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

Attorneys for Electronic Frontier Foundation

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

PEOPLE OF THE STATE OF CALIFORNIA

Plaintiff,

vs.

LAQUAN DAWES,

Defendant.

Case No.: 19002022

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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

CONSTITUTIONAL PROVISIONS

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

I. INTRODUCTION

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

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

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

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

II. BACKGROUND

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

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

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

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

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

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

(footnote continued on following page)

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

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

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

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

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

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

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

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

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

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

---

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

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

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

(footnote continued on following page)

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

III. ARGUMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

(footnote continued on following page)

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

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

B. The Geofence Warrant Violates CalECPA.

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

---

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

II. CONCLUSION

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

Respectfully submitted,

Dated: June 10, 2020

By_____
Jennifer Lynch

Attorney for Amicus Curiae Electronic Frontier Foundation

PROOF OF SERVICE

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

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

Application to File Brief of Amicus Curiae Electronic Frontier Foundation

Brief of Amicus Curiae Electronic Frontier Foundation

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

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

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

Attorneys for Laquan Dawes

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

Attorneys for the State of California

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

Madeleine Mulkern