Manohar Raju
Public Defender
City and County of San Francisco
Matt Gonzalez
Chief Attorney
Sierra Villaran, 306949
Deputy Public Defender
Brett Diehl
Certified Law Student
555 Seventh Street
San Francisco, CA 94103
Direct: (415) 553-9643
Main: (415) 553-1671
Sierra.villaran@sfgov.org

Attorneys for Defendant
LAQUAN DAWES

SUPERIOR COURT STATE OF CALIFORNIA
CITY AND COUNTY OF SAN FRANCISCO

People of the State of California, Plaintiff, vs. **Laquan Dawes,** Defendant.	Court No: 19002022 **Motion to Quash and Suppress Evidence under Penal Code §§ 1538.5 and 1546** **Date:** 07/07/2020 **Time:** 9:00am **Dept:** 11 (To Set)

LaQuan Dawes, through counsel, moves the Court to quash the warrant issued in this matter on December 4th, 2018. This "geofence" warrant authorized San Francisco Police Officers to obtain the cell phone location data for every Google user who happened to be in the vicinity of 1447 42nd Avenue on the afternoon of October 24, 2018. It then permitted the police to get additional and more extensive location data for six specific users. The geofence

warrant issued in this case is both an unlawful and an unconstitutional general warrant. It is overbroad and lacks the particularity required by the Fourth Amendment. The Court should quash the warrant.

Introduction

The San Francisco Police Department obtained LaQuan Dawes's personal information using what has been termed a "geofence" warrant. While it is not unusual for law enforcement to request and receive cell phone location data via warrant, a geofence warrant is uniquely different from a standard cell phone data warrant. This new type of warrant requires Google to produce data for every single device that is using Google location services within a certain area and at a particular time. Unlike all other warrants for personal cell data, which requests data for a particular user, number, or account—these geofence warrants do not have a particular user in mind.

Here, the warrant did not present Mr. Dawes as a suspect under investigation or mention his name in any way. San Francisco Police had no suspects in alleged burglary, so they wrote a warrant that would compel Google to act as a detective for them. The warrant they authored does not specify the name or identity of any of the people whose personal information was searched as a result of this warrant. Instead, the warrant works backwards: it chose a location and time and then required Google to comb through a huge amount of private data—held in what they call the "Sensorvault"—to find any and all devices that were using Google location services in that area or time. It then required Google to hand over all of that data to the San Francisco Police Department. Officers then had complete discretion and no oversight as they looked through the data and requested additional, private information from devices they deemed relevant.

This is the definition of a modern-day incarnation of a "general warrant," and it is strictly prohibited by the Fourth Amendment. People using their cellphones or devices have a reasonable expectation of privacy in their location

data—it is sensitive information and reveals the "privacies of life" for users.[1] It shows when and where people are in their homes, their places of worship, or in hotel rooms. These are constitutionally protected spaces. The ability to access data that can locate an individual quickly, cheaply, and retroactively is an unprecedented expansion of law enforcement power and is certainly a search within the meaning of the Fourth Amendment.

Geofence warrants like the one issued in this case are incapable of satisfying the probable cause and particularity requirements of the Fourth Amendment—and the fact that law enforcement obtained a warrant in this matter does not save the search from being constitutionally invalid. The warrant here fails to establish probable cause and establish particularity to search Mr. Dawes's Sensorvault data. Even assuming that Google phones and services are commonplace, there were no facts contained within the affidavit here to establish that those involved with the home invasion used either a Google device or an application—ever or at the time of the burglary. The government's generalizations about cell phone use, without any specific factual nexus to the allegations in this case, are insufficient to establish probable case for the sweeping search that was done here. Permitting this type of invasive and overbroad request would gut Fourth Amendment protections. For these reasons, the Court must quash the warrant and suppress the evidence obtained from the geofence warrant in this matter.

How a Geofence Warrant Works

It is common for law enforcement to compel Google, via warrant, to disclose records related to a particular user's account—including data about that user's location and movement during a particular time of interest.[2] These warrants identify a specific person of interest in a criminal investigation and

---

[1] *Carpenter v. United States,* 138 S. Ct. 2206, 2214 (2018).

[2] Exhibit A: "Google Amicus", *filed in United States v. Chatrie,* 19-cr-00130 (E.D. Va. Dec. 20, 2019) (ECF No. 59-1) at 2-3.

compel only information about that specific person.

A geofence warrant is something else entirely. As described by Google, "[r]ather than seeking information relating to a known suspect or person of interest, these requests broadly seek to identify all Google LH [location history] users whose LH data suggests that they were in a given area in a given timeframe—even though law enforcement has no particularized basis to suspect that all of those users played a role in, or possess any information relevant to, the crime being investigated."[3] This type of warrant requires Google to conduct a "broad and intrusive" search across all Google users' location history information.[4]

Essentially, instead of only requesting data about whether "John Doe's" cellphone was at a certain Whole Foods on January 1, 2020, between 6 pm and 8 p.m.., a geofence warrant requests information about **every single person** whose cellphone or device passed through the Whole Foods on January 1, 2020, between 6 and 8 p.m.. Google takes the location and timeframe provided by law enforcement and has to search its entire database of location history to determine which users' devices might have been present in that area at that time.[5] This is a search of a massive scale.

The information being provided is also of a highly sensitive nature. Location history information is "essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travel...by enabling and using LH, a Google user can keep a virtual journal of her whereabouts over a period of time....The Timeline might reflect, for instance, that the user left her home on Elm Street in the morning and walked to the bus stop, took the bus to her office on Main Street, walked to a nearby

---

[3] Exhibit A: "Google Amicus" *supra* at 3.

[4] Id at 4.

[5] Id at 11-12.

coffee shop and back to the office in the afternoon, and then went to a nearby restaurant in the evening before returning home by car."[6]

This is deeply personal and private information. These geographic areas include private homes, government buildings, and places of worship. And this information is being provided not for one, specific user—but for all of us who happen to be using Google location services in that area at that time.

This data is also substantively different from other location history data that has been previously considered by the US Supreme Court. In *Carpenter*, the Court emphasized the revealing nature of "cell site location information,"[7] (CSLI) but also noted that CSLI is a collection of time-stamped records that are automatically generated by a wireless carrier, Verizon-for example, whenever a phone connects to a physical cell site.[8] Carriers like Verizon maintain these records for their own business purposes—identifying spots of bad service or roaming rates. Thus, when law enforcement askes for this cell service location information, it is asking carriers like Verizon to turn over their automatically generated business records relating to when a device connected to a cell site.

By contrast, Google location history information "is controlled by the user, and Google stores that information in accordance with the user's decisions."[9] It is not automatically generated and it is not a business record being stored and used for the sake of Google. A user is entrusting Google to safeguard his or her "journal" in the Sensorvault—and this is the information being compelled by a geofence warrant. It is more personal, more detailed, and more specific. And the search that is done is broader and more intrusive than a traditional cell service location inquiry.

---

[6] Id at 6.

[7] *Carpenter v. United States, supra,* 138 S. Ct. at 2219.

[8] Id at 8.; *Carpenter* 138 S.Ct. at 2211-2212.

[9] Id at 9.

Memorandum of Points and Authorities

STATEMENT OF THE CASE

Laquan Dawes was arrested on February 6, 2019, by the San Francisco Police Department on an outstanding Ramey warrant, issued on January 28, 2019. Dawes is now charged with a violation of Penal Code section 459 (first degree burglary) with an allegation under Penal Code section 667.5(c)(21) (hot prowl); and with a violation of Penal Code section 487(a) (grand theft).

STATEMENT OF FACTS

Surveillance footage captures four unknown suspects before and during a reported burglary on October 24, 2018

On October 24, 2018, a residential burglary was reported at 1447 42nd Avenue in San Francisco. Nearby security cameras recorded a male suspect (S1) arrive in a four-door sedan, walk to 1447 42nd Avenue, and then return to the car before driving away a minute later. Almost two hours later, a second suspect (S2) is seen walking toward 1447 42nd Avenue and then leaving. An hour after that, footage shows a new, different four-door sedan arrive. The same two male suspects from before, S1 and S2, get out of the new car. There are two, different men who remain inside the new car. S1 and S2 are seen walking back and forth from 1447 42nd Avenue and the four-door sedan, carrying items. No suspects were identified from the video footage nor were there any discernable license plate numbers pulled for either involved vehicle.

Having made no identifications of the suspects, Sergeant Farrell requests a broad, reverse geolocation search for Google customer data.

On October 30, 2018, Sgt. Farrell of SFPD circulated a crime alert with screenshot images of the burglary suspects to surrounding law enforcement departments. As of December 3, 2018, Sgt. Farrell had received no responses.

On December 4, 2018, Sergeant Farrell authored a search warrant affidavit for reverse geolocation data from Google, Inc. in relation to this incident. This warrant cast a wide net, requesting all location history based on cellular, Global Positioning System ("GPS"), and Wi-Fi data for every mobile device within half a block of 1447 42nd Avenue on October 24, 2018. Sgt Farrell asked for:

> *"Google to conduct a search of all Android enabled mobile devices that recorded location data within the geographical area of 1447 42nd Avenue..."*[10]

The warrant requested all mobile device data from during and around the time of the reported burglary.[11] Specifically, for every single device that passed through the search area at any moment between 2:45 p.m. and 3:15 p.m., 4:30 p.m. and 5:00 p.m., and 5:20 p.m. and 6:30 p.m.

The warrant requests location information related to Google accounts. No specific applications, such as Gmail, Google Maps, Play Store, etc. are requested—instead the warrant discusses "Android enabled mobile devices."

The reason for this request was Sgt Farrell's generalized assumption that the, "most common types of cell phones used by the vast majority of the people in the United States are smart phones..." and that, "Based on my training and experience, I know the two most commonly used smart phone operating systems are iOS, which run on Apple iPhones, and Android..."[12]

After permitting police investigators to analyze any initial data return to identify suspects, the warrant enables the following:

> *"For those accounts identified as relevant to the ongoing investigation*

---

[10] Exhibit B: Warrant for LaQuan Dawes, page 11.

[11] A "reverse geolocation search" is distinguished from a "geolocation search" in that the latter seeks to reveal a specific individual's movements whereas the former begins with a location and then seeks to reveal which specific individuals were present there.

[12] Exhibit B, Warrant, pg 10.

through an analysis of provided records, and upon demand, Google shall provide additional location history ***outside of the predefined area*** *for those relevant accounts to determine path of travel."*

Such data could include up to forty-five minutes before or after the initial three time windows enumerated. Furthermore,

"For those accounts identified as relevant . . . Google shall provide the subscriber's information for those relevant accounts to include subscriber's name, email address, IMEI and phone numbers, services subscribed to, recovery SMS phone number and recovery email address."

For each of these additional steps, the warrant mandated no additional judicial oversight or threshold standards over what qualified as "relevant." Instead, the warrant permitted investigators acting only under their own discretion to access location and diverse personal account information for one or various digital device users.

From Google's data, compelled under the warrant and delivered on December 18, 2018, law enforcement targeted six different devices as being of interest to them. Under the terms of the warrant, Officer Lieu subsequently requested Google location data spanning forty-five additional minutes before and after the initial time windows for a specific device that he determined to be "relevant" to the investigation. Because there were no relevancy standards or reporting requirements contained within the warrant, the motivations of this request remain unknown. Google provided the requested location information to Lieu on January 7, 2019. Lieu then requested unmasking of the associated account, again without oversight. Google provided this on January 9, 2019. Investigators gained access to Laquan Dawes's name, two email addresses registered to him, a complete list of the Google-associated products he used, and the IP address from which he first agreed to Google's terms of use.

The information obtained from Google later formed the basis of a Ramey warrant for Dawes's arrest. The Honorable Linda Colfax authorized Dawes's Ramey warrant on January 28, 2019.

ARGUMENT

1. LaQuan Dawes had a Reasonable Expectation of Privacy in his Location Data and the Government's Acquisition of his Data was a Search

Fourth Amendment protections have long been understood to extend beyond property interests into the realm of privacy.[13] The U.S. Supreme Court's 2018 *Carpenter* ruling makes clear that an individual's expectation of privacy extends to his personal location data held by a third party.[14] So long as an expectation of privacy is objectively reasonable, state intrusion qualifies as a search governed by the Fourth Amendment's limitations.[15] A warrant to access cell-site location information must comply with all governing specificity and probable cause limitations.[16]

The location history data at issue here is even more precise with regard to an individual's specific coordinates than the cell-site location information (CSLI) discussed in *Carpenter.*[17] But both types of data give the government the ability to "travel back in time to retrace a person's whereabouts."[18] And they can do so with very little effort on their part. The traditional methods used for surveillance of individuals are logistically draining on law enforcement—they create de-facto limitations on the government's ability to conduct wide-scale and long term tracking of citizens and residents of the United States.[19]

---

[13] *Katz v. United States* (1967) 389 U.S. 347, 351.

[14] *Carpenter v. United States* (2018) 138 S.Ct. 2206, 2217.

[15] *Smith v. Maryland* (1979) 442 U.S. 735, 740.

[16] *Carpenter, supra,* 138 S.Ct. at p. 2209.

[17] Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy: How the Government is Collecting and Using Your Location Data* (2018) The Brennan Center for Justice at NYU School of Law, pp. 6-7 <https://www.brennancenter.org/sites/default/files/publications/2018_12_CellSurveillanceV3.pdf>.

[18] *Carpenter, supra,* 138 S. Ct. at p. 2218.

[19] *United States v. Jones, 565 U.S. 400, 406* (2012). As Justice Alito explained in Jones, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended

But recent advances in technology raise meaningful, decisive differences in individuals' privacy expectations as compared to traditional in-person surveillance.[20] This is because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations" and this information can be accessed by a single officer, sitting at a computer and reviewing data, without judicial oversight.[21] This potential for massively invasive searches on a large scale drove the Supreme Court to admonish lower courts to remain vigilant and "ensure that the 'progress of science' does not erode Fourth Amendment protections."[22]

LaQuan Dawes had a reasonable expectation to privacy in the location history data that was being safeguarded for him by Google. This location data was extraordinarily detailed and revealing, and San Francisco police executed a search when they demanded this information from Google. Accessing this information requires a warrant that establishes particularized and specific probable cause as to Mr. Dawes and his data.

2. The Geofence Warrant Used Here is an Unconstitutional General Warrant that Violates the Fourth Amendment Particularity Requirement and the Corresponding California Constitutional Provisions.

The United States Supreme Court has repeatedly made clear that particularity is required for any and every warrant.[23] General searches and so-

---

period of time was difficult and costly and therefore rarely undertaken." 565 U.S. at 429 (Alito, J., concurring in judgment).

[20] *Carpenter, supra,* 138 S.Ct. at p. 2216 (summarizing *United States v. Jones* (2012) 565 U.S. 400).

[21] *Jones, supra,* 565 U.S. at p. 415 (Sotomayor, J., concurring).

[22] *Carpenter, supra,* 138 S.Ct at 2223.

[23] See, e.g., *Kentucky v. King* (2011) 563 U.S. 452, 459 ("[A] warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity."); *Massachusetts v. Sheppard,* (1984) 468 U.S. 981, 988,

called "general warrants" are strictly prohibited.[24] Article 1, section 13 of the California Constitution parallels the relevant language of the Fourth Amendment. As a result, "the issue of particularity resolves itself identically under both federal and California standards."[25]

The purpose of the particularity requirement is to "ensure that a search or seizure 'will not take on the character of the wide-ranging exploratory searches [or seizures] the Framers intended to prohibit.'"[26] More specifically, a warrant's particularity must "impose[] a meaningful restriction upon the objects to be seized."[27] This prevents an individual law enforcement officer from exercising their personal discretion or satisfying their personal curiosity when executing a search – a neutral and fair Judge or Magistrate will have already set the reasonable and meaningful boundaries for the search based on particular information provided to them in an affidavit.

A. Geofence Warrants are Unconstitutional General Warrants

By its very nature, a geofence warrant is overbroad and lacks particularity. This is intentional. Geofence warrants seek out information for Google users merely due to their proximity to a crime scene—that is the only nexus. They sweep up the location data of an unlimited and unknowable number of people, all innocent, in the hopes that the data might show one potential lead to law enforcement. This is the "dragnet" law enforcement practice that the Supreme

---

n. 5 ("[A] warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional:").

[24] *Stanford v. State of Texas* (1965) 379 U.S. 480-84; *Marron v. United States* (1927) 275 U.S. 192, 195 ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

[25] *People v. Tockgo* (1983) 145 Cal.App.3d 635, 640, fn. 2.

[26] *People v. Robinson* (2010) 47 Cal. 4th 1104, 1132 (quoting *Maryland v. Garrison* (1987) 480 U.S. 79, 84) (brackets copied from quotation).

[27] *Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249.

Court has struck down and foretold against.[28] This prohibition of general warrants is historically rooted—in the times leading up to the American Revolution, a general warrant did not provide names of people to be arrested or specify homes to search. A general warrant stated "only an offense...and left to the discretion of the executing officials the decision as to which person should be arrested and which places should be searched."[29] To sweep up the location information of all Google users and then search through their data constitutes the "general, exploratory rummaging" lacking probable cause and a limited scope that our Framers and the Supreme Court requires.[30]

B. This Geofence Warrant Constituted an Unconstitutional Delegation of Discretion to the Executing Officers

It was not only the sweeping and generalized nature of general warrants that concerned the court—but it was the discretion that these warrants gave to individual officers that was feared. It allows for the abuse of power by individual officers, who, without oversight, can target large or small groups of people at their whim. This is not to say every officer will do this—but Fourth Amendment protections were critical in the eyes of our Founders because of the checks and deterrents it places on officers who might abuse their power. General warrants place "'the liberty of every [person] in the hands of every petty officer,'" and this is what must be vigilantly guarded against.[31]

The U.S. Supreme Court has recognized that physical and digital searches are fundamentally different from each other. Much of the case law and policy discussion related to search and seizure law deal with searches of physical

---

[28] *U.S. v. Knotts* (1983) 460 U.S. 276, 284.

[29] *Steagald v. United States* (1981) 451 U.S. 204, 220.

[30] *Coolidge v. New Hampshire* (1971) 403 U.S. 443, 467.

[31] *Stanford, supra,* at 379 U.S. at 481.

spaces or seizures of tangible, physical evidence. But the "search" of a digital device or inquiry for digital data propels this entire body of law into new terrain. The Supreme Court is cognizant of this trend, recognizing that to digital devices "place vast quantities of personal information literally in the hands of individuals."[32] A cell phone and the servers that store a phone's location and other data, "contains a broad array of private information never found in a home in any form."[33] This information is too invasive and private to be left in the hands of individuals officers, without judicial oversight.

The time to start implementing judicial oversight is now. Various news organizations have highlighted law enforcement's growing use of Google's Sensorvault database.[34] Sensorvault allows the reverse geolocation searches discussed here, and across all of Google's users' stored search history.[35] Although Google discloses the aggregate number of subpoenas, court orders, and warrants it receives from U.S. law enforcement (43,683 in 2018), it does not provide specific information on the number of reverse geolocation search warrants it fulfills.[36] However, in 2018, a Google employee stated that the

---

[32] *Riley v. California* (2014) 573 U.S. 373, 386.

[33] *Id.* at p. 397.

[34] E.g. Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police* (Apr. 13, 2019) New York Times <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html>; Mak, *Close Enough: Police departments are using "reverse location search warrants" to force Google to hand over data on anyone near a crime scene* (Feb. 19, 2019) Slate <https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html>; Brewster, *To Catch A Robber, The FBI Attempted An Unprecedented Grab For Google Location Data* (Aug. 15, 2018) Forbes <https://www.forbes.com/sites/thomasbrewster/2018/08/15/to-catch-a-robber-the-fbi-attempted-an-unprecendeted-grab-for-google-location-data>.

[35] Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works* (Apr. 13, 2019) <https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html>.

[36] Google, *Transparency Report: Request for User Information: US* <https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US> (as of Sept. 25, 2019).

company received up to 180 reverse geolocation search warrants in one week.[37] Brian McClendon, the lead developer of Google Maps and other location-based software for the corporation until 2015, has expressed concern in likening the new reverse searches to "a fishing expedition."[38]

A fishing expedition is exactly what was authorized in this warrant. First, this warrant is fundamentally based on Sgt Farrell's extremely broad and general statement that the, "most common types of cell phones used by the vast majority of the people in the United States are smart phones..." and that "[in general] suspects operate by using cell phones during the commission of a crime..." This is nowhere near to being specific or particularized. There is absolutely no information presented by Sgt Farrell to indicate that the suspects who burglarized the house were Google users. There is not evidence of them checking a cellphone or making a phone call—no evidence to indicate that they even owned or had cellphones in their possession. There is no indication that the suspects were messaging with each other on particular applications or through Google services. No evidence that a suspect had an Android phone instead of an iPhone. And there is no information or data backing up the Sergeant's general claims about smartphones or why suspects of crimes use phones in a unique way. Essentially, his affidavit merely makes two broad claims: people in the United States use smartphones and suspects are people. On that basis, he requests Google location history for every single individual in the vicinity of 1447 42nd Ave on October 24, 2018. This is the definition of a generalized, dragnet warrant.

Additionally, the warrant requested location information related to any and all Google accounts. No specific applications, such as Gmail, Google Maps, Play Store, etc. are requested—instead the warrant discusses "Android enabled

---

[37] Valentino-DeVries, *supra, Tracking Phones, Google Is a Dragnet for the Police.*

[38] Valentino-DeVries, *supra, Tracking Phones, Google Is a Dragnet for the Police.*

mobile devices." And beyond not specifying what basis the government had for believing some type of Google-associated technology might be involved, the warrant does not specify which Google account user it sought information about. It instead asks for every single device that passed through the search area at any moment between 2:45 p.m. and 3:15 p.m., 4:30 p.m. and 5:00 p.m., and 5:20 p.m. and 6:30 p.m. The court had no idea how many people could be affected by this warrant and how much data it was authorizing. And it never would find out—because everything after the initial signature was entirely left to the discretion of the involved police officers. Data from six devices was turned over to law enforcement. Some standard, completely opaque to anyone but the SF Police Officers involved with analyzing this data, was used to demand additional data from one device. This data was outside of the original location and timeframe specified in the affidavit. Officers then demanded that the personal information—username, email, phone number, etc.—for that device be produced. This process was impermissibly overbroad and lacking in particularity, and the warrant should be quashed under the Fourth Amendment. There were no additional showings of probable cause or judicial involvement. This is exactly the general warrant scenario that the Constitution prohibits.

Just as door-to-door sweeps of a neighborhood are overly broad under the Fourth Amendment's particularity standard,[39] so too is a search that queries the location history of all Google users. This warrant violated the Fourth Amendment's particularity requirements and it should be quashed.

[39] See, e.g., *Berger v. State of N.Y.* (1967) 87 S.Ct 1873 (invalidating electronic eavesdropping absent procedural safeguards due to the Fourth Amendment's protection against "general warrants").

2. Beyond the touchstone requirements of the Fourth Amendment and the California Constitution, this warrant fails the additional particularity requirements imposed by the California Electronic Communications Privacy Act (CalEPCA)

California state law affords elevated privacy protections for individual's data stored in electronic form. The 2016 California Electronic Communications Privacy Act (CalECPA) places a number of limitations on law enforcement's access to electronic data, including systematically stored location information.[40] Under the statute, "'Electronic device information' means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device."[41] This classification includes user information, emails, photos, videos, and other electronically stored information as well as both user-identified and anonymized location data.[42]

Unless the electronic device's possessor gives specific consent "directly to the government entity seeking information," a warrant is required for access to a device's electronic information, including related metadata and anonymized data.[43] CalECPA, in line with California Supreme Court rulings, does not recognize a third-party doctrine or any associated privacy limitations.[44]

CalEPCA makes distinct and unique demands for warrants that seek an individual's electronic data. This goes beyond the particularity requirement discussed in the prior section. CalEPCA provides four specific provisions that

---

[40] Penal Code section 1546 et seq.

[41] Penal Code section 1546, subdivision (g).

[42] *Id*; see Freiwald, *California's Electronic Communications Privacy Act (CalECPA): A Case Study in Legislative Regulation of Surveillance* in The Cambridge Handbook of Surveillance Law (Gray & Henderson edits., 2017), pp. 629–630 (clarifying the context and meaning of CalECPA's terminology).

[43] Penal Code section 1546, subdivisions (g) and (k); Penal Code section 1546.1.

[44] Penal Code section 1546; Freiwald, *supra*, at pp. 636–637, 640.

every warrant for electronic information must now include: (1) the time periods covered, (2) the target individuals and accounts—as appropriate and reasonable, (3) the "apps" or services covered by the warrant and (4) the types of information sought. [45] These limitations are put in place to prevent fishing expeditions by law enforcement when it comes to our electronic data. Worried about this possibility, the statute specifically enables a Judge or Magistrate signing a CalECPA warrant to appoint a special master to ensure that the authorized investigation is properly limited.[46]

CalECPA, in contrast to similar federal law, also includes a statutory suppression remedy.[47] "[A]ny person in a trial, hearing or proceeding may move to suppress any electronic information obtained in violation of the Fourth Amendment of the United States Constitution or [CalECPA]."[48] Alternatively, the California attorney general can bring a civil action to force a government entity to comply with CalECPA's requirements.[49]

The warrant at issue is governed by CalECPA. The location data requested from Google by Sergeant Farrell falls squarely within the "electronic data" contemplated by CalEPCA. The third provision of the contested warrant—allowing San Francisco police to unmask "accounts identified as relevant" without any additional judicial oversight—results in the government gaining access to additional electronic device information. This includes an individual's email addresses and product use data—clearly contemplated by CalEPCA.

Here, Dawes did not grant specific consent for government access to this or any other of his electronic device information. Absent this consent, CalECPA

---

[45] Penal Code section 1546.1, subdivision (d)(1).

[46] Penal Code section 1546.1, subdivision (e)(1).

[47] Freiwald, *supra,* at p. 634

[48] Penal Code section 1546.4, subdivision (a).

[49] Penal Code section 1546.4, subdivision (b).

requires a warrant that satisfies the four additional areas of particularity. The warrant authored by Sergeant Fell does not do this. Specifically, the warrant fails the second and third prongs of particularity laid out by CalEPCA.

A. Warrant fails to specify target individuals and accounts

The request here could hardly be more broad. The warrant does not specifically target individuals or accounts. Instead, it required Google to search every individual and account in its database to see which devices were using location data in the area in question during the requested times. There was no tailoring in terms of which accounts could be accessed. Instead, an indiscriminate and overbroad process of combing through up to millions of users' accounts was undertaken in hopes of identifying any individual that matched the location and time parameters. It was a fishing expedition.

After police investigators received the anonymized location data for the periods requested, they could, without any additional oversight, "identif[y] as relevant" and receive "...upon demand" any and all location data for devices up to forty-five minutes before and after the original time windows. This data would not be limited to the original geographic search area and could disclose locations from anywhere the device or devices travelled. Furthermore, "For those accounts identified as relevant . . . and upon demand of the investigative agents," the warrant mandated that Google provide the deanonymized personal information for users linked with the "relevant" devices—without any judicial oversight.

B. Warrant Fails to Identify the Apps or Services Covered

Sergeant Farrell asserts in his affidavit that he knows that, "when an Android device user first turns on a new Android device they are prompted to add a Google account" and that, "Based on my training and experience, I know it is impossible for an Android device user to install applications from the Google Play Store without a Google account." By his own admission, then, he is not requesting data from a particular application or service—but is asking for all data associated with an Android phone. Because it is his impression that

Android phones cannot and do not operate – i.e. no applications can be accessed without a Google account—he is necessarily asking for all of the data and information from every single application or service on the target mobile devices. This type of broad, sweeping search is precisely what CalEPCA was designed to prevent.

This warrant is what CalEPCA was meant to prevent. It is overbroad, lacks particularity, and fails to substantiate specific allegations of probable cause. The warrant must be quashed.

3. Broadly searching through Google account holders' personal data for a mobile device's passage through a specified geographic area amounts to an unconstitutional criminal checkpoint.

The United States Supreme Court has declared that general crime control checkpoints unconstitutional seizures.[50] The Court, "decline[d] to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes."[51] While the Court permits checkpoints with a specific purpose, such as to intercept undocumented immigrants,[52] check for drunk drivers,[53] and verify drivers' licenses and vehicle registration,[54] it bans general purpose checkpoints.[55] In *Edmond*, this ban included a narcotics checkpoint program.[56] If such general checkpoints were allowed, "there would be little check on the ability of the authorities to construct roadblocks for almost any conceivable law

---

[50] *City of Indianapolis v. Edmond* (2000) 531 U.S. 32, 40–44.

[51] *Id.* at p. 44.

[52] *United States v. Martinez-Fuerte* (1976) 428 U.S. 543.

[53] *Michigan Dept. of State Police v. Sitz* (1990) 496 U.S. 444.

[54] *Delaware v. Prouse* (1979) 440 U.S. 648.

[55] *Edmond, supra,* 531 U.S. at pp. 41–42.

[56] *Ibid.*

enforcement purpose."[57]

Edmond's reasoning is grounded in the principle that, "A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing."[58] The lack of individualized suspicion present in the reverse geolocation search warrant violates the Court's disallowance of "a checkpoint primarily for the ordinary enterprise of investigating crimes."[59]

Here, law enforcement's demand for this data is equivalent to police officers stopping each and every individual leaving the area of 1447 42nd Avenue and then demanding not only that these individuals hand over their cellphone to law enforcement—but also that they put in a passcode to unlock the phone and then allow police to extract data from that phone about where they had been that day. This type of stop, lacking any "individualized suspicion of wrongdoing," is precisely what *Edmond* prohibits.[60] "The general rule that a seizure must be accompanied by some measure of individualized suspicion" stands violated.[61]

San Francisco Police only knew that a residence had been broken into. In casting this wide net, the warrant allowed Google's Sensorvault program to produce data to the police for undefined future criminal investigation. Such data was not collected and stored for use in investigating this particular burglary; instead, law enforcement made use of data that they collected and

---

[57] *Id.* at p. 42.

[58] *Id.* at p. 37 (citing *Chandler v. Miller* (1997) 520 U.S. 305, 308).

[59] *Id.* at p. 44.

[60] *Edmond, supra,* 531 U.S. at p. 37. The reverse geolocation search warrants differ from tools that make use of user data available publicly online, such as social media geofencing, through which law enforcement collect public social media "posts" to identify or gather information on suspects. See Brennan Center for Justice at NYU School of Law, *Map: Social Media Monitoring by Police Departments, Cities, and Counties* (July 10, 2019) < https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties>.

[61] *Id.* at p. 41.

indefinitely preserved it for a general purpose. They did not collect information only for certain individuals. Instead, the warrant demanded that every registered Google's information be checked in order to determine who passed through the given location at the specified times.

As reverse geolocation search warrants do not fall within the "limited exceptions" to the general prohibition on general criminality checkpoints,[62] the resulting information, seized in violation of Dawes's Fourth Amendment rights, must be suppressed. To rule otherwise would violate the Constitution by permitting law enforcement to "simply stop cars as a matter of course to see if there just happens to be a felon leaving the jurisdiction."[63] That is the physical equivalent to the wide digital parameters laid out in this particular warrant and that is unconstitutional under all of the federal and state protections guaranteed by our legislatures and judiciary.

Conclusion

While modern technology facilitates the broad collection of data, such capabilities cannot be allowed to subject all individuals to law enforcement's digital scrutiny. Fourth Amendment protections demand that particularized suspicion be present when a warrant is used to uncover details of a crime. Here, no such individualized probable cause was present. Rather, all Google users were subjected to a combing through of their data in order to allow law enforcement to find a suspect for a case hitherto cold. To allow such investigations into users' systematically collected electronic data threatens to transform our society into one of constant police surveillance of digital devices.

Access to our digital data must be closely guarded and given to law enforcement in the most controlled and specified of situations. Here no

---

[62] *Ibid.*

[63] *Id.* at p. 44.

information beyond the occurrence of a crime at a certain location with four unnamed suspects was alleged. Nevertheless, a warrant to search the data of all Google users was permitted. Such a violation of Dawes and other users' reasonable expectation of privacy must be corrected.

Date: 6.1.20

Respectfully submitted

SIERRA VILLARAN
Deputy Public Defender
Attorney for LAQUAN DAWES