Civ. No. B318310

IN THE COURT OF APPEAL
FOR THE STATE OF CALIFORNIA
SECOND APPELLATE DISTRICT, DIVISION 7

THE PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff and Respondent,

v.

DANIEL MEZA and WALTER MENESES,

Defendants and Appellants.

Appeal from the Superior Court for the County of Los Angeles
The Honorable Laura Walton
Case No. TA150314

AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANTS-APPLELLANTS

---

*Jennifer Lynch (SBN 240701)
** Counsel of Record*
Andrew Crocker (SBN 291596)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax.: (415) 436-9993
jlynch@eff.org
andrew@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF INTERESTED ENTITIES

Pursuant to California Rules of Court 8.208, the Electronic Frontier Foundation ("EFF") states that it is a non-profit, non-partisan civil liberties organization. EFF has no parent corporation and no publicly held corporation owns more than 10% of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Legislative History

Other Authorities

INTRODUCTION AND SUMMARY OF ARGUMENT

The warrant at issue here—a so-called "geofence" or "reverse location" warrant—is a modern version of a general warrant. And like the general warrants so reviled by this country's founders, this warrant cannot survive constitutional scrutiny.

The Fourth Amendment's familiar demands of particularity and probable cause were designed to prevent warrants precisely like this one that give law enforcement broad license to rummage through individuals' private spaces. Prior to the nation's founding, general warrants and "writs of assistance" were used by officials to go house by house, searching for smuggled goods and evidence of seditious libel. *This* general warrant allowed law enforcement to go Google account by Google account, searching each user's private location data for evidence of an alleged crime. The same concerns animating the courts that addressed general warrants in the past are equally present with respect to geofence warrants today; these warrants lack individualized suspicion, allow for unbridled officer discretion, and impact the privacy rights of countless innocent individuals. And, like the 18th-century writs of assistance that inspired the Fourth Amendment's drafters, geofence warrants are especially pernicious because they also have the potential to impact freedom of speech and association. Neither the Fourth Amendment, nor Article 1, Section 13 of the California Constitution tolerate a warrant of this breadth.

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

Because the warrant here granted improper police discretion, lacks particularity, is unconstitutionally overbroad, and violates CalECPA, the warrant should have been suppressed. Amicus urges this Court to find this warrant unconstitutional, overturn the trial court ruling, and suppress all evidence derived from the warrant.

ARGUMENT

I. Geofence Warrants Allow Unfettered Police Access to Location Information on Countless Individuals.

A. Geofence Warrants Rely on Location Data Collected and Stored by Third Parties Like Google.

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

With a geofence warrant—as in this case—the police generally have no identified suspects. Instead, the sole basis for the warrant are three pieces of information: (1) a crime occurred

at a specific location around a given time; (2) people carry cell phones with them all the time that can create a detailed history of everywhere they have been in the past, and (3) companies like Google collect and retain private location-based information that is easily associated with individual user accounts.

The only public reports of geofence warrants have involved Google, which has a particularly robust collection of location data. As Appellant Meza has detailed in his Opening Brief, Google tracks users who have a feature called "Location History" enabled on their mobile devices as they move through the world. This highly precise data is collected from users of both Android devices and Apple IOS devices running Google apps. *See* Appellant Meza's Mot. To Augment the Record Ex. 3 (Br. of Amicus Curiae Google LLC at 6-8, *United States v. Chatrie*, (E.D. Va. Dec. 20, 2019) No. 19-cr-00130 , ECF No. 59-1) (hereinafter "Google Amicus"). It is also collected regardless of whether users are actively engaging with Google apps or not.[1] Users cannot even avoid data collection by putting their phones in "airplane mode."[2]

---

[1] Ryan Nakashima, *Google tracks your movements, like it or not*, AP (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb.

[2] *See* Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, Wired, (Nov. 28, 2022), https://www.wired.co.uk/article/fbi-google-geofence-warrant-january-6. Google draws on a variety of sensors to determine a user's location. *United States v. Chatrie* (E.D. Va. 2022) 590 F.Supp.3d 901, 910. Many of these sensors stay on, even if the phone is in airplane mode.

According to the *New York Times*, Google's Location History database contains information about hundreds of millions of devices around the world, going back a decade or more,[3] and Google has said that, for each geofence warrant, it must search this entire database—sifting through the data of tens of millions of users.[4]

Google emphasizes that users must now opt-in to Location History; however, opting in may be virtually automatic, especially on a mobile device running the Android operating system. (*See* Appellant Meza's Opening Br. (hereinafter "AOB") at 73 (noting that there is no evidence in this case that Mr. Meza opted into location data collection)). Further, if users do opt in, later opting *out* can be confusing; internal Google emails revealed that even the company's own engineers were not sure how to do it.[5] And there is some evidence that regardless of whether users

---

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

[4] Google Amicus at 11.

[5] *See* Alfred Ng, *Google Court Docs Raise Concerns on Geofence Warrants, Location Tracking*, CNET (Aug. 26, 2020), https://www.cnet.com/news/google-court-docs-raise-concerns-on-geofence-warrants-location-tracking/. This is because Google also collects location data through users' other interactions with its products, including web searching and even simply using an Android device. *See* Appellant Meza's Mot. to Augment the Record Ex. 4 (Decl. of Marlo McGriff) (hereinafter "Google Decl.") ¶ 16–17; Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, AP (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb.

later choose to delete their Location History data, that information is still available to Google.[6] The mere act of attempting to delete data can subject users to greater law enforcement scrutiny.[7]

Google's location data has the potential to be highly precise. Google collects location data as frequently as every two minutes from several sources, including "Global Positioning System (GPS) information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol (IP) address information, and the signal strength of nearby Wi-Fi networks." *United States v. Chatrie* (E.D. Va. 2022) 590 F.Supp.3d 901, 908. This allows Google to determine where a user was at a given date and time, sometimes to within twenty meters or less. *Id.* at 936. Google states it can even determine elevation, revealing the floor of a building a user was on at time of collection. *Id.* at 908.

But despite the quantity of sources from which Google infers its users' location, the data it produces in response to a geofence warrant may also be inaccurate, placing devices inside the geofenced area that were, in fact, hundreds of feet away, or excluding devices it mistakenly identified as outside the geographic area specified by the police. *See Chatrie*, 590 F.Supp.3d at 922. This is because Location History "estimates based on multiple inputs, and therefore a user's actual location

---

[6] *See* Harris, *supra* n. 2.

[7] *Id*. (citing geofence warrant used in January 6th investigation and noting that "37 people who attempted to delete their location data following the attacks were singled out by the FBI for greater scrutiny.").

does not necessarily align perfectly with any one isolated L[ocation] H[istory] data point." Appellant Meza's Mot. to Augment the Record Ex. 4 (Decl. of Marlo McGriff) (hereinafter "Google Decl.") ¶24. Relying on GPS, WiFi and other methodology, Google's goal is to accurately infer a user's location within a certain radius a bare 68% of the time. *Id.* In responding to a geofence warrant, Google will produce a user's data if a user's location is recorded as falling within the parameters of the requests, even if the radius corresponding to Google's 68% confidence interval lies partially outside those parameters. *Id.* ¶25. This creates the possibility of both false positives and false negatives—people could be implicated for a crime when they were nowhere near the scene, or the actual perpetrator might not be included at all in the data Google provides to police.

B. The Use of Geofence Warrants Has Increased Dramatically in Less Than a Decade.

Usage of geofence warrants has increased significantly since their first reported application in 2016.[8] In 2021, Google's transparency report revealed that the company received approximately 20,000 geofence warrants between 2018 and 2020.[9] According to the *New York Times*, Google received as

---

[8] *Supplemental Information on Geofence Warrants in the United States*, Google, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf.

[9] *Id*. *See also* Richard Nieva, *Google hit with more than 20,000 geofence warrants from 2018 to 2020*, CNET (Aug. 19, 2021), https://www.cnet.com/tech/tech-industry/google-received-more-than-20k-geofence-warrants-between-2018-20/

many as 180 requests in a single week in 2019.[10] And according to Google, geofence requests now constitute more than a quarter of the total number of all warrants it receives.[11] The vast majority of these requests (95.6%) came from state and local police agencies, with nearly 20% of those coming solely from agencies in California.[12] Further, law enforcement in many states, including California, have ramped up their use of geofence warrants significantly over the last few years—California issued 209 geofence warrants in 2018, but nearly five times that—1,909—in 2020.[13]

Geofence warrants have been used for a wide variety of major and minor crimes, from homicide to sexual assault to retail theft. Minnesota Public Radio reported the technique has been used to try to identify suspects in crimes ranging from murder to

---

[10] Valentino-DeVries, *supra* n. 3. Google does not report absolute numbers of geofence warrants, but it received over 20,000 total warrants in 2019 alone. *Global Requests for User Information*, Google Transparency Report, https://transparencyreport.google.com/user-data/overview?hl=en&user_data_produced=authority:US;series:compliance&lu=legal_process_breakdown&user_requests_report_period=series:requests,accounts;authority:US;time:Y2019H2&legal_process_breakdown=expanded:0,1 (limited to US legal process and expanded for the year 2019)

[11] *Supplemental Information on Geofence Warrants in the United States, Google*, *available at* https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf

[12] *Id.*

[13] *Id.* at 2. (*See* link within document to supplemental data available for download as a CSV file).

theft of a pickup truck and, separately, $650 worth of tires.[14]

While only a small fraction of geofence requests have been made public, reports indicate that law enforcement frequently seeks information from large geographic areas and extended time periods and may receive data on hundreds or thousands of devices in response to such warrants. In one case in Minnesota, police sought "location data for every cellphone in dense, urban areas surrounding [two] businesses over a 33-hour window."[15] In a case in Wisconsin, the federal Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") served Google with two warrants that sought data for all Google customers within areas in Milwaukee covering three hectares (roughly seven and a half football fields) during a total of nine hours.[16] In response, Google provided the government with identifying information for nearly 1,500 devices. Even in cases with more limited search windows, geofence warrants routinely produce information belonging to

---

[14] Tony Webster, *How did the police know you were near a crime scene? Google told them*, MPRNews (Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants.

[15] *Id. See also, e.g.,* Palm Beach, Florida Geofence Warrant (May 21, 2018), *available at* https://int.nyt.com/data/documenthelper/764-fdlelocationsearch/d448fe5dbad9f5720cd3/optimized/full.pdf#page=1 (warrant sought information for a six-hour time period).

[16] *See* Thomas Brewster, *Google Hands Feds 1,500 Phone Locations In Unprecedented 'Geofence' Search*, Forbes (Dec. 11, 2019, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/.

tens or even hundreds of devices.[17]

C. Geofence Warrants Can Implicate Innocent People and Threaten Protected Speech.

Nearly all of the information provided to law enforcement in response to a geofence warrant pertains to individuals unconnected to the crime under investigation. Yet geofence warrants grant law enforcement agents the sole discretion to choose which individuals to target for further investigation. This can lead to innocent people being subjected to police suspicion and the resulting consequences.

In one case in Gainesville, Florida, police sought detailed information about a man in connection with a burglary after seeing his travel history in the first step of a geofence warrant.[18] However, the man's travel history was generated through an

---

[17] *See, e.g.*, *United States v. Chatrie*, 590 F. Supp. 3d 901, 921 (E.D. Va. 2022) (warrant produced identifiers belonging to 19 devices); Tyler Dukes & Lena Tillet, *In quest to solve murders, Raleigh community targeted twice by Google warrants*, WRAL (July 25, 2019), https://www.wral.com/scene-of-a-crime-raleigh-police-search-google-accounts-as-part-of-downtown-fire-probe/17340984/ (geofence warrant produced information on 39 devices);
Jennifer Lynch, *First Court in California Suppresses Evidence from Overbroad Geofence Warrant*, EFF (Oct. 11, 2022), https://www.eff.org/deeplinks/2022/10/california-court-suppresses-evidence-overbroad-geofence-warrant (court was concerned about geofence warrant that included 13 innocent people's homes).

[18] Jon Schuppe, *Google Tracked his Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC News (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

exercise tracking app he used to log months of bike rides, including a loop ride that happened to take him past the site of the burglary several times. Investigators eventually acknowledged he should not have been a suspect. In another case in Arizona, a geofence warrant led police to believe an innocent man was responsible for murder.[19] The police eventually dropped the case, but not until after they held the man in custody for a week, leading him to lose his job and his car.[20] In Minnesota, another innocent man's name was disclosed to a local reporter after police files identified him in a burglary investigation.[21] Misidentifications like these are more likely to occur and are more likely to have serious ramifications in the geofence context because the only link between an individual and the crime is that the individual happened to be in the area around the time the crime occurred. This can force a suspect into the position of having to prove their innocence—that they were in the area for an unrelated purpose—rather than the police having to prove their guilt, and it increases the risk of both confirmation bias and implicit bias.[22]

---

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

[20] *Id.*

[21] *Id.*

[22] *See, e.g.,* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327 (2015).

Geofence warrants can and have been used in ways that impact other fundamental rights, including free speech and freedom of association. For example, during the protests following the police shooting of Jacob Blake,[23] the ATF used at least 12 geofence warrants to collect people's location data during protests in Kenosha, Wisconsin, one of which encompassed a third of a major public park for a two-hour window.[24] Police also used a geofence warrant in Minneapolis around the time of the protests following the police killing of George Floyd.[25] And geofence warrants may be used in the near future to target people for reproductive health choices and outcomes. Google has been sufficiently concerned about this possibility to pledge to delete location information shortly after someone visits an abortion clinic, though critics have argued this would be

---

[23] Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson*, Forbes (Aug. 31, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-dragnets-on-phone-data-across-13-kenosha-protest-arsons/?sh=5d279d646bfa.; Russell Brandom, *How police laid down a geofence dragnet for Kenosha protestors*, The Verge (Aug. 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake.

[24] *See* Warrant: *In the Matter of the Search of Information that is Stored at the Premises Controlled by Google Concerning 711 59th Place, Kenosha, WI*, *available at* https://www.documentcloud.org/documents/21052213-google-geofence-warrant-used-in-kenosha-riot-arson-at-library

[25] Zach Whittaker, *Minneapolis police tapped Google to identify George Floyd protesters*, TechCrunch (Feb. 6, 2021), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/

insufficient to protect patients.[26]

D. Geofence Warrants Can Reveal Sensitive Information, Impacting Californians' Strong Privacy Rights.

Geofence warrants, like all warrants for location data, can reveal sensitive and private information on where people have travelled and can create inferences about what a person might have been doing at the time. Such warrants can place people at doctors' offices, union halls, or houses of worship. And by revealing patterns of travel and devices near one another, location data can tell a story about where and with whom people live, socialize, visit, vacation, worship, and much more. As one court noted in addressing the constitutionality of a geofence warrant, "[e]ven 'anonymized' location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one- or two-hour period." *Chatrie*, 590 F.Supp.3d at 931 n.39.

California courts should be especially concerned about suspicionless warrants for location data because of California's long history of protections for residents' privacy, many of which have involved electronic data and communications and were

---

[26] Jen Fitzpatrick, *Protecting people's privacy on health topics*, Google (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/; *but see* Alfred Ng, *'A uniquely dangerous tool': How Google's data can help states track abortions*, Politico (July 18, 2022), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906.

prompted by fears of pervasive government and private snooping.

California's protections for electronic communications date back more than 150 years. It was the first state to outlaw the tapping of telegraph lines in 1862.[27] A century later, in 1967, it was one of the first states in the country to establish broad protections against private eavesdropping and wiretapping.[28] And in 1972, based largely on concerns with excessive government snooping and mass corporate collection of electronic data, Californians added an explicit right to privacy to the state constitution.

The concerns animating the push to add privacy to the state constitution resonate today, especially with respect to government access to data collected by private companies. By the late 1960s, reports of rampant government spying on labor, legislators, and left-leaning groups and individuals, both in California and across the nation, permeated public consciousness.[29] At the same time, people were increasingly concerned about the rise of computer databases, data aggregation, and data sharing. California legislators recognized the lack of sufficient explicit federal and state protections against

---

[27] H. Lee Van Boven, *Electronic Surveillance in California: A Study in State Legislative Control*, 57 Cal. L. Rev., 1182, 1189 (1969).

[28] *Id.* at 1191 (discussing the California Invasion of Privacy Act).

[29] *See, e.g.,* Van Boven, *Electronic Surveillance in California: A Study in State Legislative Control*, *supra* n. 27 at 1212-13 (citing various congressional hearings in the 1950s and 1960s and noting "Debate on the general question of whether police surveillance should be permitted at all has raged for 40 years.").

"state surveillance, record collection and government snooping into our personal lives" and the need for "new safeguards to meet the new dangers."[30] In addition, supporters of Proposition 11, which added privacy to the constitution, were expressly concerned with government and private businesses working together to "stockpile unnecessary information" and "misus[e] information gathered for one purpose in order to serve other purposes[.]"[31] Much like today, Californians recognized that "[t]he average citizen also does not have control over what information is collected about him. Much is secretly collected . . . [and] Modern technology is capable of monitoring, centralizing and computerizing this information which eliminates any possibility of individual privacy."[32]

Since adding privacy to the state constitution, California has continued to strengthen its residents' privacy rights, including those rights with respect to electronic communications and data, through both court cases and explicit statutory provisions, in many cases ensuring Californians have more robust privacy rights than anywhere else in the country. For example, in the late 1970s, the state supreme court recognized

---

[30] *See* J. Clark Kelso, *California's Right to Privacy*, 19 Pepp. L. Rev. 327, 424 (1992) (citing Assembly Staff Report for ACA 51, the measure that put the privacy right on the state ballot as Proposition 11). https://www.law.berkeley.edu/wp-content/uploads/2016/12/Kelso-Californias-Constitutional-Right-to-Privacy.pdf.

[31] *Id.* at 428 (citing Proposition 11 ballot argument).

[32] *Id.*

people have a reasonable expectation of privacy in records stored with third parties like banks and phone companies, despite the federal Supreme Court's rulings to the contrary. *See People v. Blair* (1979) 25 Cal.3d 640, 651, 602 P.2d 738, 745*; Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249*; cf Smith v. Maryland* (1979) 442 U.S. 735. And in 2015, California passed the nation's strongest protections against electronic surveillance with the California Electronic Communications Privacy Act (CalECPA), Penal Code § 1546 et seq, which created statutory privacy protections for location data, like the data at issue in this case. This occurred three years before the Supreme Court recognized similar constitutional protections through *Carpenter v. United States* (2018) 138 S.Ct. 2206. Since then, California has adopted many other privacy protections impacting data collected by both private companies and the government.[33]

Even last year, with overwhelming legislative support, California passed landmark protections to ensure electronic data cannot be shared across state lines in ways that would jeopardize reproductive or transgender rights. *See* Assem. Bill No. 1242 approved by Governor Sep. 27, 2022 (2021-2022 Reg. Sess.); Assem. Bill No. 2091 approved by Governor Sep. 27, 2022 (2021-2022 Reg. Sess.); Sen. Bill No. 107 approved by Governor Sep. 29, 2022 (2021-2022 Reg. Sess.). And, a significant majority of voters passed Proposition 1, amending the constitution to ensure that

---

[33] *See e.g.*, Privacy Laws, California Office of the Attorney General (listing various state privacy laws) https://oag.ca.gov/privacy/privacy-laws.

Californians' right to privacy also explicitly protects "an individual's reproductive freedom in their most intimate decisions." Cal. Const. art 1, §1.1, added Nov. 8, 2022, by Prop. 1. Res.Ch. 97, 2022.

Through legislative, judicial, and voter-approved privacy protections like these, Californians have repeatedly made clear the high bar that must be met before allowing government access to data that can reveal sensitive and intimate details about their lives. Modern technology and the ability of companies to stockpile vast stores of "information about every facet of an individual's life"[34]—the concerns that prompted the passage of Proposition 11 in 1972—have made it possible for companies like Google to monitor our every move and then provide that data to police in response to a geofence warrant. As in 1972, the average citizen now likely has no idea of the full scope of information Google is collecting on them and certainly has no control over whether that information is disclosed to the police.[35] California's historical protections for privacy and the concerns that prompted those

---

[34] Van Boven, *Electronic Surveillance in California: A Study in State Legislative Control*, *supra* n. 27; *Voter Information Guide for 1972 General Election*, 27, *available at* https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1773&context=ca_ballot_props ("Modern technology is capable of monitoring, centralizing and computerizing this information which eliminates any possibility of individual privacy.")

[35] Voter Guide at 27 ("The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them.")

protections should raise special concern about the constitutionality of geofence warrants.

II. The Warrant in This Case Provided LASD with Unfettered Discretion and Exposed Data of Users in Sensitive Locations.

A. LASD Took Advantage of the Warrant's Lack of Judicial Oversight.

The geofence warrant used in this case included the typical three-step process described in Appellant's Opening Brief and did not require police to seek an additional warrant at any step. AOB at 36; 1CT 186-87. Such a process, lacking in judicial oversight, provides officers with unbridled discretion to determine who to pursue further and who to unmask. LASD took full advantage of this discretion at several points in the process. First, the crime analyst refused to reduce the geographic area covered by at least one of the geofences, even after a Google employee said that area would produce "voluminous results." (AOB 45.) Second, after this exchange, the LASD crime analyst decided not to follow the three-step process laid out in the warrant, in effect ignoring the parameters of the warrant itself. Without going back to a judge, the crime analyst demanded that Google cull through results of searches of each of the six locations to find devices present at more than one location. Google did so, identifying eight devices. Finally, although the warrant said that LASD would review this list of devices and remove those that were not relevant to the investigation, the crime analyst told Google to unmask the identities of individuals associated with *all* eight devices. Six of these devices do not seem to have been linked to the crime under

investigation.

B. The Geographic Areas and Time Periods Designated by LASD Exposed the Data of Countless People in Sensitive Locations

As noted above, for each geofence warrant, Google has said that it must search its *entire* Location History database—sifting through the data of tens of millions of users, nearly all of whom are not at all connected to the crime under investigation. However, even if the searches requested in this case only involved the data of users within the geographic areas delineated in the warrant, they would still be unconstitutionally expansive. That is because the geofence warrant in this case covered six discrete, heavily populated areas during time periods where people were likely to be in sensitive places, like their homes or church or a medical center, or driving along one of the many busy streets included within the geofenced areas.

LASD used a single warrant to try to identify all devices within a total geographic area equivalent to about 24 football fields or five to six city blocks[36] during five morning commute hours on a Friday in March. These areas are in several of the most densely populated cities in the greater Los Angeles area, including Lynwood, with a population of 13,894 people per square mile and Paramount, with a population of 11,367 people per

[36] *See How Many Acres Is A City Block?*, Measuring Stuff (March 8, 2022) https://measuringstuff.com/how-many-acres-is-a-city-block/.

square mile.[37] The number of devices identifiable within in each of these six areas would have been "voluminous." (AOB 45 (citing a Google employee's conversation with LASD crime analyst.))

The geographic areas designated within the warrant also included many sensitive locations. For example,

- the "Corinthian Apartments" geofence included multiple large, multi-unit apartment buildings, likely housing hundreds of people. The Corinthian Apartments complex alone contains 54 two- and three-bedroom units;[38]

- the "Chevron" geofence in Downey includes lawyers' and accountants' offices, several restaurants, a liquor store, and a carwash;

- the "Arco" geofence includes many houses, parking lots, and a medical center;

- the "Strip Mall" geofence includes a dense residential area, the Christ First Baptist Church, restaurants, and a nail salon;

- the "Chevron" geofence in Lynwood includes the All People's Church Lynwood, several restaurants and stores, three barber shops, and the Lynwood Teachers Association, a union that represents

---

[37] *QuickFacts: Paramount city, California*, U.S. Census, https://www.census.gov/quickfacts/paramountcitycalifornia; *QuickFacts: Paramount city, California*, U.S. Census, https://www.census.gov/quickfacts/fact/table/lynwoodcitycalifornia/IPE120221.

[38] *See* The Corinthian Apartments, Apartments.com, https://www.apartments.com/the-corinthian-apartments-downey-ca/4r9qf7k/.

"approximately 725 dedicated educators serving Lynwood Unified School District."[39]

- The "Bank of America" geofence includes several banks and restaurants, a pharmacy, a medical center, and the Paramount Public Library. 1CT 184-86.

Access to identifying information on devices at any of these locations could allow officers to infer private and revealing information about the device owners and the people they were with. *See* Section I.D, *supra.*

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

LASD's request to Google to search for all location data for the mobile devices of everyone who was in the "Target Locations" around the times the crime occurred is an unconstitutional general warrant. 1 CT 186.

Like other "papers" and "effects," a person's location information can only be seized and searched with a warrant. *Carpenter v. United States* (2018) 138 S.Ct. 2206, 2217. That warrant must satisfy all the Fourth Amendment's familiar requirements—that it be issued by a neutral and detached judicial officer, supported by probable cause and describing with particularity the place to be searched and the items to be seized. *See Ex parte Jackson* (1878) 96 U.S. 727, 733; *United States v. Van Leeuwen* (1970) 397 U.S. 249, 251. It is "axiomatic that a

[39] About Us: We Are Lynwood Teachers Association, LTA, http://www.lynwoodta.org/about/.

warrant may not authorize a search broader than the facts supporting its issuance." *People v. Frank* (1985) 38 Cal.3d 711, 728.[40]

The geofence warrant in this case fails these requirements. It is overbroad because it encompasses data and accounts that were in no way connected to the crime under investigation. *See id*. at 727. In some instances, data produced was outside the boundaries of the warrant itself. Google Decl. ¶25. It fails to meet the Fourth Amendment's particularity requirement because it does not identify any particular person, device, or account to be searched. *See Stanford v. Texas* (1965) 379 U.S. 476, 485-86. And it is not supported by probable cause because the mere fact that many, or even most, people use devices that record and share location information with Google is insufficient to show the perpetrator used such a device, much less to justify a search of the location history of *all* Google's users, or even all users in the warrant's target locations during the specified time periods. *See Ybarra v. Illinois* (1979) 444 U.S. 85, 91-92 ("mere propinquity" to criminal activity insufficient to establish probable cause); *Chatrie*, 590 F.Supp.3d at 927 (warrants that "authorize the search of every person within a particular area must establish probable cause to search every one of those persons") (citing *United States v. Hurwitz* (4th Cir. 2006) 459 F.3d 463, 473).

---

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

In effect, this warrant gave LASD license to search through the location information of millions of Google users around the globe to find anyone who was in the Target Locations, without particularized probable cause to search anyone in particular. Section I.A, *supra*. It gave them the authority to require Google to produce more information about particular devices that, at LASD's own discretion, it deemed of interest, again without demonstrated probable cause that any of them were connected to a crime. And in execution, the Sheriffs' Department and Google abandoned even these unconstitutionally lax standards to design their own ad hoc search that no court had authorized. AOB 45. As the California Supreme Court has recognized, "[t]he vice of an overbroad warrant" such as this one "is that it invites the police to treat it merely as an excuse to conduct an unconstitutional general search." *Frank*, 38 Cal.3d at 726.

A. The Fourth Amendment Was Drafted to Preclude General Warrants.

In the American colonies, British agents used general warrants, also known as "writs of assistance," to conduct broad searches for smuggled goods, limited only by the agents' own discretion. *See Stanford*, 379 U.S. at 481-82 (describing writs of assistance and their influence on the drafters of the Fourth Amendment).[41] "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be

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

searched." *Steagald v. United States* (1981) 451 U.S. 204, 220. "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley v. California* (2014) 573 U.S. 373, 403.

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

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

B. Geofence Warrants Have Direct Parallels to the General Warrants that Inspired the Fourth Amendment and Are Similarly Per Se Unconstitutional.

A warrant purporting to authorize a reverse location search is a digital analogue to an arrest warrant that authorizes officers to search every house in an area of a town—simply on the chance that someone connected with a crime might be located inside one. Like the general warrants and writs of assistance used in England and Colonial America, this warrant's lack of particularity and overbreadth invites the police to treat it as an excuse to conduct an unconstitutional general search. *See Frank*, 38 Cal. 3d at 726.

Here, the geofence "warrant specified only an offense" and left to the LASD's discretion "the decision as to which persons" should be pursued. *Steagald*, 451 U.S. at 220. The warrant did not name particular suspects or even particular accounts. Instead, it sought information on *all* accounts associated with devices that happened to be in several general areas related to a crime. And as described above, it may have resulted in the search and production of data corresponding to devices that were never even in those general areas. *See* Section I.C, *supra*. The warrant gave law enforcement unrestricted license to search each of these accounts and then, *at LASD's own discretion*, to conduct a further search of a subset of those devices, based on no clear, limiting criteria other than that certain accounts would be "identified [by LASD] as relevant." 1 CT 187. But, with a proper search warrant, "[n]othing should be left to the discretion of the officer." *People v.*

Dumas (1973) 9 Cal.3d 871, 880. The geofence warrant is precisely the sort of "general, exploratory rummaging" the Fourth Amendment was intended to forestall. *Coolidge v. New Hampshire* (1971) 403 U.S. 443, 467; *Andresen v. Maryland* (1976) 427 U.S. 463, 479-480.

The California Supreme Court has held that "[t]he requirement of particularity is designed to prevent general exploratory searches which unreasonably interfere with a person's right to privacy." *Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249. When a warrant is unduly broad, it is more likely to reach information that is "ordinarily innocuous and [] not necessarily connected with a crime." *Aday v. Super. Ct. of Alameda Cty.* (1961) 55 Cal.2d 789, 796. Where, as here, the categories of records sought are "so sweeping" as to include every device in a given area, the warrant places "no meaningful restriction on the things to be seized. Such a warrant is similar to the general warrant permitting unlimited search, which has long been condemned." *Id.*[42]

---

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

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

Search warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet" of information "to be seized at the discretion of the State." *United States v. Bridges* (9th Cir. 2003) 344 F.3d 1010, 1016. Searches like these—where the only information the police have is that a crime has occurred—are just that: a "dragnet" that inevitably implicates innocent people who happen to be in the wrong place at the wrong time. *See* Section I.C, *supra*. Google releases data to the police that includes location history for people with no connection to the crime under investigation. This kind of search turns every device owner in the area during the time at issue—and some even outside the area—into a suspect, for no other reason than that they own a device

that shares location information with Google.[43]

C. The Geofence Warrant in this Case was Overbroad, Lacked Probable Cause, and Provided LASD with Nearly Unlimited Discretion in Its Execution.

Even if geofence warrants are not categorically unconstitutional general warrants, they must satisfy the requirements of particularity and probable cause on a case-by-case basis. The geofence warrant in this case failed to do so.

1. *The Vast Majority of Courts to Consider Individual Geofence Warrants Have Found Constitutional Defects.*

Although geofence warrants are a relatively new technique, the overwhelming majority of courts to consider individual geofence warrants have found significant constitutional defects that also exist in the warrant at issue in this case. Of the two available opinions adjudicating the validity of a geofence warrant after its execution, both found the geofence warrant at issue to be unconstitutional under the Fourth Amendment. *United States v. Chatrie* (E.D. Va. 2022) 590 F.Supp.3d 901*; People v. Dawes* (San

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

Francisco Sup. Ct. Sep. 30, 2022) No. 19002022.[44] Similarly, of the six publicly available federal court opinions addressing geofence warrant applications *pre*-execution, four denied the applications. *See Matter of Search of Information Stored at Premises Controlled by Google* (N.D. Ill., July 8, 2020, No. 20 M 297) 2020 WL 5491763 (hereinafter "*Pharma I*") (denying application); *Matter of Search of Information Stored at Premises Controlled by Google* (N.D. Ill. July 24, 2020 No. 20-mc-392), ECF No. 5 (hereinafter "*Pharma II*") (denying application); *Matter of Search of Information Stored at Premises Controlled by Google* (N.D. Ill. 2020) 481 F.Supp.3d 730 (hereinafter "*Pharma III*") (denying application); *Matter of Search of Information that is Stored at Premises Controlled by Google, LLC* (D. Kan. 2021) 542 F.Supp.3d 1153 (hereinafter "*Kansas Federal Crimes*") (denying application). *But see Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation* (N.D. Ill. 2020) 497 F.Supp.3d 345 (hereinafter "*Arson*") (approving application); *Matter of Search of Information that is Stored at Premises Controlled by Google LLC* (D.D.C. 2021) 579 F.Supp.3d 62 (hereinafter *"D.C. Federal Crimes*") (approving application). Finally, the only publicly available state court opinion addressing a geofence warrant pre-execution denied

[44] *See* Bart Huff & Daniel de Zayas, *Another Geofence Warrant Struck Down*, Zwillgen (Oct. 28, 2022), https://www.zwillgen.com/law-enforcement/another-geofence-warrant-knocked-down. The Superior Court opinion is available at https://www.eff.org/document/people-v-dawes-order-granting-motion-quash-geofence-warrant-california.

it, noting that it had also "previously declined to issue the handful of proposed geofence search warrants presented to it." *In re the Search of Information Stored at the Premises Controlled by Google,* 2022 WL 584326, *1 (Va. Cir. Ct. Feb. 24, 2022) (hereinafter "*Virginia Shooting*").

The unifying theme of these cases is that law enforcement must demonstrate particularized probable cause as to *every* device within the geofence whose location data is searched.

2. *The Geofence Warrant in This Case was Insufficiently Particularized and Lacked Probable Cause to Support a Search of Every Device.*

The geofence warrant in this case in no way approaches this requirement. Instead, it relies on what the *Chatrie* court called an "inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby." *Chatrie*, 509 F.Supp.3d at 933 (rejecting government's argument that rested on "'mere propinquity to others' rationale" already rejected by the Supreme Court in *Ybarra*); *see also id.* at 929 (citing *Maryland v. Pringle* (2003) 540 U.S. 366, 371). The affidavit in support of the geofence warrant here stated only that "suspects involved in criminal activity will typically use cellular phones to communicate when multiple suspects are involved." 1 CT 193. This is even less specific than in *Chatrie*, where law enforcement had surveillance footage showing the suspect holding and apparently using a cell phone during the crime. 509 F.Supp.3d at 930. Yet the *Chatrie*

court noted that even though "a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information," the warrant "on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." *Id.* at 929–930 (emphasis original). The court concluded it was "difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing." *Id.* at 930. *See also Pharma III*, 481 F.Supp.3d at 752 ("[T]he proposed warrant would admittedly capture the device IDs . . . for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone—other than the Unknown Subject—entering those locations is involved in the subject offense or in any other crime.").

Similarly, the geofence warrant here lacked particularity because it failed to place a "meaningful restriction" on the places to be searched and the objects to be seized. *Burrows,* 13 Cal.3d at 249; *Smith,* 21 Cal.App.4th at 949. This lack of particularity can be shown in a least two ways.

First, the temporal and geographic boundaries in the geofence warrant failed to limit the scope of the search. The scope of the geofence warrant in this case was at least comparable, if not even broader, than other geofence warrants courts have found to be unconstitutionally overbroad. The warrant here authorized the search of *six* separate locations of roughly a Los Angeles city block each, for a total of over 300 minutes, including a number of major thoroughfares, as well as densely populated areas full of

businesses and residences. *See* Section II.B, *supra*. In *Chatrie,* for example, the court found that the warrant authorizing the search of a circular area with 150-meter radius—an area of 17.5 acres—over the course of 120 minutes, including a church, a hotel and a residence, presented too many risks of sweeping in innocent individuals who had no way to assert their privacy rights. 590 F.Supp.3d at 918, 926. Courts have rejected applications for narrower geofence warrants as well. In *Pharma I*, the Northern District of Illinois court found that the proposed search area covering approximately eight acres of land "in a congested urban area" and including "residences, businesses, and healthcare providers" was too broad. *Pharma I*, 2020 WL 5491763, at *5; In *Virginia Shooting*, the court rejected as overbroad a proposed geofence that included the entire area a *single* motel, even though the crime being investigated took place in the motel's front parking lot. 2022 WL 584326, at *7. And in *Kansas Federal Crimes*, the court rejected a proposed area covering "the sizeable business establishment" where the crimes took place as well as "other residences and businesses" within the margin of error. 542 F.Supp.3d at 1155, 1158. The court also noted that the nexus between the crime and the proposed one-hour time window for the warrant was "weak." *Id.* Even in the two reported decisions approving geofence warrant applications, courts have highlighted that the proposed target locations covered relatively unpopulated or industrial areas that did not encompass "residences or other particularly sensitive locations." *D.C. Federal Crimes*, 579 F.Supp.3d at 85; *Arson*, 497 F.Supp.3d at 348 (target locations

excluded "residences and commercial buildings along the streets" leading to and from the sites of crimes).

3. *The Geofence Warrant Granted LASD Nearly Unlimited Discretion in Determining its Execution.*

The warrant at issue in this case was constitutionally deficient for another reason: it granted police nearly "unlimited discretion to obtain from Google the device IDs . . . of anyone whose Google-connected devices traversed the geofences . . . based on nothing more than the 'propinquity' of these persons to the Unknown Subject at or near the time" of the criminal activity. *Chatrie,* 590 F.Supp.3d at 931 (quoting *Pharma III*, 481 F.Supp.3d at 753). This is apparent even in the multi-step process for narrowing the number of devices of interest. Even though the initial release purportedly only included accounts identified on an "Anonymized List," [45] the warrant still required Google to later release, at LASD's discretion, "identifying information" on a subset of those accounts that included "but [was] not limited to, subscriber's name, email addresses, services subscribed to, last six (6) months of IP history, SMS account number, and registration IP." 1 CT 187. The second disclosure is not based on the determination of a neutral and detached

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

magistrate: it is based solely on law enforcement's own determination of "relevancy." *Id*. As in *Chatrie*, the subsequent steps "leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users." 590 F.Supp.3d at 934 (emphasis original). *See also Pharma III*, 481 F. Supp. 3d at 754 (same procedure "puts no limit on the government's discretion" to select which devices to identify). In *D.C. Federal Crimes*, the court sought to remedy this problem by requiring the government to seek further court authorization in the form of a new warrant before requiring Google to identify accounts of interest, a step notably absent here. 579 F.Supp.3d at 89 & n.25. Here, the lack of anything approaching "meaningful restrictions" on the warrant can be seen in the negotiations between the LASD representative and Google. LASD refused Google's request narrow its search areas and instead jettisoned the unconstitutional procedure outlined in the warrant in favor of an ad hoc narrowing technique. This technique still produced identifying information and location data on eight devices, none of which were subject to a particular description in the warrant. AOB at 45.

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

IV. The Geofence Warrant Violated CalECPA.

In addition to the protections provided by the Fourth Amendment and Article 1, Section 13, CalECPA, Penal Code § 1546 - § 1546.6, places important additional restrictions on law

enforcement access to private electronic information by California law enforcement officials. The geofence warrant likewise violates CalECPA's stringent requirements.

A. CalECPA Guarantees Individuals' Privacy in Electronic Information, including Location Information, by Placing Strict Limits on Law Enforcement Access to That Information.

The legislature drafted CalECPA with two goals: first, to provide a clear statutory framework for the application of existing state and federal constitutional and statutory protections for private electronic information—protections that had been unevenly applied in the digital age; second, to provide *additional* guarantees for that private electronic information, above and beyond existing statutory and constitutional protections. Assem. Comm. on Privacy and Consumer Protection Rep. at 5 (Ca. Jun. 23, 2015) ("This bill is intended to both codify and expand on existing" protections for electronic information).[46] For these reasons, CalECPA provides the strongest digital privacy protections in the nation. *See* Susan Freiwald, *CalECPA: At the*

---

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

Privacy Vanguard, 33 Berkeley Tech. L.J. 131, 133 (2018).[47]

CalECPA requires law enforcement agencies to obtain a probable-cause warrant for almost all electronic information, including location information, § 1546.1. It also imposes heightened specificity standards and stringent particularity requirements on those warrants, § 1546.1(d)(1). The statute also specifies explicit minimization rules for data unrelated to law enforcement's investigation, § 1546.1(d)(2); imposes clear notice requirements, § 1546.2; and provides a robust suppression remedy, § 1546.4(a).

The distinct risks to individual privacy posed by digital searches of electronic information were key motivation for the passage of CalECPA. *See, e.g.*, Assem. Comm. on Privacy and Consumer Protection Report at 8 (noting bill's requirements "explicitly limit the searches to necessary information"). As Professor Freiwald explains, CalECPA's specific warrant requirements work to prevent the type of expansive digital

---

[47] Professor Freiwald was intimately involved in CalECPA's passage. She served as "an issue expert for CalECPA's authors, State Senators Mark Leno and Joel Anderson, and as a member of the bill's policy and language teams. In that capacity, [she] helped answer questions about the bill's language, testified at legislative committee hearings about its legal impact, and coordinated dozens of academic colleagues to send a scholarly support letter to California Governor Jerry Brown." Freiwald, *supra*, 131 n. d1.
Professor Freiwald's account is thus more than an academic treatment of the subject: it is reliable "indicia of legislative intent." *Highland Ranch v. Agric. Labor Relations Bd.* (1981) 29 Cal.3d 848, 860 (relying on a law review article written by a law professor who assisted in drafting statute).

"fishing expeditions that violate the spirit, if not the letter, of the Fourth Amendment." Freiwald, *supra*, at 154. In furtherance of CalECPA's goals, the law requires state agencies to report electronic search warrants on an annual basis to the state Department of Justice. CalECPA §§ 1524.4 and 1546 (j). However, journalists have found huge and unexplainable discrepancies between the numbers of warrants that California agencies have reported publicly, and the number of warrants Google says it has received during that same time period.[48]

In addition to cabining wide-ranging searches of digital information, CalECPA's proponents had a special concern for the protection of location information. *See, e.g.*, Assem. Floor Analysis No. SB 178 at 5 (Ca. Sep. 4, 2015);[49] Freiwald, *supra*, at 140 ("location data [was] an area of great concern to CalECPA's proponents"). Prior to CalECPA, federal and state court decisions had left location data "ambiguously or completely unprotected." *Id*. CalECPA changed that reality with its robust warrant standard for compelled production of location information. *Id*.

---

[48] *See* Maddy Varner and Alfred Ng, *Thousands of Geofence Warrants Appear to Be Missing from a California DOJ Transparency Database*, The Markup (Nov. 3, 2021) https://themarkup.org/privacy/2021/11/03/thousands-of-geofence-warrants-appear-to-be-missing-from-a-california-doj-transparency-database (reporters "found only 41 warrants that could clearly constitute a geofence warrant"—a far cry from the 3,655 geofence warrant requests Google says it received during the same time period).

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

B. The Geofence Warrant Violates CalECPA's Particularity Requirements.

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

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

Instead of meeting CalECPA's requirement to specify the target individual or account, the geofence warrant included six locations of roughly a city block each, both residential and commercial, for a combined 300 plus minutes. The time period included the early to mid-morning hours of a weekday, when countless people are driving to work and passing through each location. And these locations included gas stations, a bank, a medical center, and stores, all locations where a large number of innocent individuals were likely to be and whose cell phone location data would have been swept up by the geofence warrant.

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

Thus, the geofence warrant in this case was neither appropriate nor reasonable as to the scope of potential individuals or accounts that were likely to be ensnared by the geofence warrant. To the contrary, given the size and the nature of the geofenced areas—which included sensitive locations full of innocent people who were not suspected to have any involvement in the crime under investigation—this deficiency was fatal to CalECPA's particularity requirement that the warrant is directed at "targeted individuals or accounts."

CONCLUSION

For the reasons stated above, this Court should reverse the lower court's decision denying Appellants' motion to suppress.

Respectfully submitted,

Dated: January 24, 2023 /s/ *Jennifer Lynch*

*Jennifer Lynch (SBN 240701)
**Counsel of Record*
Andrew Crocker (SBN 291596)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333
jlynch@eff.org
andrew@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

I, counsel for amicus curiae, certify pursuant to California Rules of Court 8.204(c) that this Brief is proportionally spaced, has a typeface of 13 points or more, and contains 9,016 words, including footnotes and excluding the cover, the tables, the Certificate of Interested Entities or Persons, the signature block, and this certificate, which is fewer than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: January 24, 2023 */s/ Jennifer Lynch*
Jennifer Lynch

CERTIFICATE OF SERVICE

I, Madeleine Mulkern, declare,

I am a resident of the state of California and over the age of eighteen years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109.

On January 24, 2023, I served the foregoing document:

AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANTS-APPLELLANTS

on the interested parties in this action as stated in the service list below:

☒ BY TRUEFILING: I caused to be electronically filed the foregoing document with the court using the court's e-filing system. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website:

Michael C. Keller
Office of the Attorney General
300 S. Spring St., Suite 1702
Los Angeles, CA 90013

Counsel for Plaintiff and Respondent the People of California

Sharon Fleming
Attorney At Law
P O Box 803
Ben Lomond, CA 95005-0803

Counsel for Defendant-Appellant Daniel Meza

Bess Louise Stiffelman
505 S. Flower Street #71892
Los Angeles, CA 90071

Counsel for Defendant-Appellant Walter Meneses

☒ BY EMAIL: I served the attached document by transmitting a true copy via electronic mail using my e-mail address as madeleine@eff.org to:

California Appellate Project
CapDocs@lacap.com

Counsel for Defendants-Appellants

☒ BY FIRST CLASS MAIL: I placed a true copy thereof enclosed in a sealed envelope with postage fully prepaid for collection and mailing following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is place for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service.

Hon. Laura R. Walton, Judge
c/o Clerk of Court
Clara Shortridge Foltz Criminal Justice Center
210 West Temple Street
Los Angeles, CA 90012

I declare under penalty of perjury under the laws of California that the foregoing is true and correct. Executed this 24th day January 2023, at San Francisco, California.

Madeleine Mulkern