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

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

Attorneys for LaQuan Dawes

Superior Court of the State of California
County of San Francisco

People of the State of California,

Plaintiff,

vs.

LaQuan Dawes,

Defendant.

Court No: 19002022

Supplemental Reply to People's Opposition to Defendant's Motion to Quash and Suppress Evidence

Date: October 22, 2021
Time: 9:00 AM
Dept: 20

LaQuan Dawes, through counsel, submits this supplemental reply to the State's opposition to Mr. Dawes's motion to quash and suppress a "geofence" warrant issued on December 4, 2018. *See* People's Opp. to Def. Mot. to Quash & Suppress Evidence at 1 ("Opp."). Mr. Dawes filed an initial reply on September 13, 2021, focused on whether he had a reasonable expectation of privacy in his Google Location History data. *See* Reply to People's Opp. to Def. Mot. to Quash & Suppress Evidence at 1 ("Reply"). Following a hearing on October 4, 2021, this Court determined that that Mr. Dawes did in fact have an expectation of privacy in his Location History data under the 2016 California Electronic Communications Privacy Act (CalECPA). The Court held that Location History is protected location information under Penal Code sections

1546.1—specifically 1546.1(a)(1), (a)(2), and (g). This matter is now set for October 22, 2021, for the purpose of determining whether the warrant should be quashed because it was overbroad and/or lacking particularity, which would be a violation of CalECPA, the California Constitution, or the Fourth Amendment to the United States Constitution.

Introduction

Although the government obtained a warrant on December 4, 2018, *see* Mot. to Quash & Suppress Evidence, Exh. B [hereinafter "Geofence Warrant"], it did not obtain one for Mr. Dawes's Location History data. In fact, it did not seek anyone's data in particular. Rather, the government compelled Google to search *everyone's* Location History data in order to develop an investigative lead, using a multi-step process that gave impermissible discretion to investigators. As a result, this warrant was unlawful and unconstitutional. It was both overbroad and lacking in particularity, constituting a forbidden general warrant that authorized a dragnet search of Google users. It did not—and could not—satisfy either the statutory or constitutional requirement for probable cause and particularity, rendering it wholly impermissible and void from inception. Indeed, it was so deficient that no objectively reasonable officer could rely on it, and as a result, Mr. Dawes asks this Court to quash the warrant and suppress all evidence obtained from it, as well as all fruits of the poisonous tree—this includes all subsequent warrants and evidence related to LaQuan Dawes and his electronic information.

Argument

1. The Geofence Warrant can be Quashed under Both the Fourth Amendment and CalECPA.

Mr. Dawes challenges the validity of the Geofence Warrant under both CalECPA and the Fourth Amendment. Though the Court did not make a finding about reasonable expectation of privacy on Fourth Amendment grounds at the October 4, 2021, hearing, CalECPA demands that the Court "suppress evidence obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter." Pen. Code § 1546.4(a). This means that a violation of *either* the Fourth Amendment *or* CalECPA warrants suppression. *See* Pen. Code § 1546.4(a); Caskey, Cal. Search & Seizure (April 2018) 18 § 10:1.

2. Overbreadth: the Geofence Warrant Was Overbroad under the Fourth Amendment and CalECPA

Geofence warrants differ from other types of law enforcement requests, entailing a uniquely broad search of all Google users who have "Location History" enabled on their devices. Whereas typical requests compel Google to disclose information associated with a specific user, "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." Mot. to Quash & Suppress Evidence, Exhibit A at 11 ("Google Amicus"). Here, the warrant did not identify Mr. Dawes in any way. Nor did it identify any of the individuals whose personal information was searched and turned over to law enforcement. Instead, the warrant operated in reverse: it required Google to search all accounts with Location History enabled, a portion of which the government then seized.

Critically, the warrant was not just a search of people near 1447 42nd Avenue, but of all Google users with Location History enabled. And according to Google, "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)" have Location History enabled. Reply, Exhibit A at 4 ("McGriff-Decl."). To date, Google has not provided a more precise estimate for the number of such users in 2018, but Mr. Dawes estimates that it was close to 500 million.[1] As Google explains, a geofence warrant requires searching the contents of *every one of these accounts* because there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." Google Amicus at 12. Thus, to conduct a geofence search, Google must "search across all [Location History] journal entries to identify users with potentially responsive data, and then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." *Id.* at 12-13.[2]

[1] Google stated that it had over 1.5 billion active users on October 26, 2018, a third of which is 500 million. *See* @gmail, Twitter (Oct. 26, 2018, 9:02), https://twitter.com/gmail/status/1055806807174725633.

[2] This process differs from a so-called "tower dump," which seeks all the cell site location information (CSLI) for devices that connected to a given cell phone tower during a specified time. Unlike Google, cell phone companies organize, or "index" data based on location, *i.e.* the cell towers in their networks. They maintain this system for internal business purposes, such as identifying towers that become overloaded and identifying where to put up more. As a result, they can provide information about devices that connected to particular towers without searching the phone records of every customer. Consequently, a tower dump entails a search of far fewer people than does a geofence warrant (hundreds or thousands vs. "numerous tens of millions"). And importantly, the constitutionality of tower dumps is also in doubt following the Supreme Court's decision in *Carpenter v. United States. See* 138 S. Ct. 2206, 2220; *id.* at 2267 ("Why isn't a tower dump the *paradigmatic* example of 'too permeating police surveillance' and a

Consequently, 'step one' of the geofence warrant was an epic dragnet, conducted by Google at the government's direction. The government commandeered Google to search through "numerous tens of millions" of private accounts to determine if any of them contained data of interest. In fact, the warrant authorized three such searches—one for each of the three time periods given—meaning that "numerous tens of millions" of people were searched three times.

A. CalECPA relies on the Federal and State Definition and Use of Overbreadth to limit warrants for electronic information.

CalECPA requires that any warrant for electronic information "shall comply with all...provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants." Cal. Pen. Code § 1546.1(d)(3). While CalECPA *does* impose additional requirements above and beyond state and federal protections when it comes to particularity, which are discussed below, it adopts and incorporates the federal and Californian use and definition of overbreadth and probable cause.

B. This Geofence Warrant Lacked Probable Cause and was Inherently Overbroad

Overbreadth concerns probable cause, which is defined as "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates* (1983) 462 U.S. 213, 238. A warrant is overbroad if the government lacks probable cause for the things to be searched or seized. *Burrows v. Superior Ct.* (1974) 13 Cal. 3d 238, 250 (en banc) ("It is axiomatic that a warrant may not authorize a search broader than the facts supporting its issuance."). It is also the case that "broad generalizations do not alone establish probable cause." *People v. Pressey* (2002) 102 Cal.App.4th. 1178, 1190. Here, the government did not have probable cause to search millions of Google users' accounts. Nor did it have probable cause to search six users' accounts. Def. Mot. to Quash at 8. The government lacked probable cause to search even one Google account, because investigators admittedly had no suspects. This complete absence of probable cause means the warrant was a massive fishing expedition; fatally overbroad from the beginning.

Indeed, it is difficult to imagine that any amount of probable cause could justify a search of millions. But in this case, the government had none. The warrant application provided no case-specific facts that the burglar had a cell phone, was a Google user, or had Location History enabled at the times in question. The State now claims that one suspect is visible on NEST

dangerous tool of 'arbitrary' authority—the touchstones of the majority's modified Katz analysis?") (Gorsuch, J., dissenting).

footage using a cell phone, Opp. at 9, but the warrant application makes *no* mention of this—and the court can only consider the face of the warrant and supporting affidavit when considering a motion to quash. *Groh v. Ramirez* (2004) 540 U.S. 551, 551. All the State offered was that people, including criminals, use cell phones to communicate; that the "vast majority" of U.S. cell phone users have smartphones; and that "the two most commonly used smart phone operating systems are iOS . . . and Android." Mot. to Quash & Suppress Evidence, Exhibit B at 10 ("Warrant & Affidavit").[3] The government contends that this is sufficient to establish probable cause, Opp. at 9, but if that is true, then the government could get a geofence warrant in any investigation, simply by reciting the facts of the crime and some statistics about Google.

Such broad conjecture about the popularity of Google or cell phones does not amount to probable cause. Rather, probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois* (1979) 444 U.S. 85, 91. In Illinois, Judge Fuentes denied a geofence application on precisely these grounds. *See In re Information Stored at Premises Controlled by Google* (N.D. Ill. 2020) 481 F. Supp. 3d 730, 754. As here, the State's position "resembles an argument that probable cause exists because those users were found in the place ... [where] the offense happened," an argument the Supreme Court rejected in *Ybarra*. *Id.*

The California Supreme Court has also applied the overbreadth rule to invalidate a warrant that uses "boilerplate" clauses and conclusory statements, because this language permitted an exploratory and overbroad search through all of someone's the papers and effects. *People v. Frank* (1985) 38 Cal.3d 711, 727; Cal. Const. Art. I § 13. In finding overbreadth, the court said, "On this record, accordingly, we must conclude that the finding of probable cause to search for the challenged notebooks was based not on facts but on mere speculation—or worse, on boilerplate allegations routinely incorporated into the affidavit…". *Franks, supra,* 38 Cal.3d at 729. This overbroad warrant also made it "necessary for the police to rummage through all defendant's personal papers and read enough of each to learn its contents—as the criminalist on

[3] While approximately 85% of Americans have a smartphone, only 40.5% of those are Android phones, which require a Google account to operate. And according to Google, only one third of Google accounts have Location History enabled. Mathematically, that means there is just a 11% chance that an unknown individual in this country owns a smartphone with Location History enabled (85% x 40.5% x 33% = 11%), a far cry from a "fair probability" in any event. *See* Pew Research Center, *Mobile Fact Sheet* (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/; Jack Wallen, *Why is Android more popular globally, while iOS rules the US?*, TechRepublic (May 12, 2021), https://www.techrepublic.com/article/why-is-android-more-popular-globally-while-ios-rules-the-us/; McGriff Decl. at 4.

the scene apparently did with respect to the three notebooks in issue." *Id.* at 726. This is directly analogous to the overbroad and unconstitutional search here—the Geofence Warrant used "boilerplate" and conclusory language about smartphone use and humanity to order Google to "rummage through" all of the numerous tens of millions of Google users who had Location History enabled. At least in *Frank,* there was an actual single suspect identified; but even still, a warrant based on "boilerplate allegations" that permitted and required the Government to go through every document and effect in Frank's home to see if it contained incriminating information was overbroad and without probable cause. Going through all of the Location History data of every single user based on conclusions about cellphone use is beyond overbroad.

Moreover, if the State had established a nexus between the burglar and Location History, then there would have been no need to fish in Google's ocean of data. The State could have simply requested the Location History data for the suspect's account, as it typically does. But the government did not seek to search a particular account; it sought to search *all* accounts with Location History enabled, the definition of a modern-day general warrant. *See Warden v. Hayden* (1967) 387 U.S. 294, 313 (Douglas, J., dissenting).

The fact that Google conducted the dragnet for them does not absolve the State of its role in compelling it. The Fourth Amendment does not distinguish between Google and the government when a warrant demands such compliance, and as a result, both the search and the seizure are squarely state action. This case does not involve a "private search." Google did not decide on its own to search for users near the burglarized residence, and Google never provides such information to advertisers. *See* Reply, Exhibit D at 197 (regardless of the type of advertising, Google "never share[s] anyone's location history with a third party."). Likewise, the data seized and sent to law enforcement was not an existing "business record." Google did not possess a list of people near 1447 42nd Avenue until the State required them to create one. In short, Google had no independent motivation to conduct this geofence search, and Google would not have done so without a warrant. The entirety of step one was conducted at the State's direction, without probable cause to search even one account.

Finally, while the State ultimately *seized* the data belonging to six people in step one, the State first had to *search* "numerous tens of millions" to identify it. The Government's argument that only "six people" were identified and therefore this was not an overbroad search is misleading. It is the breadth of the initial search, not the breadth of the ultimate fruits, which the Court must analyze.

Probable cause was still absent in steps two and three, when the government seized even more Location History data from Mr. Dawes' account and required Google to disclose his subscriber information. Step two of the warrant authorized the State to seize an additional 45 minutes of Location History data for any "accounts identified as relevant to the ongoing investigation." Warrant & Affidavit at 4. And step three required Google to provide the subscriber information for those accounts.

In sum, the government lacked probable cause to search anyone's Location History, whether one, six, or "numerous tens of millions" of people. There was no cause to justify the digital dragnet in step one, no cause to justify the additional searches in steps two and three. The warrant was therefore overbroad from start to finish and violated the Fourth Amendment which necessarily also triggers a violation under CalECPA.

4. The Geofence Warrant Lacked Particularity under both the Fourth Amendment and CalECPA—which has a heightened standard for this requirement.

A. The Warrant Lacked Particularity under the Fourth Amendment

The geofence warrant was not only overbroad by design, but also profoundly lacking in particularity. *See* U.S. Const. amend. IV (requiring that warrants "particularly describ[e]" the place to be searched and the things to be seized); Cal. Const. Art. I § 13. Particularity concerns officer discretion, and the object is to leave nothing to the discretion of the officers executing a warrant that a court has properly authorized. *See Marron v. United States* (1927) 275 U.S. 192, 196. Warrants must particularly describe both the place to be searched and the items to be seized in order to limit officer discretion and prevent the "exploratory rummaging" that the Framers abhorred. *Coolidge v. New Hampshire* (1971) 403 U.S. 443, 467; *see also Frank*, 38 Cal. 3d at 724 ("In short, 'Nothing should be left to the discretion of the officer.'"). If properly particularized, it should be obvious to anyone what can or cannot be searched and seized.

Here, the geofence warrant left it up to Google and the government to negotiate which users would have their account information searched and further revealed to investigators—the hallmark of an unparticularized warrant. *See Steagald v. United States* (1981) 451 U.S. 204, 220; *Stanford v. Texas* (1965) 379 U.S. 476, 482-83 (describing the "battle for individual liberty and privacy" as finally won when British courts stopped the "roving commissions" given authority "to search where they pleased"). The items to be searched and seized were not specified, but instead described as the product of a three-step process that explicitly requires the government to use its discretion. Each step left basic, critical questions up to Google and the State, not a judge.

i. "Step One"

Step one failed to identify the data to be searched, failed to provide clear instructions on what could be seized, and ensnared people far outside the geofence as drawn in the application.

First, the warrant did not specify the type of location data to be searched, stating instead that Google was to search "[a]ll location data." Geofence Warrant, Appendix B, at 4. The warrant application implied that Google would have such data for all Google users, but as Google explains: only a third of all accounts have Location History enabled. In fact, Google does maintain two other types of user location data, "Web & App Activity" data and "Google Location Accuracy" data (formerly known as "Google Location Services"). McGriff Decl. at 5-7. But according to Google, Location History is the only form of location data that is "sufficiently granular" and searchable to be responsive to a geofence request. *Id.* at 7.[4] The State failed to disclose this information to the court, making it appear more likely that Google could provide responsive data, and ignoring facts to the contrary. To be clear, Mr. Dawes is not suggesting that Google should have searched its other two databases. Rather, the problem is that Google and the government decided what to search, not a judge. *See Groh,* 540 U.S. at 561 ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'").

Second, the warrant did not adequately specify which data could be seized during the dragnets in step one. The warrant directs Google to produce "[a]ll location data ... at the

[4] The State was or should have been aware of this fact because the basic contours of a geofence warrant were the product of repeated discussions between Google and the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice in 2018. *See* Hr'g Tr. at 456-57, Mar. 4-5, 2021, *United States v. Chatrie*, No. 3:19-cr-00130 (Def. Exhibit B) ("CCIPS is an agency that ... our counsel engages with to discuss sort of certain procedures that may be relevant for the way that ... Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request"); *id.* at 476 (noting repeated "engagement" between CCIPS and Google "help[ed] to socialize the concept of these types of warrants"); *id* at 552-53 (discussing the relationship with CCIPS). Indeed, following their mutual understanding, the Justice Department provided "go-by" language to state and local law enforcement agencies for use in plug-and-play geofence warrant applications. *Id.* at 552-553 ("[W]e follow the steps that [CCIPS and Google] have laid out in order to ... make sure that Google understands what we are requesting and that we understand what we'll receive back").

locations specified," Geofence Warrant, Appendix B at 4. But "at the locations specified" is actually much more complicated and open to interpretation and officer discretion than the warrant makes it appear. Determining who is "at the location" involves a series of choices made by law enforcement, without judicial oversight and approval, which will be further discussed below. The State was aware of this fact and left the warrant silent on this issue, leaving it up to Google and the government to work out among themselves, without input from a judge.

Before discussing how "at the locations specified" is determined, some background information is important. As any Google Maps user is likely aware, when you look at the Maps application, there is a small, solid "blue dot" that indicates your location, and it is often accompanied by a larger, "light blue circle" around the blue dot. *See* Google, *Find and Improve your Location's Accuracy* (last visited Apr. 26, 2021) ("The blue dot shows you where you are on the map. When Google Maps isn't sure about your location, you'll see a light blue circle around the blue dot. You might be anywhere within the light blue circle.").[5]

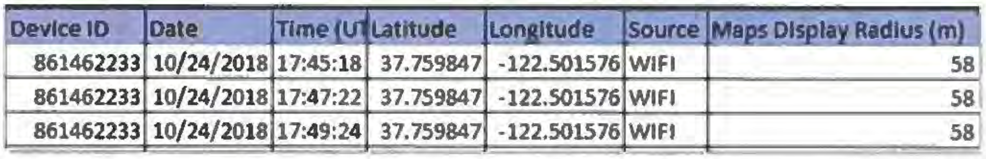
The small, solid blue dot is actually often not exactly where you are—this is because it is merely Google's *estimation* of your device's location based on different inputs, including CSLI and nearby WiFi networks. *See* Google Amicus at 10 n.7. Because this is an estimation, Google provides the larger, light blue circle as a sort of visual representation of the margin of error in its calculation about your location. Basically, Google is equally confident that a device could actually be anywhere within the larger, light blue circle, even off to the edge of the circle; the blue dot is simply placed at the center point of that circle. This leads to the "common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake." *In re Search Warrant Application for Geofence Location Data Stored at Google*, No. 20 M 525, 2020 WL 6343084 at *9 (N.D. Ill. Oct. 29, 2020).

When it comes Location History data, Google records the "blue dot" as a set of coordinates – latitude and longitude, even though GPS may not have been used. Google calls the "light blue circle" the "Map Display Radius" and records it in meters. The State was aware of all this as well, which is why the warrant explicitly asks for the "estimated radius" in addition to the coordinates. Geofence Warrant, Appendix B, at 4; Figures 1 and 2 in the expert report prepared

[5] *Available at* https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3D Android&hl=en.

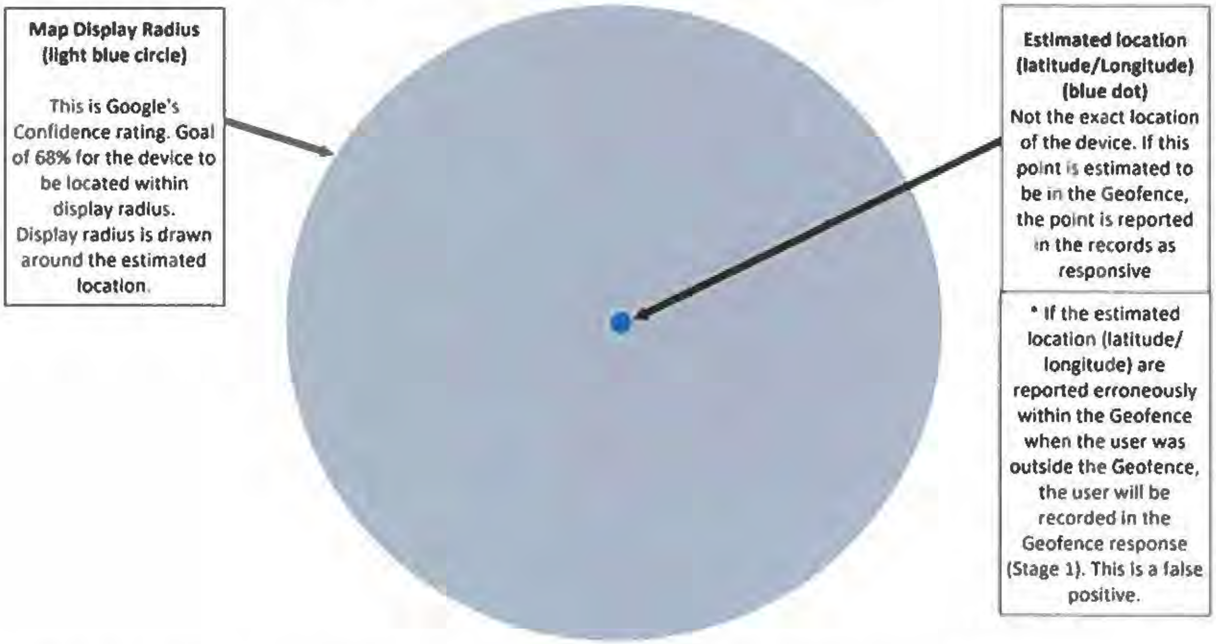
by Spencer McInvaille, attached hereto as Exhibit A, visualize this principle. *See* Report of Spencer McInvaille Report (Oct. 18, 2021) (Def. Exh. A).

Figure 1. Example of Data in Google Stage 1 Response



Device ID	Date	Time (UT	Latitude	Longitude	Source	Maps Display Radius (m)
861462233	10/24/2018	17:45:18	37.759847	-122.501576	WIFI	58
861462233	10/24/2018	17:47:22	37.759847	-122.501576	WIFI	58
861462233	10/24/2018	17:49:24	37.759847	-122.501576	WIFI	58

Figure 2. How the data is mapped (Display radius vs. Estimated Latitude and Longitude)



Map Display Radius (light blue circle)

This is Google's Confidence rating. Goal of 68% for the device to be located within display radius. Display radius is drawn around the estimated location.

Estimated location (latitude/Longitude) (blue dot)

Not the exact location of the device. If this point is estimated to be in the Geofence, the point is reported in the records as responsive

* If the estimated location (latitude/ longitude) are reported erroneously within the Geofence when the user was outside the Geofence, the user will be recorded in the Geofence response (Stage 1). This is a false positive.

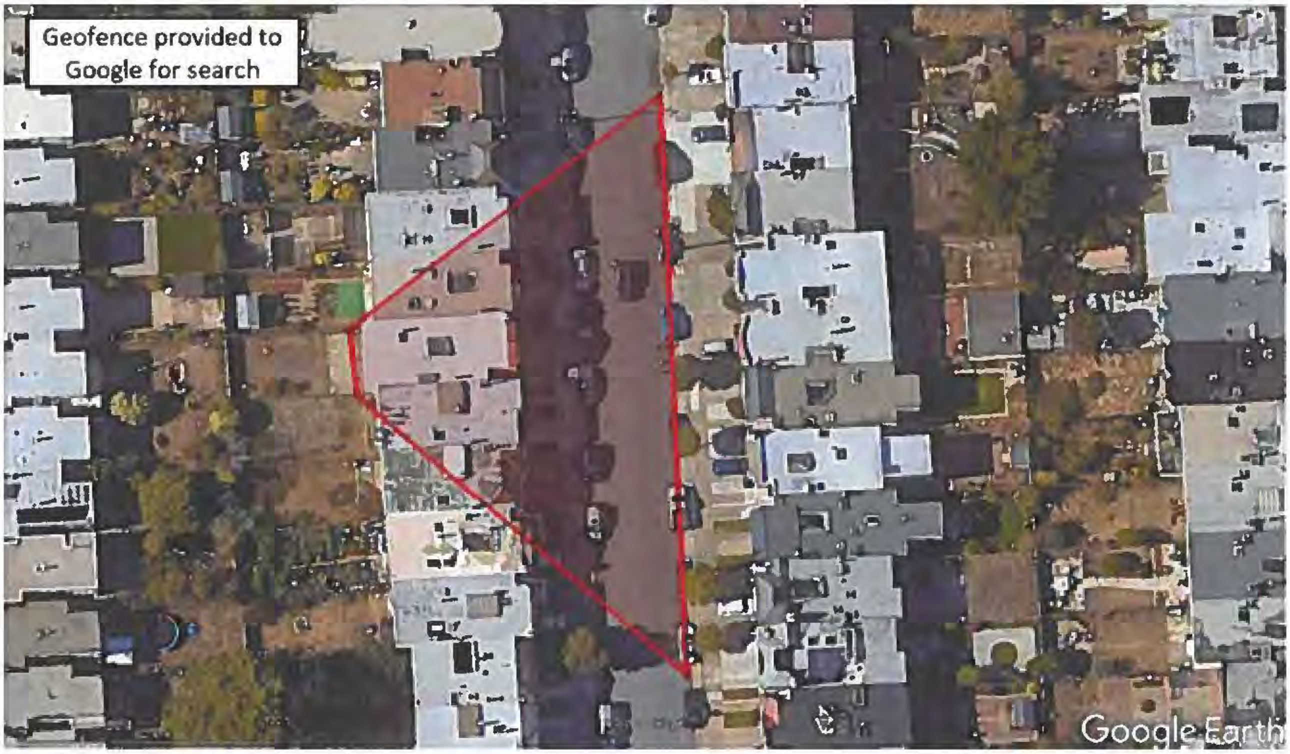
Important to note: Google is only 68% sure that the device is actually located in the larger, light blue circle. There is a 32% chance that the device is actually outside of this circle.

This background is significant because it means there are multiple ways to count which devices are "at the locations specified." The first, most conservative option is to count only those devices whose entire Map Display Radius, or whose entire larger, light blue circle, is inside the geofence. At times, Location History data can have a Display Radius of just a meter or two, so seizing data only for the devices with radii fully encompassed by the geofence would greatly reduce the likelihood of "false positives," something Google acknowledges are possible. *See* Google Amicus at 20 n.12. The second option is to count the devices whose smaller, solid blue dots (coordinates) fall within the geofence. This increases the likelihood of false positives because someone may actually, in reality, be outside the geofence, somewhere in their light blue circle, even if their blue dot falls within geofence area. *Id.* The third option is to count every device whose Display Radius (larger, light blue circle) intercepts the geofence location. This method seeks to ensure that law enforcement does not miss any suspects, but it drastically increases the chances of a false positives.

It is not clear what method the State used here because the warrant does not specify one way or another. Instead, once again, the warrant left that decision up to Google and the government, not a judge. It appears that the State likely selected option two. But as with the decision to search Location History, the question is not whether this was the 'correct' course of action. The question is who should be making these decisions, and the Fourth Amendment demands that a judge fulfill that role. *See Groh*, 540 U.S. at 561.

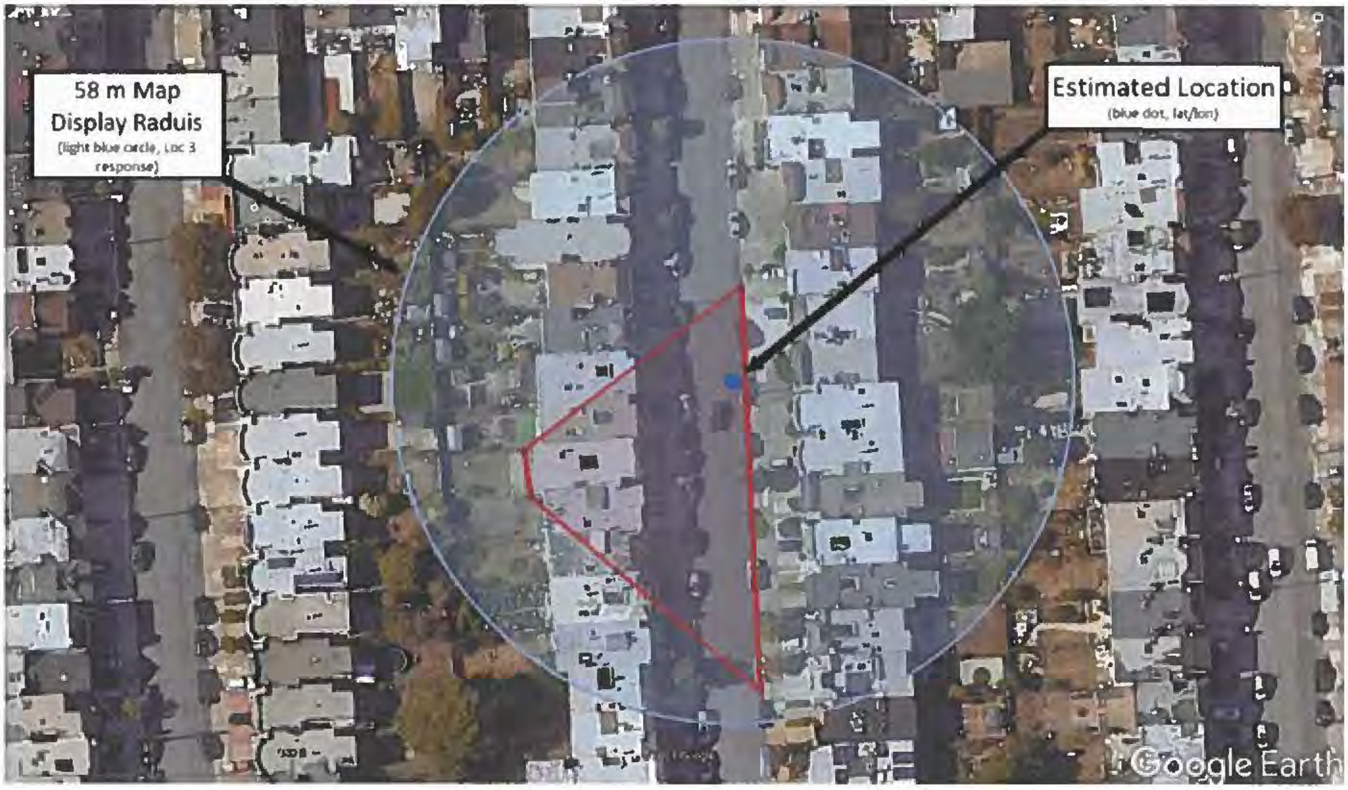
Third and finally, the Map Display Radius actually increases the range of the geofence to an uncertain degree, dependent on the (undisclosed) method of counting, and therefore ensnares people outside the stated boundaries of the geofence. If, as appears to be the situation here, the State chose option two and counted the "blue dots," then the effective range of the geofence would have extended far beyond the trapezoid drawn in the warrant application. In fact, this is precisely what the data shows. Figure 3 in Mr. McInvaille's report illustrates the geofence as

Figure 3. This is the Geofence chosen by Law Enforcement to be searched by Google.



outlined in the warrant. McInvaille 10/18/21 Report (Def. Exh. A). Figure 4 depicts the effective range of the geofence, a product of the State's chosen counting method.

Figure 4. Depicts one of the responsive points from "Location 3".



As is apparent in the above Figure 4, there are very real and measurable consequences to the choices the State made about what to search and seize—*i.e.*, how to count and the true geographic scope of the geofence. The State now contends that the warrant was "limited because it specified a limited scope of Google information directly tied to a specific burglary and a particular place and time." Opp. at 10-11. **But in reality, as evidenced by the larger, light blue circle in Figure 4, the officer discretion allowed by the warrant led to the seizure of data from an effective area that was approximately seven times the area covered by the trapezoid depicted in the original warrant**. McInvaille 10/18/21 Report (Def. Exh. A). The largest Map Display Radius reported was 58 meters, thus extending the effective range of the geofence to an approximate area of 10,523 square meters. *Id.* This area is seven times larger than the "1,800 square yards" (1,505 square meters) that the State now acknowledges. Opp. at 4 n2.[6]

[6] Defense expert Spencer McInvaille calculated the area of the trapezoid as 1,425 meters, making the effective area 7.38 times larger than then proposed geofence (10,523 / 1,425 = 7.38). *See*

And in practice, this meant that the data seized extended to 30 homes and 16 other fenced areas behind homes, compared to the 6 homes, street, and sidewalk encompassed by the trapezoid. McInvaille 10/18/21 Report (Def. Exh. A).

No judge signed off on the seizure of data for devices outside of the geofence—much less an area seven times larger than what was originally described—but that is precisely what the State achieved by having the discretion to select its preferred method of counting. GPS coordinates may appear specific, but they are inadequate for particularity purposes without accounting for the Map Display Radius and the effective range of the geofence. The warrant as written allowed the State to impermissibly expand the geographic boundaries of the geofence at its discretion.

ii. 'Step Two' and 'Step Three'

Steps two and three of the warrant *explicitly* gave the State discretion to determine which Google users will be subject to further scrutiny. Step two said: "For those accounts identified as relevant to the ongoing investigation 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." Warrant & Affidavit at 4. This means that the State was responsible for identifying what was "relevant" and what else to seize. Here, the State identified Mr. Dawes' data as "relevant," and without returning to the court for additional authorization, commanded Google to provide an additional 45 minutes of his Location History data.

Then again in 'step three,' the State had the opportunity to identify "relevant" accounts, for which Google was required to provide subscriber information, including the account holder's name, email address, and phone number. The warrant stated: "For those accounts identified as relevant to the ongoing investigation … Google shall provide the subscriber's information[.]" *Id.* at 4. Once again, the warrant left it up to law enforcement, not a judge, to determine whose data to seize. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); *In re Information Stored at Premises Controlled by Google* (N.D. Ill.

McInvaille 10/18/21 Report (Def. Exh. A). But even using the State's figure of "1,800 square yards" (1,505 square meters), the ratio is similar (10,523 / 1,505 = 6.99).

July 8, 2020) No. 20 M 297, 2020 WL 5491763, at *6 ("[T]his multi-step process simply fails to curtail or define the agents' discretion in any meaningful way.").

The government contends the instant geofence warrant was sufficiently particular by analogizing it to two other search warrants that contained mere inaccuracies: One warrant inaccurately described the home to be searched as a "two-story building . . . but the building was actually a one-story building" at a different address; the other warrant listed a mobile home street address when the actual place to be searched was a 40-acre parcel and barn almost one-half mile from the mobile home. *See* Opp. at 10. But here, the government did not simply make a mistake. It did not get the address wrong. Rather, it explicitly designed and gave itself the power to make executive decisions without judicial oversight, which led to the Government impermissibly searching "numerous tens of millions" of people and seizing data covering 30 addresses.

By explicitly empowering the government to determine which private data to seize, the geofence warrant violated constitutional requirements for particularity. *See* Def. Mot. to Quash at 8 ("[T]he 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."). At each step, the warrant allowed Google and the government to be the arbiters of what was reasonable to search and seize. No objective observer could look at the warrant and ascertain which accounts the government had authority to search or seize. The warrant therefore lacked particularity and violated the Fourth Amendment.

B. The Warrant Violated CalECPA and its Heightened Standards of Particularity

All of the above discussion about how the Geofence Warrant violates particularity should also be considered grounds for suppression under CalECPA, as both Fourth Amendment violations and statutory violations require suppression. Pen. Code §1546.4(a). But CalECPA actually provides a heightened protection for Californians when it comes to "particularity." Pen. Code §1546.1(d)(1). Particularity has a very specific and defined meaning within the context of the statute, requiring that the warrant contain four discreet types of limitations: (1) the time periods covered by the warrant; (2) the target individuals or accounts; (3) the applications or services covered; *and* (4) and the types of information sought." *Id.* Where two or more requirements are provided in a section and the conjunctive "and" is used, all requirements must be fulfilled to comply with the statute. *See Tyson v. Burton* (1930) 110 Cal.App. 428. All four of these conditions must be met for CalECPA's particularity requirements to be satisfied.

i. The warrant did not specify target individuals or accounts.

As has been emphasized multiple times, the warrant in this case never identifies a target individual or specific user account. There was no name, cell phone number, email address, or account information included in the warrant. The Government argues that this requirement is a "mechanism for seeking information when an individual's identity is unknown." State Opp. at 12. But common sense dictates that it is the exact opposite – it requires that the Government actually know which individuals or which specific accounts are to be searched before it applies for a warrant. It is an acknowledgment that there might be multiple people who use, for example, a shared office or family network. Each individual has a protected privacy interest in the electronic information on that shared network. The Government cannot just search the entire network of files, for example the entire San Francisco Superior Court network, and the data of all shared users. It must identify a specific account or individual whose information is being sought and search only that data.

The same is absolutely true here. Everyone who had "location information" described in Appendix B of the warrant had a privacy interest in that data. CalECPA's particularity requirement prohibits the Government from compelling a search of all location information for all people who use it or have it—they are explicitly required to specify the individual or accounts *before* applying for the warrant. The interpretation that the Government is putting forth, that this requirement is a mechanism for ferreting out a suspect when there are none identified, would completely void the meaning of particularity in this sense. It would literally mean the Government would *never* again need to identify a suspect for a crime, but instead could, every time a crime was alleged, ask Google to use the Sensorvault to produce a list of devices that were in the area at a given time. This regression cannot be what CalECPA, a statute designed to "both codify and expand on existing" protections for electronic information, was meant to permit. Assembly Committee on Privacy and Consumer Protection Report at 5 (Jun. 23, 2015). This is especially true considering that CalECPA's drafters and proponents had a special concern for the protection of location information. *See, e.g.*, Assembly Floor Analysis at 5 (Sep. 4, 2015); Susan Friewald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act*

(CalECPA), 33 Berk. Tech. Law J. 131 at 140 (2018) ("location data [was] an area of great concern to CalECPA's proponents").

ii. The warrant does not specific the applications or services covered.

The warrant here commands Google to provide all "location information" that Google has for all responsive users or mobile devices. While this may appear to be a limitation on service, the State knows that it was not. The Government contends that the warrant was particularized in apps and services because it sought "any and all information related to services provided by Google." State Opp. at 12. But searching all applications and services provided by Google, on a Google account-enabled phone, is not a meaningful limitation. Moreover, as discussed above, "all location information" is an extremely broad and sweeping category that, just for Google, involves at least three, giant subsets of information: "Location History," "Web & App Activity" data, and "Google Location Accuracy" data (formerly known as "Google Location Services"). McGriff Decl. at 5-7. The warrant fails to specify which type of data the State planned to search, and omits the fact that most Google users do not have Location History enabled. Had the State specified the service, it would have been obvious that there were no facts indicating that the suspect used Location History.

5. This Search was Comparable to an Unconstitutional Criminal Checkpoint

The Government wholly fails to address Dawes's argument that this reverse geolocation search was comparable to an unconstitutional and general crime control checkpoint. 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." *City of Indianapolis v. Edmond* (2000) 531 U.S. 32, 40–44. A reverse geolocation search is the equivalent of the government seizing every device that was entering, present, or leaving the geofence or Map Radius area of 1447 42nd Avenue without any individualized suspicion of wrongdoing by the owner of the device.

6. The Good Faith Exception Does Not Apply

A. There is No Good Faith Exception to CalECPA

The good faith exception does not apply to CalECPA. *See e.g. People v. Jackson* (2005) 129 Cal.App.4th 129, 153-160; Caskey, *California Search and Seizure* (2021) § 10:20. This is because *Leon* and good faith "is a judicially crafted exception to an exclusionary rule that is a judicial creation"—and it cannot be applied to a "statutory mandate." *Id.* at 153. Statutory suppression requirements, such as the one found in CalECPA, do "'not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of [the statute]" *Id. (*citing *United States v. Giordano* (1974) 416 U.S. 505, 514). And "[i]f suppression of...evidence 'does not turn on the judicially fashioned exclusionary rule'... we fail to see how it can turn on a judicially fashioned exception to the judicially fashioned exclusionary rule." *Id.*

As the *Jackson* court further points out, the argument for application of good faith to a statute like CalECPA breaks down when you consider how it would work in practice. *Id.* at 155. A violation of either a Constitutional provision or of the statute requires suppression under CalECPA. Pen. Code § 1546.4(a). A hypothetical warrant that violated only a statutory provision of CalECPA, but that did not violate the Constitution, would then require suppression under the statute. But a warrant that violated *both* a Constitutional provision and CalECPA would not require suppression if the officer executing the warrant had an objective good faith belief in its validity. The result would be that "nonconstitutional violations of the [...] statute would be more likely to lead to the suppression of evidence than constitutional violations. We do not believe this is what Congress or the California Legislature intended." *Jackson,* 129 Cal.App.4th at 155.

By enacting CalECPA, passing it by more than two-thirds majority (therefore superseding Prop 8's "Truth in Evidence" rule), and by including an explicit remedy of suppression, the California Legislature clearly indicated that suppression is necessary to protect the privacy of Californians. This statute was passed in 2016, over thirty years after the creation of the good faith doctrine. If the legislature wanted to incorporate this an exception, it would have.

B. The Good Faith Exception Also Does Not Apply under the Fourth Amendment.

The good faith exception is also inapplicable under the Fourth Amendment. The Supreme Court recognized the exception in *United States v. Leon*, 468 U.S. 897, 919 (1984), but the Court also outlined four circumstances where it does not apply: (1) if a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) if the judge acted merely as a rubber stamp for the police, *id.* (citing *Gates*, 462 U.S. at 239); (3) if the affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4), if no officer could reasonably presume the warrant was valid, *id.* at 923. The exception was not intended to diminish the power and force of the Fourth Amendment. *Id.* at 924. Rather, it tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id.* at 917, 923.

The third and fourth *Leon* exceptions apply here. With respect to the third prong: The affidavit did not only lack a substantial basis to determine probable cause. It lacked any basis at all. The warrant was "so lacking in indicia of probable cause" to search and seize Mr. Dawes's Location History data that it was entirely unreasonable for any trained officer—i.e., one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements—to rely on it. *See Leon*, 468 U.S. at 923. Contrary to established practice, the warrant did not specify any Google account(s) to search or seize. Instead, it sought to search *everyone* first, and then identify suspects later—leaving the judiciary out of critical decisions that go to heart of Fourth Amendment reasonableness.

Any reasonable jurist would have denied the warrant application had they known that the warrant authorized Google to search the private daily journals of tens of millions of people, or seizure of Location History data for anyone in a 30-house radius of the crime. And any reasonable officer would have known that such a warrant is invalid. *See United States v. Grant* (9th Cir. 2012) 682 F.3d 827, 836, 841 (holding the good faith exception did not apply because "[t]he affidavit simply d[id] not set out any plausible connection between [the defendant's] home and the gun or ammunition used in the homicide. … [N]one of the facts in the affidavit, singly or en masse, provide a reasonable basis from which to infer that the gun was in [the defendant's] home"); *see also United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013) ("A reasonable police officer would be unable to infer through normal inferences that electronic devices owned by child abusers in general or the Defendant specifically contain evidence related to the criminal activity being investigated … .").

Just as it is impermissible to search every house in the neighborhood for evidence of a local theft, any reasonable officer would have known that doing the digital equivalent is also unconstitutional. Such warrants are general warrants, and they are *void ab initio*—void from the start—and they are no warrants at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."); *United States v. Crozier* (9th Cir. 1985) 777 F.2d 1376, 1381 (holding the good faith exception did not apply to a search warrant that was "deficient because it [wa]s overbroad and d[id] not describe any particular property," meaning a law enforcement "agent could not reasonably rely on the warrant").

The State contends that good faith should apply because suppression "would not avoid future investigative error." Opp. at 13 (all caps dropped). But obtaining a warrant akin to fishing license, based on pure conjecture, is not "objectively reasonable law enforcement activity" and must be deterred. *See Leon*, 468 U.S. at 919. Suppression would provide an effective deterrent against similar unconstitutional attempts in the future. Moreover, a strong message is necessary given the thousands of geofence warrants Google is now receiving each year. *See* Zach Whittaker, *Google says geofence warrants make up one-quarter of all US demands*, TechCrunch (Aug. 19, 2021), https://techcrunch.com/2021/08/19/google-geofence-warrants/. This is one of the first cases in California involving a geofence warrant, but if this Court does not deter the State now through suppression, the creep of surveillance will only continue to slip on. *See, e.g.*, Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched A Sexual Assault Victim's Name, Address And Telephone Number*, Forbes (Oct. 4, 2021).[7] The number of geofence warrants following this one does not diminish the strength of Mr. Dawes' challenge. On the contrary, it ripens it, calling out for judicial intervention, now.

For these reasons, no officer could reasonably presume the geofence warrant here was valid. *See Leon*, 468 U.S. at 923. It was "facially deficient" under *Leon*'s fourth prong, as well as the third. *Id.* Indeed, "it is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also Crozier*, 777 F.2d at 1381; *United States v. Leary*, 846 F.2d 592, 607-09 (10th Cir. 1988) (stating "a reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases from the First, Eighth, and Ninth Circuits). Consequently, this Court should find that the good faith exception does not apply to a general warrant like the geofence warrant at issue here.

[7] *Available at* https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/.

Conclusion

For the foregoing reasons, Mr. Dawes submits that the geofence warrant was an impermissible general warrant, devoid of probable cause and particularity, the very type of warrant that the law and the Constitution was designed prohibit.

Respectfully submitted,

Sierra Villaran
Deputy Public Defender

Michael Price
NACDL

Counsel for LaQuan Dawes

EXHIBIT A:

Report of Spencer J. McInvaille

October 18, 2021

ENVISTA FORENSICS

Report Prepared for:

The People of the State of California v. Laquan Dupree Dawes

Spencer J. McInvaille CTNS, CWA, CCO, CCPA

Digital Forensic Examiner

2700 Gateway Centre Blvd, Suite 100

Morrisville, NC 27560

Qualifications

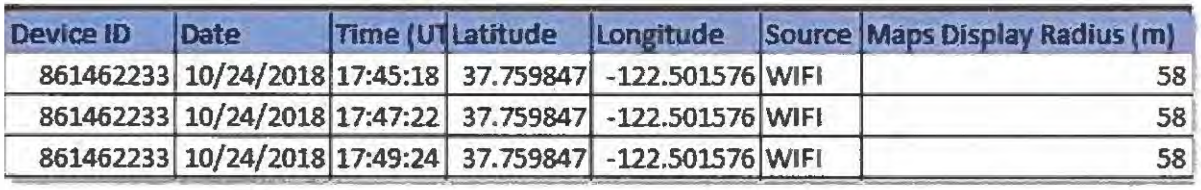
I am currently a Digital Forensic Examiner with Envista Forensics in Morrisville, North Carolina. In this capacity, I provide consulting and analytical services to defense attorneys, prosecutors, and plaintiff attorneys in the area of mobile device forensics. Coming from a law enforcement background, I have analyzed call detail records, historical cell site location information, performed mobile device extractions, and have rendered conclusions as they pertain to criminal cases. I have also performed those same duties in my capacity with Envista Forensics.

I am a Certified Telecommunications Network Specialist (CTNS) and Certified Wireless Analyst (CWA). I am also a Cellebrite Certified Operator (CCO) and Cellebrite Certified Physical Analyst (CCPA).

I have extensive training and experience analyzing location data such as, call detail records, global positioning data, mobile device forensics, mobile networks, wireless communications and rendering opinions about these data types.

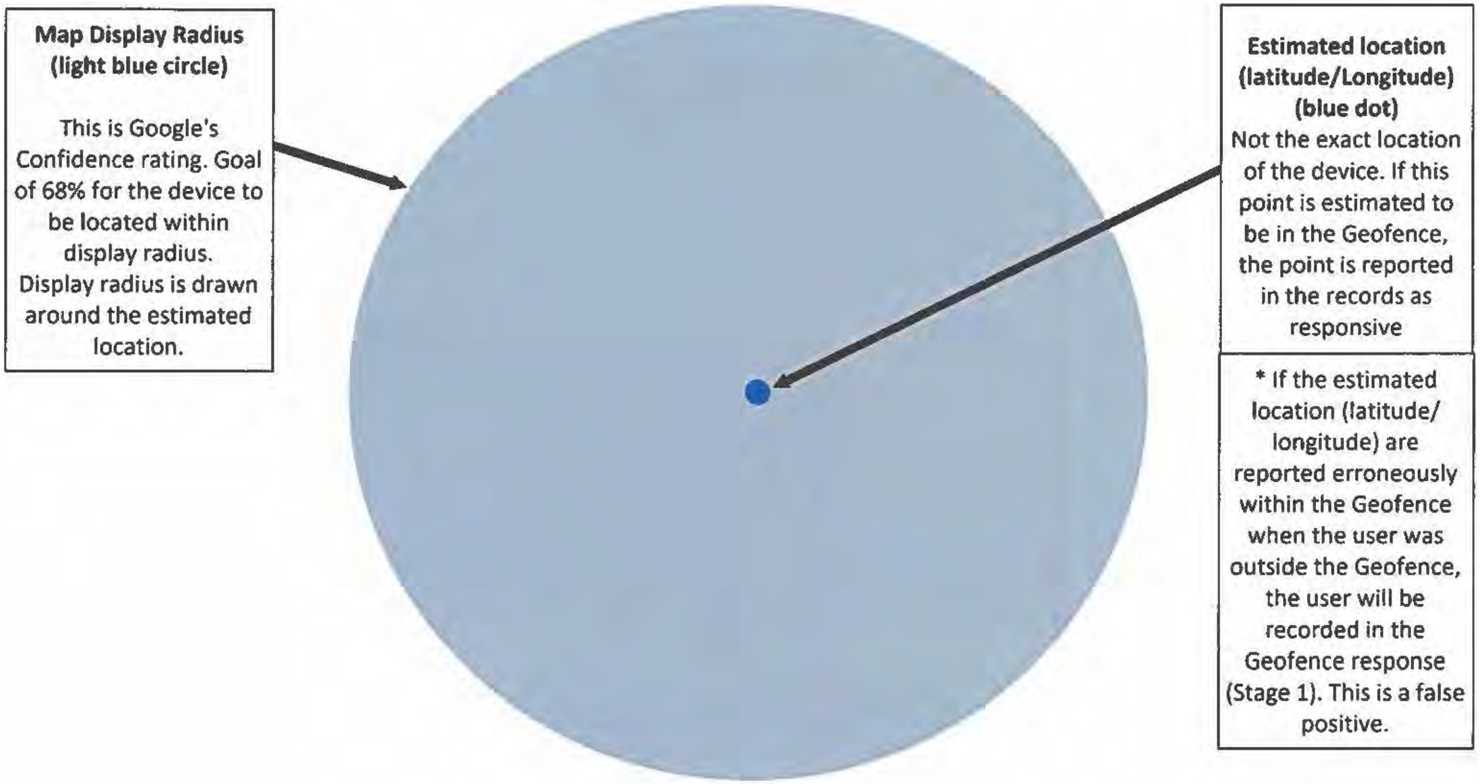
I have qualified and testified as an expert in North Carolina Superior Court, South Carolina General Sessions Court, Minnesota District Court, New Jersey Superior Court, Illinois Superior Court, Alexandria (VA) Circuit Court, Maryland Circuit Court, Texas District Court, California Superior Court, Federal Eastern District of North Carolina, and Federal Eastern District of Virginia in the area of Wireless Cellular Analysis, Location analysis and functions and Mobile Device Forensics.

Figure 1. Example of Data in Google Stage 1 Response



Device ID	Date	Time (UT	Latitude	Longitude	Source	Maps Display Radius (m)
861462233	10/24/2018	17:45:18	37.759847	-122.501576	WIFI	58
861462233	10/24/2018	17:47:22	37.759847	-122.501576	WIFI	58
861462233	10/24/2018	17:49:24	37.759847	-122.501576	WIFI	58

Figure 2. How the data is mapped (Display radius vs. Estimated Latitude and Longitude)



Map Display Radius (light blue circle)

This is Google's Confidence rating. Goal of 68% for the device to be located within display radius. Display radius is drawn around the estimated location.

Estimated location (latitude/Longitude) (blue dot)

Not the exact location of the device. If this point is estimated to be in the Geofence, the point is reported in the records as responsive

* If the estimated location (latitude/ longitude) are reported erroneously within the Geofence when the user was outside the Geofence, the user will be recorded in the Geofence response (Stage 1). This is a false positive.

Figure 3. This is the Geofence chosen by Law Enforcement to be searched by Google.

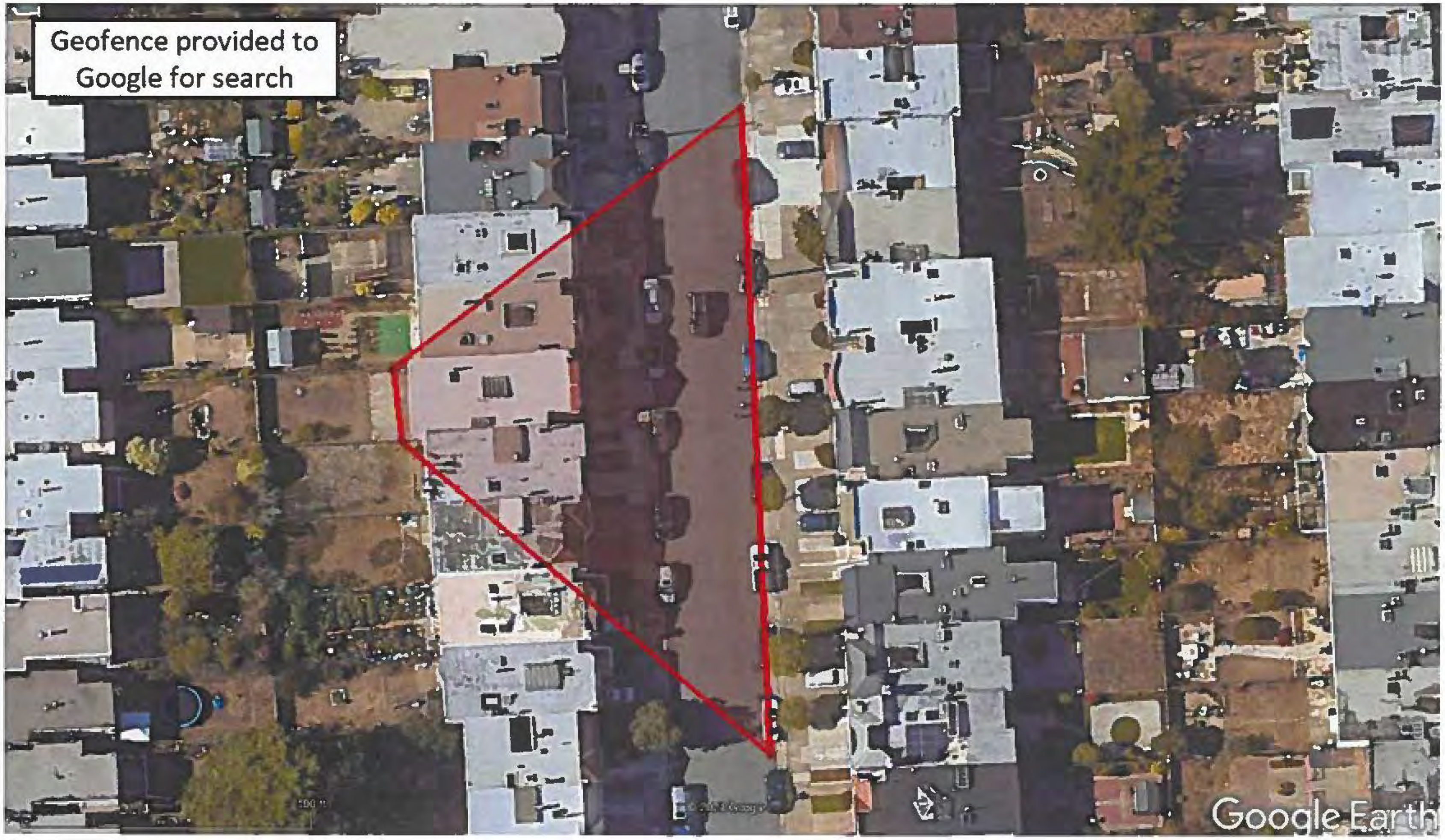
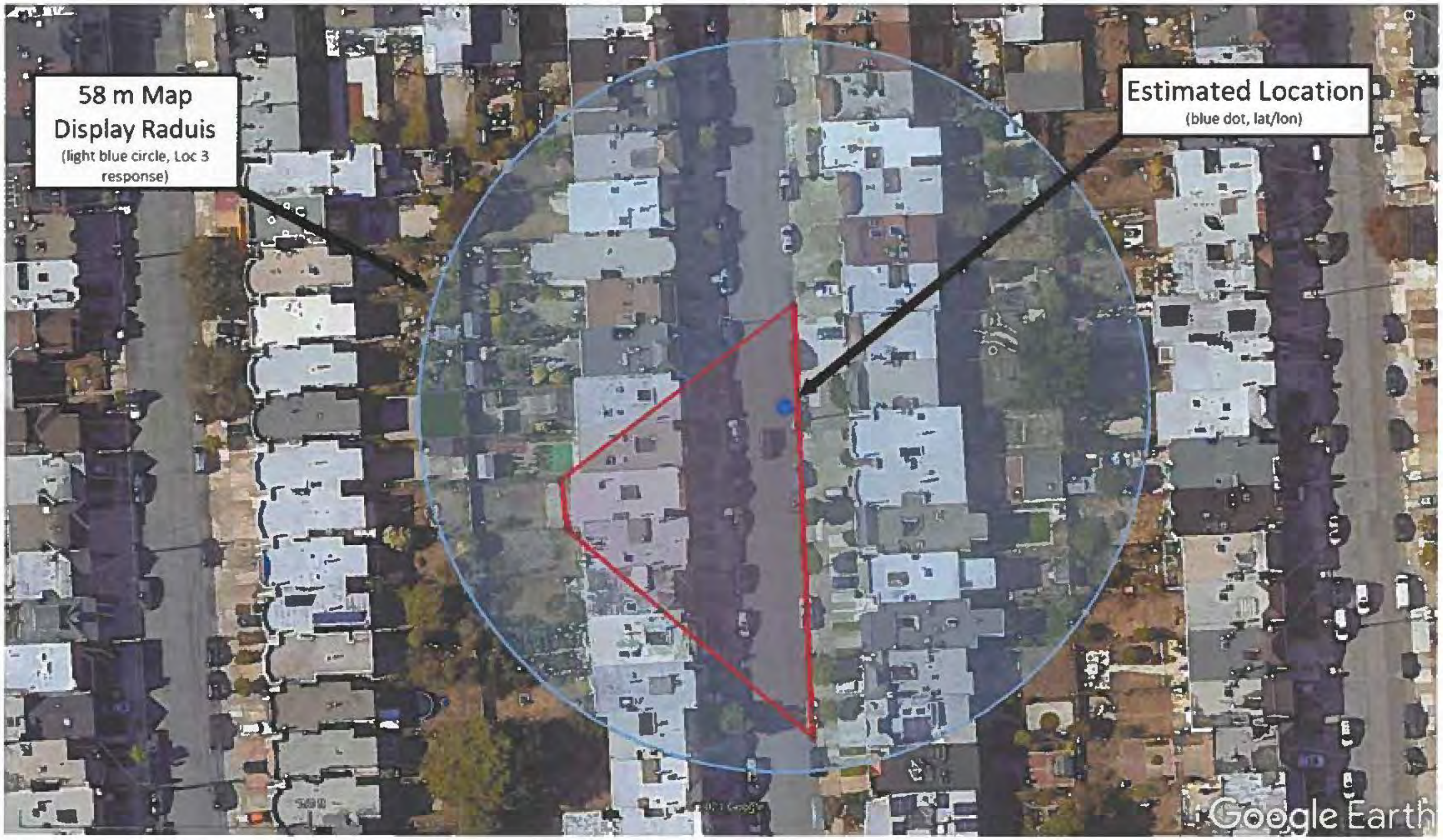


Figure 4. Depicts one of the responsive points from "Location 3".



I have reviewed the Google responses to the Geofence search warrant issued in this case. Figures 1-4 are used as visual aids to understand the Geofence and the data provided in response to its search. Figures 1 and 2 show data from the Stage 1 response as well as an aid to understand how each of the data points is reflected on the map. Figures 3 and 4 show the Geofence provided in the warrant as well as a data point from Figure 1.

When determining users' data responsive to the search, Google uses the estimated latitude and longitude point as the defining factor. This is the estimated location and is not the exact location of the device. Due to this estimate, Google provides the display radius to better understand the possible location of the device. The user is included in the response if the estimated location is within the Geofence (no matter the size of the display radius). In my experience, users' data erroneously calculated with the Geofence were recorded in responsive data to these searches. Due to these false positives, this makes the effective search area larger than the area depicted in the warrant. In Figure 4. the map display radius for the point is 58 meters. This display radius covers an area approximately 7 times the area covered by the Geofence. The area covered by a display radius can be much larger than the area covered by the Geofence. The 58-meter radius has an approximate area of 10.523 square meters. The Geofence drawn has an approximate area of 1,442 square meters. The Geofence includes portions of 6 different homes, the street and sidewalk. The 58 m map display radius shown in figure 4, covers potions of 30 homes and 16 other fenced areas behind homes, the street and sidewalk.

S.J. McInvaille October, 18, 2021
Spencer McInvaille

Digital Forensic Examiner, Envista Forensics

EXHIBIT B:

Sarah Rodriguez Testimony at March 4th and 5th, 2021 Hearing

United States v. Chatrie, No. 3:19-cr-00130

Pgs. 456-457, 552-553.

seems too big, like, the geographic area is too big?

A It's up to the specialist to determine if it needs further review by our counsel team.

Q If the specialist thinks, eh, this just looks too big, they go to the lawyers; right?

A They'll take it to the lawyers. There may be an intermediate step where they engage with a law enforcement officer to collect more information about the investigation itself to provide that context in our consult with legal counsel.

Q So that process happens -- that back and forth process happens between Google and its various employees and counsel and with the law enforcement officer; right?

A That's correct.

Q So Google also -- when did Google create this three-step process?

A I believe there was discussion around it in 2018. And the discussion also involved agencies within law enforcement. So our, like, CCIPS is an agency that works -- that we often engage with -- not us specifically, but our counsel engages with to discuss sort of certain procedures that may be relevant for the way that we -- that Google will need to handle these types of requests, especially with reverse

Location History being a relatively new type of request that Google has started to receive.

THE COURT: So, Ms. Rodriguez, I'm going to ask you to say the words of the agency that you just gave the initials for so our court reporter can get it on the record.

THE WITNESS: I'm not sure what it stands for exactly. So I know it's computer crimes, but it's a federal agency that is related to the handling of those types of requests.

THE COURT: And the full acronym is?

THE WITNESS: CCIPS, C-C-I-P-S.

THE COURT: I'm sorry?

THE WITNESS: C-C-I-P-S.

THE COURT: Okay. Thank you.

BY MS. KOENIG:

Q Do you know when in 2018 that that policy was developed?

A I don't know exactly.

Q Has that policy changed over time?

A Yes. In the early days, we didn't have a policy set forth. So there was a very, you know, sort of extended processing and engagement with our counsel team on the legal investigation side engaging with our law enforcement and information security counsel team or obtained by Google and academic papers that discuss how it's possible to derive approximate locations using Wi-Fi access points and other reference material as well.

Q But you haven't received any specific trainings on geofence warrants?

A Google has not provided us any training on Google geofence warrants.

Q And there aren't any Justice Department policies on Geofence warrants, are there?

A I'm not aware of any policies, per se. We have policies that talk about investigative techniques that we can use, but nothing that focuses particularly on a geofence warrant.

Q And, similarly, there aren't any Justice Department procedures for obtaining geofence warrants, are there?

A There's not procedures, but in working with CCIPS, Computer Crimes and Intellectual Property Section of the Department of Justice, we are able to obtain what we call a "go by," which assists us in the language needed to obtain a geofence search warrant.

Q A go by. Could you explain a little bit more about that? Did you give one to somebody in this case?

A I don't recall that I provided any go bys in this case. But a go by, for us, is a document that has wording and points to remember to make sure we include in a search warrant. For example, Google has specific information that they need in order to process the search warrant. They need a location point. They need a radius or another shape to form that geofence. They also need a time period in order to obtain the records.

And then with the process that I understand has been discussed between CCIPS and Google, we follow the steps that they have laid out in order to work with or in order to serve Google with this search warrant to make sure that Google understands what we are requesting and that we understand what we'll receive back as part of that search warrant process.

MR. PRICE: Your Honor, we have long suspected that the government used a template of some sort in this case. We've asked for it repeatedly in discovery and have not received it. And so I would request that the government provide us with a copy of this go by so that we can review it.

MR. SIMON: Judge, we have -- we didn't use any Department of Justice go by in this case. I think it's been pretty clear that any request from

Proof of Service

I say:

I am over eighteen and not a party to the above action. My business address is 555 Seventh Street, San Francisco, California 94l03.

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

Bianca Calderon-Penaloza
San Francisco District Attorney
350 Rhode Island Street
North Building, Suite 400N
San Francisco, CA 94103

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

Executed on October 18, 2021, at San Francisco, California.

Sierra Villaran