
10 the-circumstances. (*Illinois v. Gates* (1983) 462 U.S. 213, 238 (hereinafter, “*Gates*”).)

11
12 The task of the issuing magistrate is simply to make a practical, common-sense
13 decision whether, given all the circumstances set forth in the affidavit before him
14 [or her], including the ‘veracity’ and ‘basis of knowledge’ of persons supplying
15 hearsay information, there is a fair probability that contraband or evidence of a
16 crime will be found in a particular place. And the duty of the reviewing court is
17 simply to ensure that the magistrate had a ‘substantial basis for [concluding]’ that
18 probable cause existed.

17 (*Ibid.*) The issuing magistrate’s finding of probable cause is entitled to deferential review and
18 should only be overturned when the reviewing court finds, as a matter of law, that the affidavit
19 fails to set forth sufficient competent evidence to support a finding of probable cause. (*People v.*
20 *Westerfield* (2019) 6 Cal.5th 632, 659.)

21 In motions challenging the *validity* of a warrant, the defendant bears the burden of
22 establishing that the warrant was invalid or improperly executed. (*Theodor v. Superior Court*
23 (1972) 8 Cal.3d 77, 101.) This burden extends to both a motion to quash and to a motion to
24 traverse a search warrant. (*People v. Amador* (2000) 24 Cal.4th 387, 393.) Both the magistrate
25 and reviewing courts are to interpret an affidavit for a search warrant in a common sense and
26 realistic fashion. (*Gates, supra*, 462 U.S. at p. 238.) “Because they are often written by
27 nonlawyers in the midst of an investigation, technical requirements for elaborate specificity have
28

1 no place in the review of search warrant affidavits.” (*People v. Varghese* (2008) 162 Cal.App.4th
2 1084, 1103.)

3 California has further codified and clarified Fourth Amendment protections for electronic
4 devices through the California Electronics Communication Privacy Act (CalECPA). CalECPA
5 provides a suppression remedy pursuant to Penal Code section 1538.5 when electronic
6 information is collected in violation of the statute. Specifically, CalECPA provides that:

7
8 [a]ny person in a trial, hearing, or proceeding may move to suppress any electronic
9 information¹⁸ obtained or retained in violation of the Fourth Amendment to the
10 United States Constitution or of this chapter. The motion shall be made, determined,
11 and be subject to review in accordance with the procedures set forth in subdivisions
12 (b) to (q), inclusive, of Section 1538.5.

13 (Pen. Code, § 1546.4, subd. (a).) Moreover, any individual who is targeted by a warrant pursuant
14 to CalECPA “may petition the issuing court to void or modify the warrant..., or to order the
15 destruction of any information obtained in violation of this chapter, or the California
16 Constitution, or the United States Constitution.” (Pen. Code, § 1546.4, subd. (c).)

17 **II. LIMITED EXISTING JURISPRUDENCE IN THE GEOFENCE SEARCH** 18 **WARRANT CONTEXT.**

19 This Court is presented with myriad novel legal issues that involve the application of the
20 Fourth Amendment to the geofence search warrant context. At this time, there is no authority on
21 point and no California appellate court has yet to address the issue. The Court has reviewed the
22 only published federal case that reviewed the *validity* of geofence search warrants in the context
23 of a motion to quash. (*Chatrie, supra*, 2022 WL 628905, 1.) The Court has also reviewed federal
24 and out-of-state decisions reviewing the constitutionality of law enforcement’s *applications* for
25 geofence search warrants. (*Matter of Search of Information Stored at Premises Controlled by*
26 *Google* (N.D. Ill., July 8, 2020, No. 20 M 297) 2020 WL 5491763 (hereinafter, “*Pharma P*”);
27 *Matter of Search of Information Stored at Premises Controlled by Google* (N.D. Ill. 2020) 481

28 ¹⁸ “Electronic Information” is defined as “electronic communication information” or “electronic device
information.” (Pen. Code, § 1546, subd. (g).) Both are separately defined below.

1 F.Supp.3d 730 (hereinafter, “Pharma IP”); *Matter of Search Warrant Application for Geofence*
2 *Location Data Stored at Google Concerning an Arson Investigation* (N.D. Ill. 2020) 497
3 F.Supp.3d 345 (hereinafter, “Arson”); *Matter of Search of Information that is Stored at Premises*
4 *Controlled by Google, LLC* (D. Kan. 2021) 542 F.Supp.3d 1153 (hereinafter, “Kansas Federal
5 *Crimes*”); *In re the Search of Information Stored at the Premises Controlled by Google, 2022*
6 *WL 584326, 1* (Va.Cir.Ct.) (hereinafter, “Virginia Shooting”); *Matter of Search of Information*
7 *that is Stored at Premises Controlled by Google LLC* (2021) 579 F.Supp.3d 62 (hereinafter,
8 “D.C. Federal Crimes”).) Out of these geofence search warrant applications, only *Arson, supra*,
9 and *D.C. Federal Crimes, supra*, approved geofence applications, whereas the remainder found
10 the geofence applications to violate the Fourth Amendment. The Court has done an extensive
11 review of the facts and analysis from the above-referenced cases in drafting this Order.

12 The Court similarly notes that although CalECPA was enacted in 2016, there is a paucity
13 of published decisions interpreting CalECPA, none of which is particularly useful to this Court
14 in the geofence context. The Court has also reviewed the legislative history in drafting and
15 amending CalECPA.

16
17 **III. DEFENDANT DAWES HAD A REASONABLE EXPECTATION OF PRIVACY**
18 **IN HIS GEOLOCATION DATA HELD BY GOOGLE UNDER CALECPA.**

19 At the conclusion of the first evidentiary hearing held on October 4, 2021, the Court ruled
20 that Defendant Dawes had a reasonable expectation of privacy in his geolocation data held by
21 Google and that a search warrant was required. (Vol. 1, R.T. 87:19-89:15.) The Court declined to
22 address the Fourth Amendment question as to whether there was a reasonable expectation of
23 privacy under the Federal Constitution because the State Legislature already made this express
24 determination through the enactment of CalECPA and because the officers had, in fact, sought a
25 warrant.¹⁹ (Vol. 1, R.T. 87:19-26.)

26
27 ¹⁹ Additionally, the Court need not address the question of whether the third-party doctrine under *Miller v. United*
28 *States* (1976)425 U.S. 435 and *Smith v. Maryland* (1979) 442 U.S. 735 applies to geolocation data. (Vol. 1, R.T.
89:27-91:2.) Regardless of whether the third-party doctrine applies, state law applies a heightened standard to
geolocation data that always imposes the protections of a warrant requirement.

1 Penal Code sections 1546 to 1546.4, which are the relevant provisions of the California
2 Electronic Communications and Privacy Act (“CalECPA”), govern search warrants in the
3 electronic and digital context. When proposed as Senate Bill 178 (Stats. 2015, ch. 651), the
4 Legislative Counsel’s Digest indicates that, amongst many other things, the effect of the Senate
5 Bill would be to prohibit law enforcement from compelling the production of certain data
6 without a search warrant, court order, or subpoena; would provide when the government may
7 obtain certain data; would define certain technological terms; and would provide a suppression
8 remedy for a criminal defendant.²⁰ Indeed, CalECPA protects the public’s “electronic
9 information,” which is broken down into two categories: “electronic communication
10 information” and “electronic device information.” (Pen. Code, § 1546, subs. (d), (g), (h).)
11 Members from the public who are protected under CalECPA include “service providers,” and
12 device users. (Pen. Code, § 1546.1, subd. (a)(1), (2).)

13 In Penal Code section 1546.1, subdivision (a)(1), CalECPA explicitly protects “electronic
14 communication information,” which is defined by statute as:

15 any information about an electronic communication or the use of an electronic
16 communication service, including, but not limited to, the contents, sender,
17 recipients, format, or *location of the sender or recipients at any point during the*
18 *communication, the time or date the communication was created, sent, or received,*
19 or any information pertaining to any individual or device participating in the
communication, including, but not limited to, an IP address.

20 (Pen. Code, § 1546, subd. (d), italics added.) Furthermore, an “electronic communication,” is
21 broadly defined as “the *transfer of signs, signals, writings, images, sounds, data, or intelligence*
22 *of any nature* in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-
23 optical system.” (Pen. Code, § 1546, subd. (c), italics added.)

24 Correspondingly, in Penal Code section 1546.1, subdivision (a)(2), CalECPA explicitly
25 protects “electronic device information,” which is defined as “any information stored on *or*
26 *generated through the operation* of an electronic device, *including the current and prior*
27 *locations of the device.*” (Pen. Code, § 1546, subd. (g), italics added.)

28 ²⁰ (See LAW ENFORCEMENT OFFICERS—SEARCHES AND SEIZURES—CELLULAR
COMMUNICATIONS, 2015 Cal. Legis. Serv. Ch. 651 (S.B. 178) (WEST).)

1 Although CalECPA generally restricts the government’s access to electronic information,
2 the statute expressly allows for the government to compel the production of access to such
3 information in limited and specific circumstances. One such avenue for the government to
4 compel access is pursuant to a lawfully executed search warrant. (Pen. Code, § 1546.1, subd.
5 (b)(1).)

6
7 **A. Google’s Location History Data is Protected Under Penal Code Section 1546.1,**
8 **Subdivision (a)(1).**

9 Pursuant to Penal Code section 1546.1, subdivision (a)(1), CalECPA specifically protects
10 “service providers,” which are defined as “a person or entity offering an electronic
11 communication service.” (Pen. Code, § 1546, subd. (j).) An “electronic communication service”,
12 defined as “a service that provides to its subscribers or users the ability to send or receive
13 electronic communications, include[es] any service that acts as an intermediary in the
14 transmission of electronic communications, or stores electronic communication information.”
15 (Pen. Code, § 1546, subd. (e).)

16 Here, the Court finds that Google is an entity that offers an electronic communication
17 service. The Court further finds that the geolocation data collected and maintained by Google
18 through their Location History feature is encompassed in subdivision (a)(1) and falls squarely
19 within the statutory definitions of electronic communications and electronic communication
20 information. Geolocation data, generated through “the transfer of signs, signals, ... data, or
21 intelligence,” is a form of an electronic communication. A smartphone with Location History
22 enabled will connect through sensors such as GPS, cell sites, Wi-Fi, and Bluetooth signals, and
23 will send signals and transfer data that reveal an individual’s geolocation to Google, the service
24 provider.

25 This electronic communication information data collected by Google is then maintained
26 and stored in Google’s Sensorvault servers. The geolocation data stored by Google’s Sensorvault
27 includes not only the location of the user when the signal connection was made, but also the date
28 and time of the connection that corresponds with that location. As such, a user’s geolocation data

1 that is collected through the Location History feature is electronic communication information,
2 as defined by CalECPA.

3
4 **B. Google’s Location History Data is Protected Under Penal Code Section 1546.1,**
5 **Subdivision (a)(2).**

6 Pursuant to Penal Code section 1546.1, subdivision (a)(2), CalECPA specifically protects
7 “any person or entity *other than* the authorized possessor of the device.” (Pen. Code, § 1546.1,
8 subd. (a)(2), italics added.) An “authorized possessor” is someone who is the true owner of the
9 device or was authorized to possess the device by the true owner. (Pen. Code, § 1546, subd. (b).)
10 While the authorized possessor refers to physical ownership or possession of the device, this
11 second provision applies to the persons or entities *who are not the physical owner or possessor*.
12 Thus, this second provision is simply broader than the service providers protected in subdivision
13 (a)(1).

14 The kind of data that subdivision (a)(2) intends to protect is “electronic device
15 information,” which is defined as “*any information* stored on or generated through the operation
16 of an electronic device, *including the current and prior locations of the device*.” (Pen. Code, §
17 1546, subd. (g), italics added.) An “electronic device” is defined as “a device that stores,
18 generates, or transmits information in electronic form” (i.e., a smartphone). (Pen. Code, § 1546,
19 subd. (f).) The data protected in subdivision (a)(2), unlike subdivision (a)(1), need not originate
20 from an electronic communication; the data need only be stored or generated through the
21 operation of the device. (Pen. Code, § 1546, subd. (g), (h).)

22 Employing the principles and definitions above, the Court finds that geolocation data
23 collected by Google through the Location History feature falls squarely into Penal Code section
24 1546.1, subdivision (a)(2). First, Google is an “entity other than the authorized possessor of the
25 device” that the statute seeks to protect. Second, once the Location History feature is enabled and
26 the electronic device is powered on, it will passively and continuously connect to many different
27 kinds of sensors even when a user is not actively interacting with the device. When smartphone
28 devices are powered on, they are reasonably expected to be in continuous operation, as the

1 device is expected to give the user notifications about incoming calls, texts, emails, and app
2 notifications. Through this continuous but passive device operation, an electronic device's
3 geolocation data is generated and is closely connected to that specific device. Thus, a user's
4 geolocation data generated through Google's Location History feature is electronic device
5 information.

6 7 **C. Conclusion.**

8 The Court hereby reaffirms its prior ruling and findings and concludes that a search
9 warrant was required under state law to obtain Defendant's geolocation data held by Google.
10 (Vol. 1, R.T. 88:22-89:15.) More specifically, based upon a plain reading of CalECPA and
11 comparing that with the testimony regarding how the technology functions and interacts with a
12 user's electronic device, the Court finds that Defendant's geolocation data transmitted from his
13 Android smartphone to Google's Sensorvault servers through the Location History feature
14 satisfied both subdivision (a)(1) and (a)(2).

15 16 **IV. THE GEOFENCE SEARCH WARRANT DOES NOT SATISFY BOTH THE** 17 **PROBABLE CAUSE AND PARTICULARITY REQUIREMENTS OF THE** 18 **FOURTH AMENDMENT.**

19 Generally speaking, the Fourth Amendment's warrant clause requires that before a search
20 warrant is issued, three foundational conditions be present: (1) the search warrant must be
21 reviewed and signed by a neutral magistrate; (2) the application for a search warrant must be
22 supported by probable cause that a crime has been committed; and (3) the application for a
23 search warrant must describe with particularity the place or person to be searched and seized.
24 (U.S. Const. 4th Amend; *Dalia v United States* (1979) 441 U.S. 238, 255.) The Fourth
25 Amendment's warrant requirement "reflect[s] the determination of [the Founding Fathers] that
26 the people ... should forever 'be secure in their persons, houses, papers, and effects' from
27 intrusion and seizure by officers acting under the unbridled authority of a general warrant."
28 (*Stanford v. State of Tex.* (1965) 379 U.S. 476, 481.) After all, "[t]he overriding function of the

1 Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by
2 the State.” (*Schmerber v. California* (1966), 384 U.S. 757, 767.)

3
4 **A. The Fourth Amendment’s Probable Cause Requirement.**

5 **1. Probable Cause Defined.**

6 The determination of probable cause is a decision requiring “a fair probability that
7 contraband or evidence of a crime will be found in a particular place.” (*Gates, supra*, 462 U.S. at
8 p. 238.) “The task of the issuing magistrate is simply to make a practical, common-sense
9 decision whether, given all the circumstances set forth in the affidavit before him [or her],
10 including the ‘veracity’ and ‘basis of knowledge’ of persons supplying hearsay information,
11 there is a fair probability that contraband or evidence of a crime will be found in a particular
12 place.” (*Gates, supra*, 462 U.S. at p. 238.) Probable cause sufficient for issuance of a warrant
13 requires a showing that makes it “substantially probable that there is specific property lawfully
14 subject to seizure presently located in the particular place for which the warrant is sought.”
15 (*People v. Frank* (1985) 38 Cal.3d 711, 744 (“*Frank*”), quoting *People v. Cook* (1978) 22 Cal.3d
16 67, 84, fn. 6.) “That showing must appear in the affidavit offered in support of the warrant.”
17 (*People v. Carrington* (2009) 47 Cal.4th 145, 161; *Frank, supra*, 38 Cal.3d at p. 744.) The
18 reviewing neutral magistrate must have a “substantial basis for concluding a fair probability
19 existed that a search would uncover wrongdoing.” (*People v. Kraft* (2000) 23 Cal.4th 978, 1040,
20 citing *Gates, supra*, 462 U.S. at pp. 238–239.)

21 Our California Supreme Court has held that for the purpose of issuing a search warrant
22 under California state law, the standard of probable cause is “whether the affidavit [1] states facts
23 [2] that make it substantially probable [3] that there is specific property [4] lawfully subject to
24 seizure [5] presently located [6] in the particular place for which the warrant is sought.” (*Frank,*
25 *supra*, 38 Cal.3d at p. 727.) Additionally, the first requirement that the affidavit states facts “is a
26 precondition of all the others, and has been separately codified in our statutes....” (*Ibid.*)
27 Specifically, Penal Code section 1527 provides that “[t]he affidavit or affidavits *must set forth*
28

1 *the facts* tending to establish the grounds of the application, or probable cause for believing that
2 they exist.” (Pen. Code, § 1527, italics added.)

3 On review in the context of a motion to quash a search warrant, the magistrate’s
4 determination of probable cause is entitled to deferential review. (*Kraft, supra*, 23 Cal.4th at p.
5 1041, citing *Gates, supra*, 462 U.S. at p. 236.) “Ultimately, the magistrate’s determination will
6 not be overturned unless the supporting affidavit fails as a matter of law to support the finding of
7 probable cause.” (*People v. French* (2011) 201 Cal.App.4th 1307, 1315, internal quotations
8 omitted, quoting, *Fenwick & West v. Superior Court* (1996) 43 Cal.App.4th 1272, 1278.)

9
10 2. Probable Cause Existed to Support the Issuance of a Geofence Search
11 Warrant.

12 a. The Search Warrant’s Affidavit Established Probable Cause.

13 The Court finds that there was sufficient probable cause to issue a geofence search
14 warrant.²¹ To start, probable cause existed that a crime had occurred. The warrant affidavit
15 described in detail that on October 24, 2018, Pham reported to police that his home had been
16 burglarized and that some of his property had been stolen. Specifically, Pham’s laptop, a safe
17 containing \$9,000 in cash, and two car keys had been stolen from his residence. Police observed
18 that the home’s front door appeared to have been kicked in, suggesting a forced entry had
19 occurred. Police also recovered surveillance footage from a neighbor that recorded a suspect
20 vehicle and three burglary suspects.

21 Second, despite the fact that no suspect captured by the surveillance footage was depicted
22 using a cell phone, there was probable cause to believe the suspects did possess smartphones
23 during the commission of the crime. As he reviewed the surveillance footage, Sergeant Farrell
24 observed three suspects—two who entered the unit and the third who functioned as the look-out
25 and getaway driver. As Sergeant Farrell attested in his affidavit, based on his training and
26 experience, burglary suspects often use cell phones to communicate during the commission of a
27 crime. More specifically, in burglary situations in which some suspects are inside while others

28

²¹ While there was sufficient probable cause to issue a geofence search warrant, the Court notes that a more particular warrant was required, as discussed below in the particularity discussion.

1 remain outside as a lookout, cellphones provide the method to be able to communicate with one
2 another. (Exhibit D.) Sergeant Farrell explained that in this case, the driver of the suspect vehicle
3 remained outside and therefore likely communicated with the suspects inside the residence by
4 cell phone to arrange where to meet or to alert them if they needed to flee. (Exhibit D.)

5 Third, there was probable cause to believe that Google was collecting and storing
6 location data from the suspects' smartphones. As Sergeant Farrell indicated in his affidavit the
7 two most commonly used Smartphone operating systems are iOS (Apple) and Android systems
8 and that it was nearly certain that a person using an Android device has an associated Google
9 account. In his training, Sergeant Farrell learned that Google collects and retains location data
10 from Android enabled mobile devices as well as non-Android devices that are registered to a
11 Google account and with location services enabled. (Exhibit D.) Sergeant Farrell also indicated
12 in his affidavit that Google collects this location information for advertising purposes, which
13 makes it reasonable to infer that Google will continue to collect and store the location
14 information, as Google financially benefits from doing so. (Exhibit D.)

15 Fourth, there is a fair probability that Google was in possession of identifying
16 information for the users of the devices found within the geofence. Sergeant Farrell stated in his
17 affidavit that he knows Google collects and stores every user's "subscriber name, email address,
18 IP address, IMEI, phone numbers, services subscribed to, SMS recovery phone number and a
19 recovery email address." (Exhibit D.) This was the kind of information that law enforcement was
20 seeking through the geofence search warrant so they could utilize it to identify their suspects.

21
22 b. Modern Day Realities Regarding Cellphone Usage Further Supported
23 the Finding of Probable Cause.

24 Modern day realities regarding cellphone usage further support, rather than contradict,
25 the probable cause finding, as provided by our evidentiary record and the United States Supreme
26 Court's recent technology cases. For example, Sergeant Farrell's belief that the suspects were in
27 possession of a cell phone was reasonable and is consistent with recent United States Supreme
28 Court reasoning. As the United States Supreme Court declared in in *Carpenter*, "[e]ven if

1 nobody knew for sure whether the [suspect] *actually* possesses a cell phone.....most people
2 ‘compulsively carry cell phones with them all the time.’” (*Carpenter, supra*, 138 S. Ct. at p.
3 2218.) In an earlier case, the United States Supreme Court also recognized that in today’s age, “it
4 is the person who is not carrying a cell phone ... who is the exception.” (*Riley v. California*
5 (2014) 573 U.S. 373, 395.) This reasonable inference is further supported by the evidence from
6 this Court’s two evidentiary hearings. As defense expert McInville testified, according to the
7 census bureau, 84% of Americans owned smartphones in 2018. (Vol. 2, R.T. 30:2-10).

8 Moreover, the evidentiary record in this case supported the reasonable belief that Google
9 collected and stored location data responsive to the geofence search warrant. According to Emily
10 Mosley, a Google employee, in 2018 there were approximately 592 million daily active users of
11 Location History worldwide and roughly one-third of those active users had Location History
12 enabled on their accounts. (Emily Mosely Declaration, Ex. E.) Additionally, as of 2018, Google
13 had not yet set up the “supported consent flows” that alerted users at set-up about Location
14 History activation to allow users to make an opt-in or opt-out decision. During this era, Location
15 History often would activate by default when a user, whose old device had Location History
16 enabled, purchased a new device and used the same account. (Vol. 1, R.T. 18:26-19:7; 20:8-28;
17 43:9-44:12.) As indicated in the evidentiary record, through Location History, Google
18 geolocation data is collected about every two minutes from the device through cellular networks,
19 Wi-Fi, Bluetooth, and GPS, which are all used to locate and track a device. (Vol. 1, R.T. 10:14-
20 18; 12:2-11.)

21 As to the probability that Google was in possession of *identifying* information for the
22 users of the devices found within the geofence, the evidentiary record confirmed that Google can
23 link the Location History data with a particular Google account, transmit and store that data to
24 the Sensorvault and ultimately match it to a specific user. (Vol. 2, R.T. 42:31-43:1; McGriff
25 Decl., p. 7, ¶20.)

26 Because there was a “fair probability” that the suspects were: (i) located inside the
27 geofence²² during the specified time period; (ii) using their cell phones; (iii) communicating

28 _____
²² The Court discusses *infra* both particularity and overbreadth as it relates to the geofence location.

1 location history to Google through the cell phones; and (iv) traceable through the information
2 stored in Google's Sensorvault, there was probable cause that the search would produce evidence
3 useful to Sergeant Farrell's investigation into the residential burglary.

4
5 **B. The Fourth Amendment's Particularity Requirement.**

6 1. Particularity and Overbreadth Defined.

7 The warrant clause of the Fourth Amendment provides that no warrant may issue except
8 those "particularly describing the place to be searched, and the persons or things to be seized."
9 (See generally, *Walter v. United States* (1980) 447 U.S. 649, 656-657, fn. 8.) Three conditions
10 must be met to satisfy the Fourth Amendment's particularity requirement: The "warrant must
11 identify [1] the specific offense for which law enforcement has established probable cause; [2] it
12 must describe the place to be searched; and [3] it must specify the items to be seized by their
13 relation to designated crimes." (*Matter of Search of [Redacted] Washington, District of*
14 *Columbia* (2018) 317 F. Supp.3d 523, 527 fn.3, internal quotations and citations omitted; see
15 also *Groh v. Ramirez* (2004) 540 U.S. 551, 557 (hereinafter, "*Groh*").) "The uniformly applied
16 rule is that a search conducted pursuant to a warrant that fails to conform to the particularity
17 requirement of the Fourth Amendment is unconstitutional." (*Groh, supra*, 540 U.S. at p. 559,
18 citing *Stanford v. Texas* (1965) 379 U.S. 476, 485-486; *United States v. Cardwell* (9th Cir.
19 1982), 680 F.2d 75, 77-78.)

20 The Fourth Amendment's particularity requirement is designed to prevent general
21 exploratory searches. (*Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249 ("*Burrows*");
22 *People v. Smith* (1994) 21 Cal.App.4th 942, 947-950 ("*Smith*"); *People v. Murray* (1978) 77
23 Cal.App.3d 305, 308; *Maryland v. Garrison* (1987) 480 U.S. 79, 84 ("*Garrison*").) General
24 warrants leave "to the discretion of the executing officials the decision as to which persons
25 should be arrested and which places should be searched...[and] provide no judicial check on the
26 determination of the executing officials that the evidence available justified an intrusion into any
27 particular [place]." (*Steagald v United States* (1981) 451 U.S. 204, 220.)

1 Furthermore, particularity is satisfied if the warrant imposes a “*meaningful restriction*”
2 on the place to be searched and the objects to be seized. (*Burrows, supra*, 13 Cal.3d at p. 249;
3 *Smith, supra*, 21 Cal.App.4th at p. 949.) Conversely, a warrant lacking such restriction “is
4 similar to the *general warrant* permitting [an] unlimited search, which has long been
5 condemned.” (*Aday v. Superior Court of Alameda County* (1961) 55 Cal.2d 789, 796, italics
6 added.) “However, a warrant need only be reasonably specific [citation], and the specificity
7 required varies depending on the circumstances of the case and the type of items involved.”
8 (*People v. Robinson* (2010) 47 Cal.4th 1104, 1132, internal quotations omitted.) “The touchstone
9 of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by
10 ‘assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on
11 the other, the degree to which it is needed to promote legitimate governmental interests.’”
12 (*United States v. Knights* (2001) 534 U.S. 112, 118-119, quoting *Wyoming v. Houghton* (1999)
13 526 U.S. 295, 300.)

14 The “reasonable particularity” requirement is a “flexible concept, reflecting the degree of
15 detail available from the facts known to the affiant and presented to the issuing magistrate.”
16 (*People v. Tockgo* (1983) 145 Cal.App.3d 635, 640.) “In considering whether a warrant is
17 sufficiently particular, courts consider the purpose of the warrant, the nature of the items sought,
18 and ‘the total circumstances surrounding the case.’” (*People v. Eubanks* (2011) 53 Cal.4th 110,
19 133; quoting *People v. Rogers* (1986) 187 Cal.App.3d 1001, 1008 (“*Rogers*”).) “A warrant that
20 permits a search broad in scope may be appropriate under some circumstances, and the warrant’s
21 language must be read in context and with common sense.” (*Eubanks, supra*, at p. 133.) For
22 example, “in a complex case resting on the piecing together of ‘many bits of evidence,’ [a]
23 warrant properly may be more generalized than in a simpler investigation resting on more direct
24 evidence.” (*Kraft, supra*, 23 Cal.4th at p. 1041.)

25 “It is axiomatic that a warrant may not authorize a search broader than the facts
26 supporting its issuance.” (*Burrows, supra*, 13 Cal.3d 238, 250.) “[T]he scope of a lawful search
27 is ‘defined by the object of the search and the places in which there is probable cause to believe
28 that it may be found.’” (*Garrison, supra*, at p. 84, quoting *United States v. Ross* (1982) 456 U.S.

1 798, 824.) The particularity requirement not only prevents general searches, but limits “[a]s to
2 what is to be taken, [as] nothing is left to the discretion of the officer executing the warrant.”
3 (*Andresen v. Maryland* (1976) 427 U.S. 463, 480.)

4 At the end of the day, the particularity requirement “ensures that the search will be
5 carefully tailored to its justifications, and will not take on the character of the wide-ranging
6 exploratory searches the Framers intended to prohibit.” (*Garrison, supra*, 480 U.S. at p. 84;
7 *Marron, supra*, 275 U.S. at p. 196.) The particularity requirement operates as a protection against
8 arbitrary government intrusions, as the Fourth Amendment’s very purpose is “to safeguard the
9 privacy and security of individuals against arbitrary invasions by governmental
10 officials.”(*Carpenter, supra*, 138 S.Ct. at p. 2213, quoting *Camara v. Municipal Court of City*
11 *and County of San Francisco* (1967) 387 U.S. 523, 528.) For the reasons set forth below, the
12 Court finds that although the geofence search warrant was supported by probable cause, it was
13 not sufficiently particular under the Fourth Amendment to the Federal Constitution.

14
15 2. The Geofence Search Warrant was Not Sufficiently Particular and was
16 Overly Broad Under the Fourth Amendment.

17 The Court finds that the geofence search warrant issued in this case failed the
18 particularity requirement because it did not narrowly identify “the place to be searched” by both
19 time and geographic location, rendering it overbroad in scope. In the context of a geofence
20 search warrant, to satisfy particularity as to the place to be searched, law enforcement must
21 “appropriately contour[] the temporal and geographic windows in which it is seeking location
22 data.” (*D.C. Federal Crimes, supra*, 579 F.Supp.3d at p. 76 [geofence search warrant application
23 granted].) In doing so, law enforcement “limit[s] the place to be searched in time and location,
24 and [presents a] warrant application [that] is not otherwise overly-broad, but [rather] confined to
25 the breadth of the probable cause that supports it.” (*Ibid.*, internal quotations omitted; see also,
26 *Virginia Shooting, supra*, 2022 WL 584326 at pp. 7-8 [geofence search warrant application
27 denied because the search zone was overbroad as to size, time, and location.]; *Arson, supra*, 497
28

1 F.Supp.3d 345 [geofence search warrant application approved because it was particular in time,
2 location, and scope.]

3 The Court is mindful that some of the information elicited during the two evidentiary
4 hearings, and contained within the stipulated testimony, may not have been available to the
5 affiant officer at the time of drafting the search warrant. The Court points out the deficiencies to
6 ensure that SFPD has guidance for future applications for geofence search warrants.

7
8 *a. Particularity as to Specific Offense.*

9 In his affidavit, Sergeant Farrell identified the specific offenses for which probable cause
10 had been established: a residential burglary and grand theft of personal property. As described
11 *supra*, Sergeant Farrell collected statements by Pham establishing his house had been burglarized
12 and surveillance footage supporting Pham's assertions. As such, the geofence warrant was
13 sufficiently particular as to the specific offense.

14
15 *b. Particularity as to the Items to be Seized.*

16 While Sergeant Farrell attempted to identify the specific items to be seized by their
17 relation to the crime, the text of the warrant failed to be sufficiently particular. In the geofence
18 context, because the items to be seized involved geolocation data, which corresponded closely
19 with a real physical location, the particularity of "the items to be seized" is closely tied to the
20 particularity of "the place to be searched." Some components of the items to be seized were
21 particularly described; others were not.

22 To begin, Sergeant Farrell correctly identified that the item to be seized was Location
23 History information. The warrant's text specifically provided that "Google Inc. SHALL provide
24 Cellular, GPS and Wi-Fi sourced *location history* for mobile devices that reported a location
25 within the geographical region(s) bounded by the listed latitude and longitude coordinates on the
26 date and time as stated on Appendix 'A'" (Exhibit D, p. 1, italics added.) As McInville's
27 testimony uncovered during this Court's evidentiary hearings, Location History data is collected
28 through cellular, GPS, Bluetooth, and Wi-Fi signals and networks. (Vol. 1, R.T. 10:14-18.)

1 Contrary to the Defendant’s argument, Location History is explicitly mentioned in the search
2 warrant affidavit.²³ Although Location History is explicitly mentioned, the Court notes that
3 Sergeant Farrell’s affidavit does not provide specific information as to Location History as a
4 Google service and how Google collects and stores users’ geolocation data in its Sensorvault
5 servers.

6 Sergeant Farrell’s geofence search warrant request reduced the scope of data that he
7 sought from the Sensorvault by both geographical and temporal constraints. These constraints
8 included the date of the crime, the three specific timeframes in which the suspects were visible
9 on the surveillance footage, and the specific residential address with longitude and latitude
10 coordinates. In so doing, he created a virtual filter to eliminate the majority of the 590 million
11 other users’ data in Sensorvault. As discussed later below, Sergeant Farrell’s efforts failed to
12 satisfy the Fourth Amendment’s particularity requirement because the geometric shape created
13 by law enforcement was not sufficiently narrow in scope.

14
15 *c. Particularity as to the Place to be Searched.*

16 The geofence context provided more than one “place” to be searched by law
17 enforcement. On the one hand was Google’s offices in Mountain View, CA, the physical
18 location to which law enforcement directed its demand. That physical location holds Google’s
19 Sensorvault servers, which hosts the geolocation data sought. On the other hand, was the San
20 Francisco location that directly corresponded with the alleged crime —the residential area where
21 the burglary occurred. Although the crime’s location did not involve any physical intrusions or
22 physical sweeps of the area by law enforcement, it did require a digital search of the area to
23 determine who was present during the commission of the crime. As to each location, law
24 enforcement was required to particularly describe the places to be searched.

25
26
27 ²³ In Exhibit D, the search warrant affidavit, references to Location History are found in the “Reverse Geolocation
28 Data” section, Appendix B, section (c), and the end of the “Probable Cause Statement” that repeats the information
from Appendix B, section (c). The Court does not refer to page numbers as the written page numbers appear to be
inconsistent and out of order at times.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

i. Google's HQ and Sensorvault Servers.

The first place to be searched, and the location explicitly described in the search warrant affidavit, was for "Google Inc.," located at "1600 Amphitheatre Parkway, Mountain View, CA 94093."²⁴ The geofence search warrant, however, failed to be more specific in identifying Google's Sensorvault servers as the location where the particular geolocation data would be found. The Court notes that the record failed to establish that Sergeant Farrell was personally aware that Google stored its geolocation data responsive to geofence search warrants in Sensorvault. The Court recognizes that this information was not information readily available to those who work outside of Google nor to those not familiar with our now-existing evidentiary record, including the testimony provided in *Chatrie*. The Court points this out so that SFPD is now aware and knows to provide this information in any future applications for geofence search warrants. This distinction is significant because the geofence search warrant cannot lawfully authorize a full-blown search of Google's entire headquarters, and all of its servers, when the data sought is known to be stored in one specific location—Sensorvault.

17
18
19
20
21
22
23
24
25
26

ii. Location of the Crime and Geometric Shape.

The next place to be searched was the general location of the crime. Sergeant Farrell did provide the precise residential address, along with longitude and latitude coordinates that corresponded with that general area. The Court recognizes that Sergeant Farrell did attempt to draft a sufficiently particular warrant. However, a general location of where a crime occurred is rarely ever sufficiently particular for Fourth Amendment purposes. In the geofence context, it is possible to cure this deficiency by creating a geometric shape that is narrowly crafted to encompass only the area where the crime actually occurred, as well as where suspects were known to have been present.²⁵ Ultimately, SFPD had an obligation to further reduce and narrow the quantity of devices that would be furnished as responsive to their geofence search warrant by

27
28

²⁴ According to Google's website, Google changed their name from INC to LLC in 2017. (Evid. Code, § 452, subd. (h).) Unless being used within a quotation, this Court will simply refer to the company as Google.

²⁵ The consideration for an appropriate geometric shape will ultimately be fact specific. Out of the geofence cases reviewed, many considered factors such as whether the area was a residential, commercial, or industrial area, whether a rural or urban area, whether the general population in the area was high density or low density.

1 narrowly crafting a geometric shape to exclude areas where the crime and suspects were not
2 present.

3 The geofence cases reviewed by this Court focused on the sizes and shapes of the
4 geometric shapes to determine whether the scope of the search was sufficiently particular. For
5 example, in *Chatrie, supra*, 2022 WL 628905 1, the federal district court was especially
6 concerned with law enforcement simply drawing a circle with a 150-meter radius in an urban
7 area encompassing the bank where the robbery occurred. (*Chatrie, supra*, 2022 WL 628905 at p.
8 11.) The geofence was equivalent to 17.5 acres, and touched on a nearby church, parking lot, and
9 wooded area. (*Ibid.*) This could have revealed devices that “may not have been *remotely* close
10 enough to the Bank to participate in or witness the robbery.” (*Id.* at p. 21, italics in original.)

11 Similarly, in *Virginia Shooting, supra*, 2022 WL 584326, the Virginia Circuit Court
12 denied the geofence search warrant application in part because the geometric shape was too
13 broad. (*Virginia Shooting, supra*, 2022 WL 584326 at p. 7.) There, surveillance footage recorded
14 a shooting, which occurred at the *front* of a motel. (*Ibid.*) However, the geofence search warrant
15 sought location information from the *entire* motel property and adjacent parking lots. (*Ibid.*) The
16 court indicated there was “no good reason to search patrons *beyond* the front area.” (*Ibid.*, italics
17 added.)

18 On the other hand, in *Arson, supra*, 497 F.Supp.3d 345, the federal district court
19 approved a geofence search warrant application because the geometric shape was sufficiently
20 narrow for Fourth Amendment purposes. (*Arson, supra*, 497 F.Supp.3d 345.) There, law
21 enforcement was investigating a series of arsons in six geofenced locations. (*Id.* at p. 353.) In
22 constructing their geofence, law enforcement “focus[ed] on the arson sites and the streets leading
23 to and from those sites. Residences and commercial buildings along the streets [were] excluded
24 from the geofence zones.” (*Id.* at p. 358.)

25 And in *D.C. Federal Crimes, supra*, 579 F.Supp.3d 62, the federal district court approved
26 a geofence search warrant where the geometric shape was narrow in scope. (*D.C. Federal*
27 *Crimes, supra*, 2021 WL 6196136 at p. 82.) The geofence shape encompassed only a portion of
28 the front half of the center, which is where the crime occurred, and its parking lot, which was

1 where the suspects had to have traveled through to enter the center. (*Ibid.*) The geofence was
2 constructed in a manner to exclude the business sharing the same building as the center and the
3 abutting road. (*Id.* at p. 85.) This was also an industrial area, not a congested urban area, and no
4 residences were within the geofence. (*Ibid.*)

5 In this case, the geometric shape used by Sergeant Farrell failed to be sufficiently narrow
6 in scope to the target location and was overbroad. As Sergeant Farrell testified at the second
7 evidentiary hearing, he could have limited the geometric shape to have excluded the neighboring
8 homes and to have only included the burglarized residence, in addition to the entire street area in
9 which the suspect vehicle traveled. (Vol. 2, R.T. 45:1-11; 59:4-60:11.) Instead, his geofence
10 design not only included the burglarized house, but five other private homes on the same block.
11 (See Exhibit D, Appendix A.) This deficiency in the warrant is critical because the geofence
12 intruded upon a residential neighborhood and included, within the geofence, innocent people's
13 homes who were not suspected to have any involvement in the burglary, either as a suspect,
14 victim or witness. "At the very core of the Fourth Amendment stands the right of a person to
15 retreat into his or her own home and there be free from unreasonable government intrusion."
16 (*Chatrie, supra*, 2022 WL 628905, at p. 18, internal brackets omitted, quoting *Silverman v.*
17 *United States*, 365 U.S. 505, 511.) Similarly, so to *Virginia Shooting, supra*, 2022 WL 584326,
18 Sergeant Farrell's "geofence search warrant application affirmatively target[ed] the location
19 information of the innocent" habitants and visitors of the neighboring residences along with the
20 suspects. (*Virginia Shooting, supra*, 2022 WL 584326 at p. 6.)

21 Further, the Court is mindful that within a geofence request, there is an inherent margin
22 of error and radius associated with the responsive devices as to whether the device will appear
23 inside or outside the geofenced area. At this time, the Court need not address the issue, as the
24 geometric shape alone fails to satisfy the particularity requirement and it is unclear whether the
25 margin of error was a fact available to the officer at the time of drafting the warrant. The Court
26 notes, however, that to the extent law enforcement can make clear specifications to Google in the
27 warrant to ensure that the responsive devices in the return have a reduced radius falling
28 significantly outside the geometric shape, they should do so. (See *Chatrie, supra*, 2022 WL

1 628905 at p. 14 [one device in the return had a confidence interval of roughly 387 meters, more
2 than twice the size of the original geofence].)

3
4 **iii. Time Periods.**

5 The geofence cases reviewed by this Court have consistently held that the geofence
6 requests should “narrow the timeframe [requested] to only the points at which evidence of a
7 crime could reasonably be found.” (*D.C. Federal Crimes, supra*, 579 F.Supp.3d at p. 81.) For
8 example, in *D.C. Federal Crimes, supra*, 579 F.Supp.3d, law enforcement sought “a total of 185
9 minutes of geofence data on 8 days across a five-and-a-half-month period.” (*Ibid.*) “[T]he time
10 windows requested by the government [were] closely keyed to the periods during which the
11 suspects were inside the [Redacted] center,” which the government knew by reviewing the
12 CCTV footage of when the suspects appeared and the time stamps on the footage. (*Ibid.*) “Thus,
13 the warrant [did] not seek location data for days or even hours to track the whereabouts of the
14 perpetrators, but rather location data that [was] tailored and specific to the time of the alleged
15 crimes only.” (*Ibid.*, quoting *Arson, supra*, 497 F.Supp.3d at p. 357.)

16 In this case, although there was a discrepancy in the time periods between Appendix A
17 and Appendix B, because the raw data in the return to the geofence search warrant reflects the
18 time periods consistent with Appendix A, the Court hereby adopts for review the three time
19 periods as specified therein. (Vol. 2, R.T. 26: 20-28) Further, the magistrate, in fact, authorized
20 150 minutes (2.5 hours) of geofence data on a single day, October 24, 2018. (See Exhibit D,
21 Appendix A & B.) Time Period One calls for a total of 30 minutes; Time Period Two calls for a
22 total of two hours.²⁶ The Court notes that this total duration of time is longer in only two of the
23 seven out-of-state geofence search warrants for which a written opinion exists. (*D.C. Federal*
24 *Crimes, supra*, 579 F.Supp.3d at p. 81 [authorizing approximately three hours of data in a
25 geofence request]; *Virginia Shooting, supra*, 2022 WL 584326, 1 (Va.Cir.Ct.) [authorizing
26 slightly under 3 hours of data in a geofence request].)

27
28 ²⁶ The Court notes that Time Period 2 essentially swallows Time Period 3, as provided in Appendix A. However,
even if the time periods had been followed as indicated in Appendix B instead, this would provide a buffer of only
20 minutes, which is rather insignificant in light of the time periods being so close to each other.

1 Despite the length of time sought by Sergeant Farrell and authorized by the Magistrate,
2 the time window was reasonable in this case. Specifically, the time frames closely correspond
3 with the time periods that the suspects were alleged to have either been casing the residence,
4 burglarizing the residence, or fleeing the residence with the stolen property. (Exhibit D; Vol. 2,
5 R.T. 60: 15-18.) For example, Time Period 1 captured time between 2:45 pm to 3:15 pm. In the
6 surveillance video, at 2:59 pm, Suspect #1 was observed exiting a vehicle and walking to Pham's
7 home. A minute later, he leaves. Thus, Time Period 1 was narrow in scope to capture Suspect #1
8 arriving to the scene and being present at the scene.

9 Time Period Two, on the other hand, ranged from 4:30 pm to 6:30 pm. The suspects were
10 recorded on the surveillance video outside of Pham's home at the following times: 4:42 pm, 5:43
11 pm, 5:53 pm, 6:06 pm, and 6:09 pm. The suspect vehicle was seen leaving the scene at 6:11 pm.
12 The time periods Sergeant Farrell requested in his search warrant were narrow in scope to match
13 those times that the suspects were casing and burglarizing the home. The warrant did not seek
14 location data for days or even hours to track the whereabouts of the perpetrators, but rather
15 location data that is tailored and specific to the time of the [alleged crimes] only." (*D.C. Federal*
16 *Crimes, supra*, 579 F.Supp.3d at p. 81, quoting *Arson, supra*, 497 F.Supp.3d at p. 357.) At no
17 point did the time periods become unreasonably broad to allow Sergeant Farrell to "follow"
18 suspects to their destination; rather, the time periods were limited to the times the individuals
19 were present at the scene.

20
21 **C. The Scope of the Three-Step Search Protocol Was Overbroad and Afforded**
22 **SFPD Unbridled Discretion Due to a Lack of Additional Judicial Review.**

23 As described in the Statement of Facts and explained in greater detail at the evidentiary
24 hearing, Sergeant Farrell's geofence search warrant application detailed a three-step²⁷ process by
25 which Google would be required to obtain and disclose Location History information that
26 satisfied the warrant's time and location parameters. In Step One, law enforcement received
27 geolocation data pertaining to the date, time, and location provided in the geofence search

28

²⁷ Mr. McInville refers to these as "stages" as well as "steps".

1 warrant. In Step Two, from the devices responsive in Step One, law enforcement selected the
2 devices they believed to be relevant to their investigation and requested additional data. The
3 additional data extended beyond the bounds of the geofence and included 45 minutes before and
4 after the specified time periods. In Step Three, law enforcement would select which device to
5 unmask and obtain subscriber information.

6 The Court finds that nowhere does the warrant's text require law enforcement to return to
7 the Court and permitted law enforcement to demand additional data *at law enforcement's*
8 *discretion*. In executing this geofence search warrant, Sergeant Farrell exercised that discretion
9 to demand Step Two and Step Three data *without additional judicial authorization*. This three-
10 step process afforded law enforcement unbridled discretion, and at each step, law enforcement
11 should have returned for additional judicial review and authorization.

12 13 1. Step Two Data Required Judicial Authorization.

14 The warrant's text allowing law enforcement to request Step Two data afforded too much
15 officer discretion with no judicial review and authorization. The federal district court in *Chatrie*,
16 *supra*, 2022 WL 628905, points out the same concerns this Court holds in regard to this warrant:

17
18 This warrant, for instance, contains no language objectively identifying *which*
19 accounts for which officers would obtain further identifying information. Nor does
20 the warrant provide objective guardrails by which officers could *determine* which
21 accounts would be subject to further scrutiny. Nor does the warrant even simply
22 limit the number of devices for which [law enforcement] could obtain identifying
information. Instead, the warrant provided [law enforcement] unchecked discretion
to seize more intrusive and personal data with each round of requests –without ever
needing to return to a neutral and detached magistrate for approval.

23 (*Chatrie, supra*, 2022 WL 628905 at p. 25.)

24 Returning to the magistrate is critical in the geofence context, as the return to Step One
25 may yield zero accounts, five accounts, fifteen accounts, or fifty accounts. It is difficult for the
26 magistrate to know how many accounts may be returned as responsive at the time of signing the
27 warrant and will ultimately vary from case-to-case. Further, whether it is reasonable for law
28 enforcement to obtain Step Two data for specific devices will ultimately turn on the facts of that

1 investigation. The discretion to select which devices for which Google must provide additional
2 Step Two data should fall on the judiciary, not the executive, to ensure that the selection process
3 comports to the Fourth Amendment's reasonableness requirement. (*Ibid.*) Thus, without
4 additional safeguards in place, this would essentially permit exploratory rummaging of innocent
5 people's location information.

6
7 2. Step Three's Unmasking of the Suspect Device Required Judicial
8 Authorization.

9 The Court further finds that the warrant's text allowing law enforcement to select which
10 devices to unmask without judicial review and authorization further provided unbridled
11 discretion. This is consistent with *D.C. Federal Crimes, supra*, 579 F.Supp.3d 62, which
12 ultimately required law enforcement to return to the judiciary to unmask a suspected device.
13 (*D.C. Federal Crimes, supra*, 579 F.Supp.3d at pp. 88-90; see also *Chatrie, supra*, 2022 WL
14 628905 at p. 25 [extending the finding of unbridled discretion to the unmasking procedure in
15 Step Three].) In *D.C. Federal Crimes*, the federal district court indicated that it had first rejected
16 a geofence search warrant application that did not require law enforcement to return to unmask a
17 suspected device. (*Id.* at p. 88.) The district court approved law enforcement's second request,
18 which included as a second-step²⁸ the need for law enforcement to return to unmask a suspected
19 device and obtain identifying information. (*Id.* at pp. 88-89.)

20 The district court granted this geofence search warrant application because it:

21
22 eliminated law enforcement's discretion ... by requiring it to return to the Court
23 and justify any device deanonymization based on its review of the anonymized
24 information provided by Google and other evidence in the case. [Citation.] This
25 second step serves two functions. First, it delimits the government's discretion in
26 the search and seizure process. The government is free to choose the devices for
27 which it seeks identifying information, but the ultimate decision as to which
28 subscribers, if any, Google will be compelled to identify lies with the Court.
[Citation.] The second step also ensures that the government's search is
particularized; that is, before any identifying information is disclosed to the

²⁸ Unlike the warrant in this case, the *D.C. Federal Crimes* geofence search warrant did not have a step for requesting additional geolocation data of select devices. In comparison to our warrant, it only provided for Step One and Step Three data.

1 government, it must justify the specific devices for which it seeks that information,
2 consistent with its showing of probable cause.

3 (*D.C. Federal Crimes, supra*, 579 F.Supp.3d at pp. 88-89.)

4 Further, the district court held that this additional process “ameliorate[d] possible
5 overbreadth concerns.” (*Id.* at p. 89.) In part, it ensured that the devices “not likely to be relevant
6 to the investigation” remain anonymized. (*Id.* at pp. 89-90.) And in specific situations where
7 there is a:

8 geofence that returns a larger number of anonymized devices than expected, and
9 which cannot be further narrowed by law enforcement to make the result useful...
10 additional justification for such request can be required. In other words, the two-
11 step process can serve as a court-supervised filter, winnowing geofence results that
12 are unlikely to provide useful evidence to the government, thereby further
minimizing third-party privacy concerns.

13 (*D.C. Federal Crimes, supra*, 579 F.Supp.3d at p. 990.) Thus, this Court finds that in the
14 geofence search warrant context, law enforcement needs to return for additional judicial
15 authorization for unmasking a suspect device and obtaining identifying information. As the
16 geofence search warrant’s text did not require Sergeant Farrell to return for an additional
17 warrant to unmask, the Court finds that that geofence search warrant was overly broad and
18 afforded Sergeant Farrell unbridled discretion.

19
20 **D. Conclusion.**

21 Ultimately, this Court does not find that a geofence search warrant can never pass Fourth
22 Amendment muster, rather, this specific geofence search warrant was not sufficiently particular
23 and was overly broad. The Court’s finding is based on the geometric shape not having been
24 narrowly tailored to exclude the other residential homes belonging to innocent people with no
25 connection to the crime. The Court also found the warrant to afford too much discretion during
26 the execution of the warrant because at no point, between each step, did law enforcement return
27 for additional judicial oversight. Each step of this warrant procedure should be broken down into
28

1 separate warrants with law enforcement establishing probable cause to a neutral magistrate at
2 each step.

3
4 **V. SERGEANT FARRELL ACTED IN GOOD FAITH IN SEEKING THE JUDGE'S**
5 **APPROVAL FOR THE GEOFENCE SEARCH WARRANT.**

6 The People have the burden of proving objectively reasonable reliance to support
7 application of the good faith exception to the exclusionary rule. (*People v. Willis* (2002) 28
8 Cal.4th 22, 36-37; *People v. Camarella, supra*, 54 Cal.3d at p. 596.) Evidence seized by an
9 officer who is reasonably relying on the validity of a search warrant will not be excluded even if
10 the warrant is later determined to have been issued without probable cause. (*United States v.*
11 *Leon* (1984) 468 U.S. 897, 922 (*Leon*); *People v. Lopez* (1985) 173 Cal.App.3d 125, 139-142;
12 *People v. MacAvoy* (1984) 162 Cal.App.3d 746, 759-765.) The exclusionary rule is designed to
13 deter the misconduct of police, not the errors of judges and magistrates. (*Leon, supra*, 468 U.S. at
14 p. 3418.)

15 In the seminal *Leon* decision, the United States Supreme Court held evidence seized
16 pursuant to a search warrant should be suppressed only on a case-by-case basis and only in those
17 unusual cases in which exclusion will further the purposes of the exclusionary rule. The purpose
18 of the exclusionary rule, namely, a deterrent effect on police conduct, is not well served where
19 “an officer acting with objective good faith has obtained a search warrant from a judge or
20 magistrate and [has] acted within its scope,” even though later review of the warrant found it
21 legally insufficient. (*Leon, supra*, 468 U.S. at p. 920.) The Court further noted that the very fact
22 that the officer is acting on a warrant issued by a neutral and detached magistrate normally
23 suffices to establish that the officer is acting in good faith. (*Id.* at p. 922; see also *Messerschmidt*
24 *v. Millender* (2012) 565 U.S. 535, 546; *United States v. Ross* (1982) 456 U.S. 798, 823, fn. 32.)

25 The High Court in *Leon* found suppression of evidence seized pursuant to a warrant
26 lacking probable cause is appropriate in only limited circumstances; for example, when officers
27 mislead a magistrate by dishonest or reckless statements in the affidavit; or when the issuing
28 magistrate wholly abandoned its judicial role; or where the affidavit is “ ‘so lacking in indicia of

1 probable cause as to render official belief in its existence entirely unreasonable;’ ” or where a
2 warrant is so facially deficient in describing the place to be searched or items to be seized an
3 executing officer could not presume it to be valid. (*Leon, supra*, 468 U.S. at p. 923; see also
4 *Messerschmidt v. Millender, supra*, 565 U.S. at p. 547.)

5 When a warrant is challenged on the grounds of lack of probable cause, the “good faith”
6 test becomes “whether a reasonable and well-trained officer ‘would have *known* that his affidavit
7 failed to establish probable cause and that he should not have applied for the warrant.’

8 [Citation.]” (*People v. Camarella* (1991) 54 Cal.3d 592, 605-606, italics in original.) When the
9 affidavit presents only a close or debatable question on the issue of probable cause, however, an
10 officer can reasonably rely on the magistrate’s warrant. (*Id.* at p. 606; *People v. French* (2011)
11 201 Cal.App.4th 1307, 1323-1325; *People v. Romero* (1996) 43 Cal.App.4th 440, 447; but see,
12 e.g., *People v. Hulland* (2003) 110 Cal.App.4th 1646, 1653-1656 [good faith did not apply to
13 warrant issued based upon stale information]; *People v. Gotfried* (2003) 107 Cal.App.4th 254,
14 265 [officer should have known affidavit lacked sufficient corroboration].) In addition, “the fact
15 that the officers sought and obtained approval of the warrant application from a superior and a
16 deputy district attorney before submitting it to the magistrate provides further support for the
17 conclusion that an officer could reasonably have believed that the scope of the warrant was
18 supported by probable cause.” (*Messerschmidt v. Millender, supra*, 565 U.S. at p. 553.)

19 Here, the Court finds that the good faith exception applies to Sergeant Farrell when he
20 obtained judicial authorization for the geofence search warrant. The record contains many
21 reasons to support this finding. First, this geofence search warrant, which was signed by Judge
22 Bolanos, was one of four total warrants issued in the investigation of this case. This suggests that
23 not only did Sergeant Farrell continue returning for judicial authorization each step of the way,
24 but that the geofence search warrant provided him with limited information that required him to
25 seek additional warrants.

26 Second, Sergeant Farrell testified that the geofence search warrant at issue in this case
27 was not the first geofence search warrant for which he had sought judicial authorization; rather,
28 this warrant was his third or fourth. In the two or three geofence search warrants he authored

1 prior to this one, all were signed by a judge. Thus, Sergeant Farrell reasonably believed that he
2 could continue to obtain a valid geofence search warrant and that the geofence search warrant, as
3 drafted, was lawful under the Constitution and statutory authorities. He was, after all, relying on
4 prior judicial authorizations.

5 Third, Sergeant Farrell also testified that after this warrant was issued, a Google
6 employee came to provide SFPD with training specifically in geolocation. This further suggests
7 that at the time the 2018 geofence search warrant was authored, the scope of information
8 available to Sergeant Farrell as to how the technology functioned was limited.

9 Fourth, nothing in the record suggests Sergeant Farrell acted in bad faith with the
10 intention of deceiving the magistrate or that he acted with reckless disregard for the truth. Aside
11 from the few other geofence search warrants he obtained, Sergeant Farrell had the experience of
12 having authored 300 to 400 non-geofence search warrants. Prior to seeking this geofence search
13 warrant, he did have a conversation with two other law enforcement officers to discuss how they
14 understood geofence warrants at that time. And to be clear, there was no appellate opinion on
15 geofence search warrants in 2018. This continues to be a novel issue even at this time, as no
16 appellate court in California has weighed in on the issue, and neither has any federal appellate
17 court.

18 In conclusion, the Court finds that Sergeant Farrell acted in good faith, and that the
19 evidence cannot be suppressed under the Federal Constitution. As discussed later below,
20 however, the Court finds that the good faith doctrine cannot be extended to a violation of
21 CalECPA.

22 **VI. THE GEOFENCE WARRANT ISSUED FOR DEFENDANT'S GEOLOCATION**
23 **DATA VIOLATED CALECPA'S STATUTORY MANDATE, BARRING THE**
24 **APPLICATION OF THE GOOD FAITH DOCTRINE, AND REQUIRING THE**
25 **GEOLOCATION EVIDENCE TO BE SUPPRESSED.**

26 Defendant argues that geofence search warrants can never be issued because they fail to
27 identify a target individual or account, and therefore, violate CalECPA. Defendant further argues
28 that the listed criteria of CalECPA's particularity requirement was violated. This Court disagrees

1 and instead finds that CalECPA’s express statutory language authorizes a magistrate, in
2 appropriate circumstances, to issue a geofence search warrant. The Court, however, finds that the
3 geofence search warrant issued in this case did violate CalECPA’s particularity provisions, and
4 therefore, the evidence must be suppressed under state law.

5
6 **A. CalECPA’s Statutory Language Suggests a Legislative Intent to Permit**
7 **Warrants That Do Not Identify a Target Individual.**

8 The Court disagrees with Defendant’s proposition that CalECPA will always prohibit the
9 issuance of a geofence search warrant simply because the suspect’s identity is unknown.
10 CalECPA provides the following particularity requirement for search warrants pertaining to
11 electronic information:

12 The warrant shall describe with particularity the information to be seized by
13 specifying, *as appropriate and reasonable*, the time periods covered, the target
14 individuals or accounts, the applications or services covered, and the types of
15 information sought, provided, however, ... the court may determine that it is not
16 appropriate to specify time periods because of the specific circumstances of the
investigation, including, but not limited to, the nature of the device to be searched.

17 (Pen. Code, § 1546.1, subd. (d)(1), italics added.) CalECPA essentially requires the warrant to
18 describe the target of the search: that is, “the information to be seized.” (*Ibid.*) Thus, whether
19 “the time periods covered, the target individuals or accounts, the applications or services
20 covered, and the types of information sought,” need to be described is dependent on the kind of
21 data that is sought. This will ultimately vary and change depending on what kind of electronic
22 information is at issue (i.e. geolocation data, emails, private messages, etc.).

23 Next, although the statute expressly lists which items should be described with
24 particularity, the requirement is tempered by the language, “*as appropriate and reasonable.*” The
25 “appropriate and reasonable” inclusion requires the Court to examine the particular context in
26 which law enforcement seeks a warrant. In the geofence search warrant context, it is appropriate
27 and reasonable to require the geofence search warrant to provide the relevant time periods of
28 when the suspects were known to be present, the relevant location(s) where the suspects were

1 known to be present, the type of service covered (a Google account), and the type of information
2 sought from the Google account (Location History geolocation data). On the other hand, it is not
3 appropriate nor reasonable to require law enforcement to specify a specific suspect's account or
4 name, as that is the purpose of the search—to identify an otherwise unknown culprit. Law
5 enforcement does not have reasonable access to this information and simply cannot provide it.

6 Moreover, the State Legislature created through CalECPA an explicit procedure outlining
7 the government's notice requirement for warrants issued *without an identified suspect*. In Penal
8 Code section 1546.2, subdivision (c), CalECPA provides the following procedure regarding its
9 notice requirement:

10
11 *(c) If there is no identified target of a warrant or emergency access at the time of*
12 *its issuance, the government entity shall submit to the Department of Justice within*
13 *three days of the execution of the warrant or issuance of the request all of the*
14 *information required in subdivision (a). If an order delaying notice is obtained*
15 *pursuant to subdivision (b), the government entity shall submit to the department*
16 *upon the expiration of the period of delay of the notification all of the information*
17 *required in paragraph (3) of subdivision (b). The department shall publish all those*
18 *reports on its Internet Web site within 90 days of receipt. The department may*
19 *redact names or other personal identifying information from the reports.*

20 (Pen. Code, § 1546.2, subd. (c).) In other words, the State Legislature intended to permit, not
21 prohibit, search warrants for electronic information with no identified targets. When coupled
22 with the language of section 1546.1, subdivision (d)(1), “as appropriate and reasonable,”
23 CalECPA’s express language essentially allows geofence warrants to be permissible even though
24 there is no identified target at its issuance.²⁹ Therefore, the Court rejects Defendant’s argument
25 that CalECPA’s statutory language prohibits geofence search warrants from ever being issued.

26
27
28 ²⁹ To briefly note, this is consistent with the rest of the Penal Code when read together. For example, in the context
of an arrest warrant, Penal Code section 815 provides: “A warrant of arrest shall specify the name of the defendant
or, *if it is unknown* to the magistrate, judge, justice, or other issuing authority, the defendant may be designated
therein *by any name*.” In the context of a regular search warrant, Penal Code section 1525 provides: “A search
warrant cannot be issued but upon probable cause, supported by affidavit, *naming or describing the person to be*
searched or searched for...” As indicated by our Supreme Court, when “a name that would reasonably identify the
subject to be arrested cannot be provided, then some other means *reasonable to the circumstances* must be used to
assist in the identification of the subject of the warrant.” (*People v. Robinson* (2010) 47 Cal.4th 1104, 1131.)

1 **B. The Geofence Search Warrant Issued in This Case Failed to Satisfy CalECPA’s**
2 **Statutory Particularity Requirements.**

3 The Court finds that the geofence search warrant issued in this case failed to satisfy
4 CalECPA’s statutory particularity requirements. A geofence search warrant must specify, “*as*
5 *appropriate and reasonable*, the time periods covered, the target individuals or accounts, the
6 applications or services covered, and the types of information sought....” (Pen. Code, § 1546.1,
7 subd. (d)(1).) The Court notes that, at this time, there is no published appellate court opinion on
8 point that has interpreted this provision, so the Court applies a plain reading of the statute to the
9 facts of this case. The Court will discuss each listed requirement in Penal Code section 1546.1,
10 subdivision (d)(1) in turn to demonstrate how the warrant satisfied CalECPA in some parts but
11 failed in another.

12 The Court first begins with the parts that were satisfied. First, “the time periods covered”
13 were specified in the geofence search warrant. Appendix A to the geofence search warrant
14 provided a single date and three relevant time periods. Specifically, the time frames closely
15 corresponded with the time periods that the suspects were alleged to have either been casing the
16 residence, burglarizing the residence, or fleeing the residence with the stolen property. (Vol. 2,
17 R.T. 60: 15-18.) As explained in the Court’s Fourth Amendment analysis, the Court finds that
18 the time periods sought by Sergeant Farrell were appropriate and reasonable. Thus, the “time
19 periods covered” requirement is satisfied under CalECPA.

20 Next, “the applications or services covered” was also specified. The services are provided
21 by Google, which pertains to users’ Google accounts. The specific service, Location History, is
22 mentioned throughout the warrant. There was no testimony that Location History has its own
23 unique application; rather, it can be accessed through different ways and is not limited to an
24 application. Thus, the “applications or services covered” requirement is satisfied under
25 CalECPA.

26 Further, “the types of information” sought is Location History information, which was
27 more than adequately described. The search warrant affidavit described how the data is collected
28

1 (i.e. GPS, cellular, Bluetooth, and Wi-Fi), how often it is collected, and that Google retains this
2 data for business advertising. Thus, “the types of information” requirement is satisfied.

3 The Court next turns to the part that was not satisfied. Specifically, that “the target
4 individuals or accounts” or individuals or accounts expected to be included inside the geofence
5 were not reasonably specific enough in this geofence search warrant as required under CalECPA.
6 Because of the nature of a geofence warrant, the “target individuals or accounts” will never be
7 specified or described with pinpoint particularity because law enforcement only knows that the
8 target is a suspect who committed a crime on a particular date, at a particular time and in a
9 particular location. Instead, the issue for a reviewing magistrate is whether, given the specific
10 facts presented by the law enforcement affiant, the geofence created would be appropriate and
11 reasonable in its goals in catching potential suspects while also not sweeping up innocent
12 civilians. This analysis is substantially affected by the size of the geometric design, the density of
13 the area, and whether it’s urban, residential, commercial, or industrial in nature.

14 The Court concludes that the geofence warrant in this case was neither appropriate nor
15 reasonable as to the scope of potential individuals or accounts that were susceptible to be
16 ensnared by the geofence warrant. To the contrary, given the size and the residential nature of the
17 geofenced area, which included innocent peoples’ homes who were not suspected to have any
18 involvement in the burglary, either as a suspect, victim or witness, this deficiency was fatal to the
19 CalECPA particularity requirement. Thus, the “target individuals or accounts” requirement was
20 not satisfied under CalECPA, and therefore, CalECPA requires suppression of the geolocation
21 evidence.

22 To be clear, this Court is not holding that a geofence warrant can never satisfy
23 CALECPA. After all, a target individual will never be known to law enforcement in the
24 geofence context, otherwise, law enforcement would simply secure a search warrant for that
25 specific person alone. Similarly, because the individual’s identity is unknown, law enforcement
26 will never have a target Google account either. The entire purpose of a geofence warrant is to
27 *identify* suspects present at the scene of the crime and from there to execute a series of additional
28 search warrants to further narrow the scope of the investigation. The fatal deficiencies in

1 Sergeant Farrell's warrant were the size of the geometric design for the densely populated
2 residential neighborhood in which this net was cast. In circumstances with a more finely drawn
3 geometric shape or warrants seeking information from a rural, industrial or low-density area, for
4 example, might very well satisfy CAELECPA requirements of reasonable and appropriate.

5
6 **C. Because There is a Statutory Violation of CalECPA, the Good Faith Doctrine**
7 **Cannot be Extended and the Geolocation Evidence Must be Suppressed.**

8 Because the particularity requirement of CalECPA was violated in respect to the "target
9 individuals or accounts" under Penal Code section 1546.1, subdivision (d)(1), the Court finds
10 that the good faith doctrine cannot be extended to a violation of this state law. The Court agrees
11 with Defendant's cited-to authority in *People v. Jackson* (2005) 129 Cal.App.4th 129. The
12 People failed to address and provide a justification supported with authority that the good faith
13 doctrine can be extended to a statutory violation that includes its own suppression remedy.

14 In *People v. Jackson* (2005) 129 Cal.App.4th 129, 153, 160, the Second District Court of
15 Appeal held that the good faith doctrine cannot be extended to a statutory violation of the state's
16 wiretap statutes (Pen. Code, § 629.50-629.98). In *Jackson*, a trial court granted an application by
17 the Los Angeles County District Attorney to intercept telephone conversations to and from a
18 detention facility for a period of 30 days. (*Jackson, supra*, 129 Cal.App.4th at p.143.) The
19 defendant in *Jackson* ultimately contested that "the applications for the [wiretap] order ... failed
20 to demonstrate compliance with the statutory prerequisites for a wiretap, and the magistrates
21 issuing the wiretap orders failed to make the statutorily required findings and failed to include
22 the statutorily required provisions in the orders." (*Ibid.*) The wiretap statutes include the
23 following suppression remedy:

24
25 Any person in any trial, hearing, or proceeding, may move to suppress some or all
26 of the contents of any intercepted wire or electronic communications, or evidence
27 derived therefrom, only on the basis that the contents or evidence were obtained in
28 violation of the Fourth Amendment of the United States Constitution *or of this*
chapter. The motion shall be made, determined, and be subject to review in
accordance with the procedures set forth in Section 1538.5.

1 (Pen. Code, § 629.72, italics added.)

2 The *Jackson* court ultimately declined to extend the good faith doctrine under *U.S. v.*
3 *Leon* (1984) 468 U.S. 897, finding that it “is a judicially crafted exception to an exclusionary
4 rule that is a judicial creation,” whereas, suppression under the wiretap statute was “required by
5 mandate.” (*Id.* at p. 153.) Moreover, while Penal Code section 629.86 provided a “good faith
6 reliance on a court order” as a complete defense to criminal or civil liability, it did not do so in
7 the context of a motion to suppress unlawfully obtained evidence. (*Id.* at p. 154.) Thus, the
8 appellate court held that the Legislature deliberately chose not to incorporate a good faith
9 exception into the statutory exclusionary rule. (*Ibid.*)

10 Similarly, CalECPA’s express language provides a suppression remedy for a violation of
11 CalECPA itself that mirrors the wiretap statute’s suppression remedy in *Jackson, supra*, and is
12 not limited to enforcing a Fourth Amendment violation. CalECPA specifically provides:

13
14 Any person in a trial, hearing, or proceeding may move to suppress any electronic
15 information obtained or retained in violation of the Fourth Amendment to the
16 United States Constitution *or of this chapter*. The motion shall be made,
17 determined, and be subject to review in accordance with the procedures set forth in
18 subdivisions (b) to (q), inclusive, of Section 1538.5.

18 (Pen. Code, § 1546.4, subd. (a), italics added.) By using the words “or of this chapter,” the
19 Legislature intended to expand a defendant’s suppression remedy to beyond the reaches of the
20 Fourth Amendment.

21 Moreover, upon review of other provisions in CalECPA, a good faith exception is built-
22 into the statute for narrow circumstances. (Pen. Code, § 1546.1, subd. (c)(6) [emergency of death
23 or serious physical injury], (c)(7) [lost, stolen, or abandoned devices].) Thus, the State
24 Legislature certainly was aware of the good faith doctrine in drafting CalECPA and chose to
25 exclude it from generally applying, absent the narrowly defined circumstances.

26 As such, the Court finds that, as a matter of law, the good faith doctrine does not apply to
27 a violation of CalECPA’s statutory requirements under Penal Code section 1546.1, subdivision
28 (d)(1). The Court reiterates the finding that Sergeant Farrell acted in good faith, but is cognizant

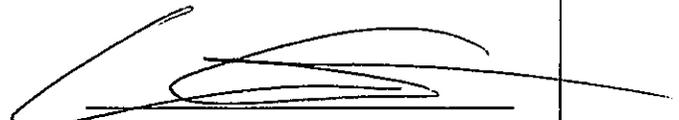
1 that CalECPA, unlike Fourth Amendment jurisprudence, does not have a good faith exception
2 built into the statute.

3
4 **CONCLUSION**

5 For the above stated reasons, the motion to quash the search warrant is **GRANTED** and
6 the geolocation evidence pertaining to Defendant Dawes seized from this search warrant is
7 ordered suppressed.

8
9 **IT IS SO ORDERED.**

10
11 9/30/2022
12 Date

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Hon. Linda Colfax
Judge of the Superior Court