2023 WL 5287224
Only the Westlaw citation is currently available.
Court of Appeal, Second District, Division 7, California.

The PEOPLE, Plaintiff and Respondent,
v.
Daniel MEZA et al., Defendants and Appellants.

B318310
|
Filed April 13, 2023

Synopsis

Background: After their motions to suppress evidence found pursuant to geofence search warrant were denied, defendant pleaded guilty to first degree murder and co-defendant pleaded no contest to second degree murder before the Superior Court, Los Angeles County, No. TA150314, Tammy Chung Ryu and Laura Walton, JJ. Defendant and co-defendant appealed.

Holdings: The Court of Appeal, Perluss, P.J., held that:

[1] magistrate reasonably concluded probable cause generally existed to support warrant;

[2] warrant sufficiently described place to be searched and items to be retrieved;

[3] warrant lacked particularity as to officers' discretion to filter initial search results;

[4] warrant was overbroad with respect to geographic boundaries of geofence searches;

[5] warrant was overbroad with respect to temporal boundaries of geofence searches;

[6] at time of search, reasonable officers would not have known of warrant's constitutional infirmities, for purposes of good faith exception to exclusionary rule; and

[7] warrant did not violate California Electronic Communications Privacy Act of 2016 (CalECPA).

Affirmed.

Lui, P.J., filed dissenting statement which Evans, J., joined.

Procedural Posture(s): Appellate Review; Pre-Trial Hearing Motion.

West Headnotes (35)

[1] Criminal Law State or federal law
Criminal Law Search or seizure in general

Notwithstanding the separate warrant requirement in the California Constitution, pursuant to the California Constitution's Truth-in-Evidence provision, evidence sought to be introduced at a criminal trial is generally subject to suppression as the fruit of an unconstitutional search and seizure only if exclusion is mandated by the federal exclusionary rule applicable to evidence seized in violation of the Fourth Amendment of the United States Constitution. U.S. Const. Amend. 4; Cal. Const. art. 1, §§ 13, 28(f)(2).

[2] Searches and Seizures Necessity of and preference for warrant, and exceptions in general

A search is presumptively reasonable, and thus in compliance with the Fourth Amendment, if supported by a warrant describing with particularity the thing or place to be searched. U.S. Const. Amend. 4.

[3] Searches and Seizures Particularity or generality and overbreadth in general

The manifest purpose of the Fourth Amendment's particularity requirement for warrants is to prevent general searches; by limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Constitution's Framers intended to prohibit. U.S. Const. Amend. 4.

[4] **Searches and Seizures** Probable or Reasonable Cause

Searches and Seizures Particularity or generality and overbreadth in general

In determining the validity of a warrant, courts examine three main factors: probable cause, particularity and overbreadth. U.S. Const. Amend. 4.

[5] **Searches and Seizures** Expectation of privacy

No search warrant is required if an individual has no reasonable expectation of privacy in the place or thing searched. U.S. Const. Amend. 4.

[6] **Searches and Seizures** Probable or Reasonable Cause

Probable cause will be found to support the issuance of a search warrant if the magistrate had a substantial basis for concluding a fair probability existed that a search would uncover wrongdoing. U.S. Const. Amend. 4.

[7] **Searches and Seizures** Particularity or generality and overbreadth in general

"Particularity" is the requirement that a search warrant must clearly state what is sought. U.S. Const. Amend. 4.

[8] **Searches and Seizures** Places, objects, or persons to be searched

To satisfy the particularity requirement for a search warrant, complete precision in describing the place to be searched is not required; it is enough if the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended. U.S. Const. Amend. 4.

[9] **Searches and Seizures** Particularity or generality and overbreadth in general

Breadth, as a factor in determining the validity of a search warrant, deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based. U.S. Const. Amend. 4.

[10] **Searches and Seizures** Particularity or generality and overbreadth in general

The breadth requirement for the validity of a search warrant is distinct from the particularity requirement because it prevents the magistrate from making a mistaken authorization to search for particular objects in the first instance, no matter how well the objects are described. U.S. Const. Amend. 4.

[11] **Criminal Law** Evidence wrongfully obtained

In reviewing a trial court's suppression ruling, the Court of Appeal defers to its factual findings if supported by substantial evidence. U.S. Const. Amend. 4.

[12] **Criminal Law** Illegally obtained evidence

In reviewing a trial court's ruling on a motion to suppress, the Court of Appeal independently assesses the legal question of whether the challenged search or seizure satisfies the Fourth Amendment. U.S. Const. Amend. 4.

[13] **Searches and Seizures** Probable or Reasonable Cause

The probable cause requirement for a warrant does not require conclusive evidence that a search will uncover relevant evidence, only that there is a fair probability that contraband or evidence of a crime will be found in a particular place; sufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment. U.S. Const. Amend. 4.

[14] **Searches and Seizures** Probable or Reasonable Cause

In determining whether probable cause supports the issuance of a search warrant, a magistrate may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the type of offense. U.S. Const. Amend. 4.

[15] **Searches and Seizures** Particular concrete applications

Magistrate reasonably concluded, when granting application for geofence search warrant, that perpetrators of murder were carrying cell phones on morning of murder and used them in coordinating their movements, and, thus warrant was generally supported by probable cause to believe search of cell phone location data would lead to identity of potential suspects or recovery of other evidence related to murder; detective who submitted affidavit in support of application opined based on his training and experience that criminal suspects used cell phones to coordinate criminal activity, perpetrators were suspected of moving to various locations in separate vehicles, and inference was reasonable in today's society. U.S. Const. Amend. 4.

[16] **Searches and Seizures** Objects or information sought

The purpose of the particularity requirement of the Fourth Amendment is to avoid general and exploratory searches by requiring a particular description of the items to be seized. U.S. Const. Amend. 4.

[17] **Searches and Seizures** Particularity or generality and overbreadth in general

A search warrant need only be reasonably specific, and the specificity required to satisfy the Fourth Amendment's particularity requirement varies depending on the circumstances of the case and the type of items involved. U.S. Const. Amend. 4.

[18] **Searches and Seizures** Objects or information sought

The particularity requirement of the Fourth Amendment is satisfied if the search warrant imposes a meaningful restriction upon the objects to be seized. U.S. Const. Amend. 4.

[19] **Searches and Seizures** Places, objects, or persons to be searched

Under the Fourth Amendment's particularity requirement, the description in a search warrant must be sufficiently definite that the officer conducting the search can, with reasonable effort, ascertain and identify the place intended; nothing should be left to the discretion of the officer. U.S. Const. Amend. 4.

[20] **Searches and Seizures** Objects or information sought

Searches and Seizures Places, objects, or persons to be searched

Geofence search warrant sufficiently described place to be searched and items to be retrieved from that search, as necessary to satisfy particularity requirement of Fourth Amendment, where warrant called for search of technology company's database of users' location history and specified items to be retrieved were designated records for users found within boundaries of certain coordinates at certain times corresponding to murder victim's movements on day of murder. U.S. Const. Amend. 4.

[21] **Searches and Seizures** Objects or information sought

In murder investigation, geofence search warrant, which authorized search of technology company's database of user location history and retrieval of designated records for users found near certain coordinates at certain

times, provided law enforcement with unbridled discretion regarding whether or how to narrow initial list of users identified by company, and thus warrant was insufficiently particular; after first step of search, law enforcement officials could enlarge geographic parameters of search and request additional information on any user identified without any objective limiting criteria, and at third step, officials could seek identifying information of any users found in search parameters without numerical restriction or showing that information on each user would be relevant. U.S. Const. Amend. 4.

[22] **Searches and Seizures** Objects or information sought

In determining whether a search warrant is overbroad, courts consider whether probable cause existed to seize all items of a category described in the warrant and whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued. U.S. Const. Amend. 4.

[23] **Searches and Seizures** Objects or information sought

Geofence search warrant seeking murder suspects' locations, which authorized search of technology company's database of user location history and retrieval of records for users found near six sets of coordinates at certain times, was overbroad in that it authorized identification of any individual within large search areas without particularized probable cause as to each person or their location; geographic boundaries of searches incorporated large surface areas where no evidence indicated murder suspects had entered, such as victim's apartment complex and surrounding buildings, permitting identification of individuals at home with no connection to murder, and size of search areas increased inclusion of individuals in warrant return who were merely near rather than in search boundaries. U.S. Const. Amend. 4.

[24] **Searches and Seizures** Objects or information sought

Law enforcement officials seeking murder suspects' locations did not draw geofence search boundaries as narrowly as possible given information available at time of warrant application, rendering warrant, which authorized search of technology company's database of user location history and retrieval of designated records for users in six search areas at certain times, impermissibly overbroad; for example, crime analyst who established search boundaries used center of victim's apartment complex as starting point for circle large enough to incorporate desired area, namely street outside complex, causing search area to include whole apartment complex and adjacent buildings, where suspects had not been, and using polygon boundaries would have reduced number of unrelated devices in search. U.S. Const. Amend. 4.

[25] **Searches and Seizures** Objects or information sought

Timeframes designated in warrant for geofence search, which sought murder suspects by authorizing search of technology company's database of user location history and retrieval of records for users found near six sets of coordinates for total of five hours, were not narrowly tailored, and thus warrant was overbroad; for example, warrant sought devices near victim's meeting with brother-in-law at gas station, but search ran from 90 minutes before meeting until end of meeting, nothing indicated victim or suspects were present before meeting, time of suspects' presence could be determined from surveillance footage, and many unrelated devices likely passed through area during extraneous 90-minute period, given setting of urban gas station during commuting hours. U.S. Const. Amend. 4.

[26] **Searches and Seizures** Objects or information sought

While it may be impossible to eliminate the inclusion of all uninvolved individuals in a geofence search warrant, it is the constitutionally imposed duty of the government to carefully tailor its search parameters to minimize infringement on the privacy rights of third parties. U.S. Const. Amend. 4.

[27] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Denial of a motion to suppress evidence found in a search must be upheld under the good faith exception to the exclusionary rule where the search has been conducted in objectively reasonable reliance on a subsequently invalidated search warrant. U.S. Const. Amend. 4.

[28] **Criminal Law** Presumptions and burden of proof

The government bears the burden to establish the applicability of the exception to the exclusionary rule where a search has been conducted in objectively reasonable reliance on a subsequently invalidated search warrant. U.S. Const. Amend. 4.

[29] **Criminal Law** Exceptions Relating to Defects in Warrant

In determining whether a search warrant was so facially deficient that the executing officers could not have reasonably presumed it to be valid, such that the good faith exception to the exclusionary rule does not apply, courts apply the objective test of whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization; this objective standard requires officers to have a reasonable knowledge of what the law prohibits. U.S. Const. Amend. 4.

[30] **Criminal Law** Particular cases

At time of execution of geofence search warrant, which sought murder suspects by authorizing search of technology company's database of user location history and retrieval of records for users found near six sets of coordinates at certain times, reasonable law enforcement officers would not have known that warrant was overbroad and insufficiently particularized, and thus under good faith exception to exclusionary rule, suppression of evidence found pursuant to search was not warranted; at time of warrant application and search, geofence warrants were novel investigative tool, warrant at issue was only third one prepared by official who drew search boundaries, who was not fully trained, and there were no published cases in United States on constitutionality of geofence warrants. U.S. Const. Amend. 4.

[31] **Criminal Law** Particular cases

In executing geofence search warrant, which sought murder suspects by authorizing search of technology company's database of user location history and retrieval of records for users found near six sets of coordinates for total of five hours, law enforcement officers did not knowingly exceed warrant's scope, and thus manner in which officers executed search did not preclude application of good faith exception to exclusionary rule on defendants' motion to suppress, even though company filtered search results before providing results to law enforcement instead of providing unfiltered results as called for in warrant; manner of execution narrowed search authorized by warrant, resulting in law enforcement receiving information about only eight devices instead of thousands. U.S. Const. Amend. 4.

[32] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Law enforcement officers may not rely on the good faith exception to the exclusionary rule when they have knowingly exceeded the scope of a search warrant. U.S. Const. Amend. 4.

[33] **Searches and Seizures** Objects or information sought

Failure of geofence search warrant, which sought murder suspects by authorizing search of technology company's database of user location history and retrieval of records for users found near six sets of coordinates at certain times, to specify name or other identifying information of targeted individuals did not violate requirement under California Electronic Communications Privacy Act of 2016 (CalECPA) that warrant describe with particularity the information to be seized "as appropriate and reasonable"; warrant described targets with greatest available degree of particularity, namely, individuals whose devices were within search boundaries at specified times, and CalECPA contemplated that warrant target might not be identifiable. Cal. Penal Code § 1546 et seq.

[34] **Searches and Seizures** Objects or information sought

Failure of geofence search warrant, which sought murder suspects by authorizing search of technology company's database of user location history and retrieval of records for users found near six sets of coordinates at certain times, to name particular application or service covered by warrant did not violate requirement under California Electronic Communications Privacy Act of 2016 (CalECPA) that warrant describe with particularity the information to be seized "as appropriate and reasonable"; government did not seek data or content related to any particular application or service, but, rather, sought service provider's record of all electronic content with each device within scope of geofence, regardless of which application or service originated such contact. Cal. Penal Code § 1546 et seq.

[35] **Searches and Seizures** Particular concrete applications

Geofence search warrant's overbreadth and lack of particularity in violation of Fourth Amendment, which law enforcement officers relied on in good faith, did not render warrant invalid under California Electronic Communications Privacy Act of 2016 (CalECPA), which required warrant to comply with federal law and granted standing to any person to seek suppression of electronic information obtained in violation of Fourth Amendment; CalECPA did not convert Fourth Amendment violation into independent statutory violation, but, rather, merely preserved an individual's existing rights under federal Constitution. U.S. Const. Amend. 4; Cal. Penal Code §§ 1546.1(d)(3), 1546.4(a).

APPEALS from judgments of the Superior Court of Los Angeles County, Tammy Chung Ryu, Judge, and Laura R. Walton, Judge. Affirmed. (Los Angeles County Super. Ct. No. TA150314)

Attorneys and Law Firms

Sharon Fleming, Ben Lomond, under appointment by the court of appeal, for Defendant and Appellant Daniel Meza.

Bess Stiffelman, under appointment by the court of appeal, for Defendant and Appellant Walter Meneses.

Rob Bonta, Attorney General, Lance E. Winters, Chief Assistant Attorney General, Susan Sullivan Pithey, Senior Assistant Attorney General, Wyatt E. Bloomfield and Michael C. Keller, Deputy Attorneys General, for Plaintiff and Respondent.

Jennifer Lynch and Andrew Crocker for Electronic Frontier Foundation as Amicus Curiae on behalf of Defendants and Appellants.

PERLUSS, P. J.

INTRODUCTION

***1** "A geofence is a virtual fence or perimeter around a physical location. Like a real fence, a geofence creates a separation between that location and the area around it.... [¶] It can be any size or shape, even a straight line between two points. [¶] Geofences are created using mapping software, which allow the user to draw the geofence over the desired geographic area. It is made up of a collection of coordinates

(i.e., latitude and longitude) or in the case of a circular geofence one point that forms the center." [1]

"Geofence warrants (sometimes called 'reverse location searches') are official requests by law enforcement authorities to access the device location data gathered by large tech companies like Google. The warrants specify a time and geographic area, and require the companies to turn over information on any devices that were in that area at that time. While this data is typically anonymized, it can be used in conjunction with other investigative techniques to tie devices to specific users—and identify persons of interest in a criminal investigation." [2]

"The government filed its first geofence search warrant in 2016, and by the end of 2019, Google was receiving about 180 search warrant requests per week from law enforcement officials across the country.... Between 2018 and 2020, Google received about 20,000 geofence warrant requests for data, including over 11,500 in 2020 alone." [3]

* * *

Daniel Meza and Walter Meneses were identified as suspects in the murder of Adbadalla Thabet after a geofence search warrant directed to Google revealed cell phones signed in to Google accounts connected to them were in several of the same locations as Thabet on the day of his murder. After their motions to quash and suppress evidence were denied, Meza pleaded guilty to first degree murder; and Meneses pleaded no contest to second degree murder.

On appeal Meza and Meneses contend the trial court erred in denying their motion to suppress, arguing the geofence warrant violated their rights under the Fourth and Fourteenth Amendments to the United States Constitution and did not comply with the California Electronic Communications Privacy Act of 2016 (Pen. Code, § 1546 et seq.) [4] (CalECPA). Although the geofence warrant satisfied the requirements of CalECPA, we agree it lacked the particularity required by the Fourth Amendment and was impermissibly overbroad. Nonetheless, we affirm Meza's and Meneses's convictions under the good faith exception to the exclusionary rule established by *United States v. Leon* (1984) 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (*Leon*).

FACTUAL AND PROCEDURAL BACKGROUND

1. *The Murder of Adbadalla Thabet and the Initial Investigation*

***2** According to surveillance footage viewed by police officers, at approximately 10:30 a.m. on March 1, 2019 Thabet drove into the parking lot of a bank in Paramount, followed by a gray sedan and a red sedan. [5] The driver of the red car parked, got out of his vehicle and walked to the gray car, where he stopped to speak to the driver of the gray car. The driver of the gray car then drove slowly toward Thabet's parked car. The driver of the red car followed on foot. As Thabet got out of his vehicle, the gray car pulled up next to Thabet's car; and an occupant of the gray car shot Thabet in the torso. Thabet fell to the ground as the gray car sped away. The driver of the red car approached Thabet, took his backpack, retreated to the red car and drove away. Thabet died from his injuries.

The investigating officers were able to retrace Thabet's steps from the morning of the shooting. They learned Thabet worked for his uncle's business, which included managing several gas stations. Twice per week Thabet picked up cash receipts from the gas stations and deposited the cash at the bank in Paramount. The day of the shooting Thabet left his apartment building in Downey around 7:00 a.m. and drove to a gas station in Downey to pick up cash for deposit. Thabet was at the Downey gas station from approximately 7:15 a.m. to 7:30 a.m. Thabet then met his brother-in-law at approximately 9:00 a.m. at a gas station in Bellflower. Thabet and his brother-in-law departed the gas station in separate cars at approximately 9:40 a.m. and drove to a strip mall in Compton where the brother-in-law was contemplating renting retail space. Thabet left the strip mall alone, driving to a gas station in Lynwood to pick up cash receipts. From Lynwood Thabet drove to the bank in Paramount where he was killed.

In addition to the video surveillance from the bank parking lot, investigators obtained video surveillance from other locations Thabet visited that morning. The gray and red vehicles from the bank surveillance footage were also identified in surveillance footage from at least two of those additional locations. Investigators concluded the suspects had been following Thabet, anticipating his arrival at the bank with the cash deposits. The license plate numbers of the gray and red vehicles were not legible in any of the footage.

2. *The Search Warrant Affidavit*

a. *Probable cause*

Los Angeles County Sheriff's Detective Jonathan Bailey applied for a search warrant directing Google to identify individuals whose location history data indicated they were in the vicinity of the six locations visited by Thabet on March 1, 2019. In an affidavit supporting the application, Bailey described Thabet's murder as seen on the surveillance footage of the bank parking lot. Bailey stated he had viewed surveillance camera footage from several of the other locations Thabet had visited that morning and had seen the gray and red sedans in the footage. Bailey did not state how many of the six locations had available surveillance footage, nor did he identify the locations at which the red and gray cars were visible.

The affidavit included a brief overview of how Google tracks and stores location history data, stating Google collected data through "Global Position System (GPS) data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points." Bailey stated, "I know most people in today's society possess cellular phones and other items (e.g. tablets, watches, laptops) used to communicate electronically.... Most people carry cellular phones on their person and will carry them whenever they leave their place of residence." In addition, Bailey explained, "Suspects involved in criminal activity will typically use cellular phones to communicate when multiple suspects are involved." Therefore, Bailey concluded, identification of individuals in Thabet's vicinity on the day of the murder would assist investigators in locating the drivers of the vehicles involved in the murder, who investigators believed had been following Thabet throughout the morning.

b. *Search parameters*

***3** The warrant application sought location history data for individuals within six target locations. The first location was Thabet's apartment, which was located in the middle of a large city block, surrounded by both residential and retail buildings. The area designated for the search was a circle with a radius of 100 meters from the center of the apartment complex (approximately seven and a half acres). It included the entire apartment building as well as portions of several surrounding buildings and approximately three-quarters of the street in front of the building. The timeframe for this search was 6:00 a.m. to 7:15 a.m. on March 1, 2019.

The second location was the gas station in Downey where Thabet picked up cash for deposit. The gas station is on the corner of a large intersection and is surrounded by other retail establishments. The search area consisted of a circle with a radius of 75 meters from the approximate center of the gas station (more than four acres). Included in the circle were the gas station, a restaurant and portions of other businesses, as well as the intersection in front of the gas station and the two main streets bordering the gas station. The timeframe for this search was 7:00 a.m. to 7:30 a.m. on March 1, 2019.

The third location was the gas station in Bellflower. The search area consisted of a circle with a radius of 50 meters from the approximate center of the gas station (almost two acres). Included in the circle were part of the intersection and approximately 50 meters of the streets bordering the gas station, as well as portions of the surrounding businesses. The timeframe for this search was 7:30 a.m. to 9:40 a.m.

The fourth location was the strip mall in Compton. The search area was a rectangle that included the strip mall, three streets bordering it and some neighboring buildings and parking lots (approximately one and one-half acres). The timeframe for this search was 9:40 a.m. to 10:15 a.m.

The fifth location was the gas station in Lynwood. The search area was a rectangle that included the gas station, neighboring buildings, including buildings across the street that appeared to be residences and the intersection bordering the gas station (approximately three acres). The timeframe for this search was 10:15 a.m. to 10:30 a.m.

The sixth and final location was the bank in Paramount where the murder took place. The search area was a circle with a radius of 75 meters from the center of the bank building (more than four acres). The search area included the bank and parking lot, neighboring businesses and parking lots, the intersection in front of the bank and approximately 50 meters of the streets bordering the bank.

c. *The warrant process*

The warrant set forth a three-step process by which Google would respond to the request for information. At step one, Google was directed to search location history data for the six

designated locations and times and produce an anonymized list of devices found within the search areas in the designated timeframes, including the individual times each device was recorded in the search area during the applicable time period.

At step two, law enforcement would review the anonymized list of devices "to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time." If law enforcement believed additional information was needed to determine whether a particular device was relevant to the investigation, law enforcement could request that Google provide additional location history information for that device even if that information fell outside of the initial geographic and temporal search parameters.

***4** At step three, law enforcement could demand identifying information from Google for all devices law enforcement deemed relevant to the investigation. The warrant directed Google to provide this identifying information without additional legal process.

3. *Execution of the Search Warrant and Charges Against Meza and Meneses*

A Los Angeles superior court judge, acting as magistrate, signed the geofence search warrant on March 21, 2019.

After reviewing the anonymized data provided by Google, the Sheriff's Department sought identifying information for eight devices that had been in the relevant locations on March 1, 2019. Google provided corresponding email addresses to law enforcement. The Sheriff's Department then drafted additional search warrants related to two of those email addresses, which eventually led to the identification of Meza and Meneses as suspects.

In an information filed December 4, 2020 Meza and Meneses were charged with murder (Pen. Code, § 187, subd. (a)) with three special circumstances—murder for financial gain (§ 190.2, subd. (a)(1)), murder by means of lying in wait (§ 190.2, subd. (a)(15)) and intentionally discharging a firearm with intent to inflict death (§ 190.2, subd. (a)(21)). It was specially alleged as to the murder charge that a principal was armed with a rifle within the meaning of section 12022, subdivision (a)(2). The information included special firearm-use enhancement allegations as to Meza (§ 12022.53, subds. (b), (c) and (d)). Meneses was also charged with two counts of possession of a firearm by a felon (§ 29800, subd. (a)(1)), possession of an assault weapon (§ 30605, subd. (a)) and unlawful possession of ammunition (§ 30305, subd. (a)(1)). Finally, the information specially alleged Meneses had suffered a prior serious felony conviction within the meaning of section 667, subdivision (a)(1).

4. *The Motion To Quash and Suppress*

On March 18, 2021 Meza moved pursuant to section 1538.5 to quash the geofence warrant and suppress all evidence seized as a result of the warrant, including evidence seized pursuant to subsequent warrants and statements made by witnesses and other individuals. Meneses joined the motion. The motion contended Detective Bailey's affidavit failed to establish probable cause and the geofence warrant lacked the particularity required by the Fourth Amendment. In a supplemental brief Meza and Meneses argued the geofence warrant did not comply with CalECPA because it did not adequately identify the target individuals or accounts and applications to be searched.

A hearing on the motion was held on April 12, 2021. Spencer McInvaille, an expert on geolocation and mobile devices, testified on behalf of Meza and Meneses. McInvaille's testimony was based on his training and experience, as well as his review of documents publicly filed by Google. [6]

***5** McInvaille explained Google's location data is derived from several sources: GPS, Bluetooth signals, cellular network data and the strength of nearby WiFi networks. [7] Google logs each device's location hundreds of times each day—as often as every two minutes according to some estimates. (See *United States v. Chatrie* (E.D.Va. 2022) 590 F.Supp.3d 901, 908 & fn. 10 (*Chatrie*).) However, Google cannot pinpoint a user's location with 100 percent accuracy. McInvaille stated the longitude and latitude recorded by Google as the device's location is "not a physical actual location of the device. It's just the estimate derived from the measurement that they took." Thus, Google also reports a confidence interval, measured in meters, that indicates Google's confidence in the location of the device. For example, a confidence interval of 15 meters indicates Google estimates the device is within a 15 meter radius of the given coordinates. The size of the confidence interval varies depending on the type of data from which the measurement was taken. Google aims to estimate a device's location with 68 percent accuracy—that is, there will be a 68 percent chance the user was actually within the circle created by the confidence interval. When responding to a geofence warrant, Google considers a device within the search parameter if the

estimated location is within the search boundaries even if the confidence interval extends beyond the search boundaries. Similarly, a device with an estimated location outside the search boundaries will not be included in the search results even if the confidence interval extends within the search boundaries.

Romy Haas, a crime analyst for the Sheriff's Department, testified for the prosecution regarding the application for and execution of the geofence warrant in this case. Haas explained she typically consults with detectives prior to drafting a geofence warrant application and assists in establishing the geographic parameters and timeframes of the requested warrant. She had participated in drafting and processing returns on more than 50 geofence warrants by the time of the motion to suppress hearing in 2021, but at the time she assisted Detective Bailey with drafting the geofence warrant in this case in 2019 she had worked on only two other geofence warrants. Haas had participated in a number of trainings regarding location history data and geofence warrants, most of which took place after the warrant had been drafted in this case.

The court directly questioned Haas regarding how she and Detective Bailey decided on the search parameters for the warrant. For the first location (Thabet's apartment building), Haas testified the search radius of 100 meters from the center of the apartment building was selected so that it would capture the street in front of the building "in the event that [Thabet] was being watched before he left." Haas explained it was typical with early geofence warrants to draw a circle from a midpoint, but she noted a polygon "will help reduce the number of devices that will show up in the geofence."

For the second location, Haas testified the geofence perimeter was again drawn to capture the streets bordering the gas station "to see if ... someone had been coming down those streets or parked on those streets if the—if someone was watching the victim at that location." The perimeter for the third location was drawn to include the street on the north side of the gas station because there was surveillance video footage showing the suspect vehicles parked on that street. The perimeters for locations four and five were drawn as rectangles because Haas found using a circle captured too much area and would "encompass a bunch of devices that I didn't feel would be necessary because they were in the outer neighborhood." Instead, for location four she drew a rectangle that encompassed the area the victim visited inside the strip mall, and for location five the rectangle encompassed a parking lot across the street from the gas station where one of the suspect vehicles had been seen on surveillance video.

***6** Haas also testified regarding the warrant's three-step process for Google's production of data in response to the warrant. Haas explained the process was mandated by Google as the procedure that would most likely ensure Google's compliance with a geofence warrant. [8] However, the process was not strictly followed in this case. Rather than produce an anonymized list of users found within the six geofence perimeters at step one, a Google employee called Haas and told her the strip mall location had produced "voluminous results." Google requested Haas either shorten the timeframe or decrease the search area to reduce the number of responsive results. Haas testified she declined the request because "based on our careful consideration of the location and the timeframe involved, I didn't think that would be fair to the case to do that.... I in discussion explained to [the Google employee] really what I was looking for based on the facts of the case.... I said I was looking to find devices that were [in] at least two or more of the geofence locations." The Google representative responded she could filter the search and produce information for devices that were only in two or more of the specified locations at the applicable times. Haas agreed.

Google produced a list of eight anonymized accounts that had been at two or more of the six locations at the relevant time periods. Of the eight accounts, one had been at four of the geofence locations, one at three locations and the remaining six had been at two locations. Haas requested, and Google produced, identification information for all eight accounts. Two of those accounts (the ones that had been at three and four of the locations) ultimately led authorities to Meza and Meneses.

5. *The Superior Court's Denial of the Motions To Suppress*

The superior court found there was sufficient probable cause to support issuance of the geofence warrant. The fact that the two suspect cars were seen in multiple surveillance videos made it reasonably probable "that they were using their phones to communicate or to determine the location that they're going to." The court further found the warrant satisfied the particularity requirements of the United States Constitution and CalECPA. The court stated it was satisfied the boundaries of the search areas were based on the locations of the suspect vehicles as seen in the video footage and were not so broad as to unnecessarily include devices of uninvolved

bystanders. Finally, the court ruled, even if the warrant had been defective, the officers were entitled to rely on it under the good faith exception of *United States v. Leon* (1984) 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (*Leon*). Accordingly, the court denied the motions to suppress.

6. *The Pleas and Sentences*

Following denial of the motions to suppress evidence, Meza pleaded guilty to first degree murder and Meneses pleaded no contest to second degree murder. Pursuant to negotiated agreements the special circumstances and special allegations were stricken, and the remaining counts as to Meneses were dismissed. Meza was sentenced to an indeterminate state prison term of 25 years to life. Meneses was sentenced to an indeterminate state prison term of 15 years to life.

DISCUSSION

1. *The Geofence Warrant Violated the Fourth Amendment*

a. *Governing Law and Standard of Review*

[1] The Fourth Amendment to the United States Constitution, applicable to the States by the Fourteenth Amendment, prohibits unreasonable searches and seizures and guarantees that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const., 4th Amend.; see *People v. Robinson* (2010) 47 Cal.4th 1104, 1131, 104 Cal.Rptr.3d 727, 224 P.3d 55; *People v. Camacho* (2000) 23 Cal.4th 824, 830-831, 98 Cal.Rptr.2d 232, 3 P.3d 878.) [9]

***7 [2] [3]** A search is presumptively reasonable, and thus in compliance with the Fourth Amendment, if supported by a warrant describing with particularity the thing or the place to be searched. (See *People v. Weiss* (1999) 20 Cal.4th 1073, 1082, 86 Cal.Rptr.2d 337, 978 P.2d 1257.) " 'The manifest purpose of this particularity requirement [is] to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.' " (*People v. Amador* (2000) 24 Cal.4th 387, 392, 100 Cal.Rptr.2d 617, 9 P.3d 993; accord, *Maryland v. Garrison* (1987) 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72.)

[4] [5] [6] Accordingly, in determining the validity of a warrant, courts examine three main factors: probable cause, particularity and overbreadth. [10] Probable cause will be found to support the issuance of a warrant if " 'the magistrate had a substantial basis for concluding a fair probability existed that a search would uncover wrongdoing.' " (*People v. Westerfield* (2019) 6 Cal.5th 632, 659-660, 243 Cal.Rptr.3d 18, 433 P.3d 914; accord, *People v. Miles* (2020) 9 Cal.5th 513, 576, 263 Cal.Rptr.3d 144, 464 P.3d 611; *People v. Kraft* (2000) 23 Cal.4th 978, 1040-1041, 99 Cal.Rptr.2d 1, 5 P.3d 68; see *Illinois v. Gates* (1983) 462 U.S. 213, 238-239, 103 S.Ct. 2317, 76 L.Ed.2d 527 (*Gates*).)

[7] [8] "Particularity is the requirement that the warrant must clearly state what is sought." (*In re Grand Jury Subpoenas Dated Dec. 10, 1987* (9th Cir. 1991) 926 F.2d 847, 856.) To satisfy this requirement, "[c]omplete precision in describing the place to be searched is not required." (*People v. Amador, supra*, 24 Cal.4th at p. 392, 100 Cal.Rptr.2d 617, 9 P.3d 993; accord, *People v. Minder* (1996) 46 Cal.App.4th 1784, 1788, 54 Cal.Rptr.2d 555.) " 'It is enough if the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended.' " (*Amador*, at p. 392, 100 Cal.Rptr.2d 617, 9 P.3d 993; accord, *Steele v. United States* (1925) 267 U.S. 498, 503, 45 S.Ct. 414, 69 L.Ed. 757.)

[9] [10] "Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." (*In re Grand Jury Subpoenas Dated Dec. 10, 1987, supra*, 926 F.2d at pp. 856-857.) This is distinct from the particularity requirement because it "prevents the magistrate from making a mistaken authorization to search for particular objects in the first instance, no matter how well the objects are described." (*United States v. Weber* (9th Cir. 1990) 923 F.2d 1338, 1342 [although rules regarding particularity and overbreadth "serve the same ultimate purpose, they achieve the purpose in distinct ways"]; see also *United States v. Purcell* (2d Cir. 2020) 967 F.3d 159, 179 ["A warrant that comports with the particularity requirements may, however, be defective due to overbreadth. '[B]readth and particularity are related but distinct concepts' "].)

***8 [11] [12]** "In reviewing the trial court's suppression ruling, we defer to its factual findings if supported by substantial evidence. We independently assess the legal

question of whether the challenged search or seizure satisfies the Fourth Amendment." (*People v. Brown* (2015) 61 Cal.4th 968, 975, 190 Cal.Rptr.3d 583, 353 P.3d 305; accord, *People v. Eubanks* (2011) 53 Cal.4th 110, 133, 134 Cal.Rptr.3d 795, 266 P.3d 301.)

b. *The Search Warrant Was Supported by Probable Cause*

Meza and Meneses contend Detective Bailey's assertion of probable cause in his affidavit was insufficient because "[t]here was absolutely no evidence that either suspect had, or was using, a phone or other device at any time during the relevant timeframe." Accordingly, they argue, there was no basis for determining that searching cell phone location history would lead to the identity of potential suspects or the recovery of other evidence related to the murder.

[13] **[14]** Probable cause does not require conclusive evidence that a search will uncover relevant evidence, only that " 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.' " (*People v. Kraft, supra*, 23 Cal.4th at p. 1041, 99 Cal.Rptr.2d 1, 5 P.3d 68; accord, *Gates, supra*, 462 U.S. at p. 238, 103 S.Ct. 2317.) " ' "[S]ufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment." ' " (*People v. Beck and Cruz* (2019) 8 Cal.5th 548, 592, 256 Cal.Rptr.3d 1, 453 P.3d 1038; see also *People v. Carrington* (2009) 47 Cal.4th 145, 163, 97 Cal.Rptr.3d 117, 211 P.3d 617 ["[t]he showing required in order to establish probable cause is less than a preponderance of the evidence or even a prima facie case"].) In making this determination a magistrate may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the type of offense. (See *Gates,* at p. 240, 103 S.Ct. 2317; *People v. Sandlin* (1991) 230 Cal.App.3d 1310, 1315, 281 Cal.Rptr. 702.)

[15] It was reasonable for the magistrate to conclude the perpetrators were carrying cell phones the morning of the murder and used them in coordinating their movements. Not only did Detective Bailey opine, based on his training and experience, that criminal suspects use cell phones to coordinate criminal activity, but also such an inference was reasonable in today's society, especially given the suspected movement of the individuals to various locations in separate vehicles. (See *Riley v. California* (2014) 573 U.S. 373, 385, 401, 134 S.Ct. 2473, 189 L.Ed.2d 430 [cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy"; "[c]ell phones have become important tools in facilitating coordination and communication among members of criminal enterprises"]; *United States v. James* (8th Cir. 2021) 3 F.4th 1102, 1105 [finding probable cause supported warrant for cell phone records "[e]ven if nobody knew for sure whether the robber *actually* possessed a cell phone, the judges were not required to check their common sense at the door and ignore the fact that most people 'compulsively carry cell phones with them all the time' "].)

c. *The Search Warrant Lacked Sufficient Particularity*

[16] **[17]** **[18]** **[19]** As discussed, the "purpose of the 'particularity' requirement of the Fourth Amendment is to avoid general and exploratory searches by requiring a particular description of the items to be seized." (*People v. Bradford* (1997) 15 Cal.4th 1229, 1296, 65 Cal.Rptr.2d 145, 939 P.2d 259.) "However, a warrant 'need only be reasonably specific' [citation], and the 'specificity required "varies depending on the circumstances of the case and the type of items involved." ' " (*People v. Robinson, supra,* 47 Cal.4th at p. 1132, 104 Cal.Rptr.3d 727, 224 P.3d 55 ["particularity 'is a flexible concept, reflecting the degree of detail available from the facts known to the affiant and presented to the issuing magistrate' "].) " '[T]his requirement is held to be satisfied if the warrant imposes a meaningful restriction upon the objects to be seized.' " (*People v. Frank* (1985) 38 Cal.3d 711, 724, 214 Cal.Rptr. 801, 700 P.2d 415.) In other words, "[t]he description in a search warrant must be sufficiently definite that the officer conducting the search 'can, with reasonable effort ascertain and identify the place intended.' [Citation.] Nothing should be left to the discretion of the officer." (*People v. Dumas* (1973) 9 Cal.3d 871, 880, 109 Cal.Rptr. 304, 512 P.2d 1208; see also *United States v. Blakeney* (4th Cir. 2020) 949 F.3d 851, 863 [warrants met particularity requirement where they "describe the items to be seized with enough particularity to constrain the discretion of the executing officers and prevent a general search"]; *United States v. Collins* (9th Cir. 1987) 830 F.2d 145, 145-146 [warrant not sufficiently particular where it contained an incorrect address and imprecise description, resulting in search of the wrong house].)

***9** **[20]** The warrant in this case sufficiently described the place to be searched (Google's database of users' location history) and the items to be retrieved from that search

(designated records for users found within the boundaries of certain coordinates at certain times). Indeed, Mesa and Meneses do not argue there was any ambiguity in the warrant that would lead law enforcement or Google personnel to search an incorrect database or to identify individuals not contemplated by the text of the warrant.

[21] However, the warrant here failed to meet the particularity requirement because it provided law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users identified by Google. Once the step one search had been conducted, law enforcement officials were able to enlarge the geographic parameters of the search and request additional information on any of the potentially thousands of users identified without any objective criteria limiting their discretion. Again, at step three law enforcement could seek identifying information of any of the users found within the search parameters without restriction on how many users could be identified or any further showing that information concerning each individual user would be relevant to the case.

This failure to place any meaningful restriction on the discretion of law enforcement officers to determine which accounts would be subject to further scrutiny or deanonymization renders the warrant invalid. (See *Chatrie, supra,* 590 F.Supp.3d at p. 934 [geofence warrant lacks requisite particularity because "Steps 2 and 3 of this warrant leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users"]; *In re Search of: Info. Stored at Premises Controlled by Google* (N.D.Ill. 2020) 481 F.Supp.3d 730, 754 (*In re Google N.D.Ill*) [denying geofence warrant application because "the warrant puts no limit on the government's discretion to select the device IDs from which it may then derive identifying information from among the anonymized list of Google-connected devices that traversed the geofences"]; *In re Search of Info. Stored at the Premises Controlled by Google* (Va.Cir.Ct., Feb. 24, 2022, KM-2022-79) 2022 WL 584326, at p. *9, 2022 Va.Cir. Lexis 12, at pp. *24-*25 [denying geofence warrant application that allowed police to "unilaterally ... enlarge the Court-authorized search zone" and "unilaterally tell Google which cell phones it wants to unmask to obtain the owner's personal information"].) [11]

d. *The Search Warrant Was Overbroad*

[22] In determining whether a warrant is overbroad courts consider "whether probable cause existed to seize all items of a category described in the warrant" and "whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued." (*United States v. Shi* (9th Cir. 2008) 525 F.3d 709, 731-732; see also *People v. Hepner* (1994) 21 Cal.App.4th 761, 778, 26 Cal.Rptr.2d 417 ["overbreadth also hinges on whether a more precise description [of the items to be seized] was reasonably possible"]; *People v. MacAvoy* (1984) 162 Cal.App.3d 746, 754-755, 209 Cal.Rptr. 34 ["[o]n its face, the warrant would allow the officers to search every part of the fraternity house; since probable cause existed to search appellant's room only, the warrant, as a general rule, is void"]; *Owens v. Lott* (4th Cir. 2004) 372 F.3d 267, 276 [warrant authorizing search of "all persons" at certain location was valid "if the affidavit and information provided to the magistrate supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity"]; *In re Grand Jury Subpoenas Dated Dec. 10, 1987, supra*, 926 F.2d at p. 857 ["the concept of breadth may be defined as the requirement that there be probable cause to seize the particular thing named in the warrant"].)

***10 [23]** The geofence warrant in this case ran afoul of both of these requirements. First, the warrant authorized the identification of any individual within six large search areas without any particularized probable cause as to each person or their location. For example, the first search location, the area around Thabet's apartment complex, allowed law enforcement to obtain information on every individual in a seven-and-a-half-acre area over a 75 minute period in the early morning. The search area included Thabet's entire apartment complex and surrounding buildings despite the lack of any evidence (or supported inference) that the suspects left their vehicles, let alone entered the apartment building. Given the early morning timeframe for the search, the warrant permitted identification of numerous individuals with no connection to the murder who were simply still at home. Indeed, for many of the search locations, the geographic boundaries incorporated more surface area where the suspects were not believed to have been present (inside buildings) than area where they were (adjacent roads and intersections). This overbreadth is even more pernicious given that individuals (especially those near the perimeters of the search area) would be included in the warrant return despite an estimated 32 percent chance they were actually not within the search parameter at all.

[24] Second, law enforcement officials failed to draw the search boundaries as narrowly as they could have given the information available. For the first location Haas explained her goal was to capture the street in front of the apartment complex. Rather than draw a shape that would include only that targeted area, Haas used the center of the apartment building as a starting point for a circle large enough to incorporate the desired area. Haas implicitly conceded this method resulted in an overbroad search and no longer constituted best practices, explaining, "I feel that sometimes a polygon shape will help reduce the number of devices that will show up in the geofence. But a lot of circles in this type of shape [were] being used in the beginning to indicate the actual geofence."

[25] The timeframes designated in the geofence warrant were also not narrowly tailored. The most striking example of this overbreadth was with location three, the Bellflower gas station where Thabet met his brother-in-law. According to preliminary hearing testimony, Thabet's brother-in-law told police he met Thabet at the gas station at approximately 9:00 a.m. and they left at approximately 9:40 a.m. The warrant, however, directed Google to search the location for any devices present between 7:30 a.m. and 9:40 a.m. Even allowing for some uncertainty, there is no evidence Thabet or the suspects were at the gas station 90 minutes before the time that the brother-in-law recalled arriving. Given this was a gas station in a metropolitan area during normal commuting hours, there were likely many devices travelling through the search area during that 90 minutes that were entirely unrelated to Thabet's murder.

Haas's testimony there was surveillance footage from the Bellflower location showing one or both suspect cars parked on the street near the gas station constituted further evidence of the failure to narrow the parameters. The Sheriff's Department presumably could have determined a far shorter time period during which the suspects were present based on a timestamp in the surveillance footage, but they failed to narrow the search accordingly. In fact, the evidence presented to the magistrate was devoid of any detail regarding the surveillance footage that would have supported a finding of probable cause for the particular search areas and times. Detective Bailey's affidavit stated only that surveillance footage was available at "several locations" without identifying which locations had surveillance footage and which footage showed the suspects' vehicles, let alone the precise location and time the suspects' vehicles were seen. This information should have been used to more narrowly focus the search parameters.

[26] The failure to sufficiently narrow the search parameters potentially allowed a location-specific identification of thousands of individuals—likely a search within the ambit of the Fourth Amendment [12] — for whom no probable cause existed. While we recognize it may be impossible to eliminate the inclusion of all uninvolved individuals in a geofence warrant, it is the constitutionally imposed duty of the government to carefully tailor its search parameters to minimize infringement on the privacy rights of third parties. (See *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation* (N.D.Ill. 2020) 497 F.Supp.3d 345, 362 (*In re Arson Investigation*) ["[I]t is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are impacted. Similarly, in the geofence context, there is no way to exclude the possibility that at any given time a delivery truck may drop off a parcel within the geofence location. The proper line of inquiry is not whether a search of location data could impact even one uninvolved person's privacy interest, but rather the reasonableness of the search, the probability of finding evidence at the location, and the particularity of the search request"]; *In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc.* (D.D.C. 2013) 21 F.Supp.3d 1, 7 [rejecting "overly broad search and seizure warrant application directed to Facebook, at least in part because it unduly invaded the privacy of third parties"].) The warrant here, authorizing the search of more than 20 acres total over a cumulative period of more than five hours in residential and commercial areas did not meet this fundamental threshold requirement.

***11** Other cases that have considered the validity of geofence warrants have also, almost uniformly, determined that such warrants are valid only if they are narrowly tailored to avoid unnecessary infringement on the privacy of uninvolved third parties. For example, in *Chatrie* a geofence warrant was issued directing Google to search a 17.5-acre area surrounding a bank where a robbery had occurred. The timeframe was for approximately 30 minutes prior to the robbery and 30 minutes after the robbery—a total of one hour. The district court noted the search area included a church and the search identified individuals "who may not have been *remotely* close enough to the Bank to participate in or witness the robbery." (*Chatrie, supra*, 590 F.Supp.3d at p. 930.) The court found the warrant was overbroad

because it failed to "include any facts to establish probable cause to collect such broad and intrusive data" from each individual within the search area. (*Id.*, at p. 929; [13] see also *In re Search of Information That Is Stored at the Premises Controlled by Google, LLC* (D.Kan. 2021) 542 F.Supp.3d 1153, 1158 (*In re Google D.Kan.*) [denying geofence warrant application because search area included two public streets and an uninvolved business with no explanation as to why suspects might be found in those locations and contained no justification for the time period requested]; *In re Google N.D.Ill, supra*, 481 F.Supp.3d at p. 757 [denying geofence warrant application because search area included unrelated business, public street, residential units and parking lot during 90 minute period despite no showing all individuals in those locations were involved in the offense].)

An example at the other end of the spectrum is *In re Google D.D.C., supra*, 579 F.Supp.3d 62. In that case, police were investigating criminal activity at a business located in an industrial area. Police obtained surveillance footage from inside the business showing the suspects engaging in criminal activity. Based on the precise locations of the suspects and the times depicted in the footage, police designated a geofence area of less than a quarter of an acre, including the front-half of the business and the parking lot but excluding another business in the building and the road bordering the building. The time period in the warrant totaled 185 minutes in increments of two to 27 minutes on 8 different days based on when police knew the suspects had been present. The warrant affidavit also explained that, during the designated time periods, the suspects were either alone inside the business or were in the proximity of " 'on average' no more than 2 or 3 others." (*Id.* at p. 73.) The magistrate judge granted the warrant application, finding the government had "appropriately contoured the temporal and geographic windows in which it is seeking location data" and the warrant did not "have the potential of sweeping up the location data of a substantial number of uninvolved persons." (*Id.* at pp. 80 & 85; see also *In re Arson Investigation, supra*, 497 F.Supp.3d at p. 353 [granting geofence warrant application where search area excluded residences and commercial buildings, time periods sought were approximately 15 to 30 minutes per location and there was evidence premises in search areas were unoccupied during relevant time periods; "the government has structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses"]; *United States v. Rhine* (D.D.C. Jan. 24, 2023, No. 21-0687) —— F.Supp.3d ——, ——, 2023 WL 372044, at pp. *16–17, 2023 U.S.Dist. Lexis 12308, at pp. *95-*103 [denying motion to suppress where geofence warrant had sought identification of individuals in the United States Capitol Building over a four and a half hour period on January 6, 2021; court found warrant was narrowly tailored to include individuals improperly inside the Capitol given that the building was closed to the public and the search area excluded nearby grounds, did not include any commercial businesses or residences and there had been substantial road closures during the relevant time period].)

2. *The Officers Reasonably Relied on the Geofence Warrant in Good Faith*

[27] **[28]** "In *Leon*, the [United States] Supreme Court held that when 'an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope,' the 'marginal or nonexistent benefits' produced by suppressing the evidence obtained 'cannot justify the substantial costs of exclusion.' " (*People v. Lazarus* (2015) 238 Cal.App.4th 734, 766, 190 Cal.Rptr.3d 195, quoting *Leon, supra,* 468 U.S. at pp. 920-922, 104 S.Ct. 3405.) Accordingly, denial of the motion to suppress must be upheld under the "good faith" exception to the exclusionary rule where a search has been conducted "in objectively reasonable reliance on a subsequently invalidated search warrant." (*Leon*, at p. 922, 104 S.Ct. 3405.) *Leon* set forth four scenarios in which such objectively reasonable reliance should not be found and suppression remained the appropriate remedy: (1) "[T[he magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) if "the issuing magistrate wholly abandoned his [or her] judicial role"; (3) the affidavit is " 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable' "; or (4) if the warrant was "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." (*Id.* at p. 923, 104 S.Ct. 3405.) The government bears the burden to establish applicability of the good faith exception. (*People v. Willis* (2002) 28 Cal.4th 22, 36-37, 120 Cal.Rptr.2d 105, 46 P.3d 898.)

***12** Meza and Meneses argue both the third and fourth *Leon* scenarios—a total lack of probable cause and an obvious failure to satisfy the requirement of particularity—apply here. As discussed, probable cause supported issuance of the warrant. This factor does not preclude application of the good faith exception.

[29] In determining whether the warrant was so facially deficient that the executing officers could not have reasonably presumed it to be valid, "we apply the objective test of 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.' " (*People v. Hochanadel* (2009) 176 Cal.App.4th 997, 1015, 98 Cal.Rptr.3d 347; see also *People v. Camarella* (1991) 54 Cal.3d 592, 605, 286 Cal.Rptr. 780, 818 P.2d 63.) "This objective standard 'requires officers to have a reasonable knowledge of what the law prohibits.' " (*People v. Gotfried* (2003) 107 Cal.App.4th 254, 265, 131 Cal.Rptr.2d 840.)

[30] That standard was not met here. At the time law enforcement officers sought and executed the search warrant, geofence warrants were still a novel investigative tool. The warrant was only the third prepared by Haas, and she had not yet had much of the training on the practice that she would eventually receive. In early 2019 when this warrant was drafted and executed, there were no published cases anywhere in the country, let alone in California, analyzing the constitutionality of geofence warrants. (See *Chatrie, supra,* 590 F.Supp.3d at p. 938 [when warrant was obtained in June 2019, "no court had yet ruled on the legality" of geofence warrants]; *In re Search of: Information Stored at Premises Controlled by Google* (N.D.Ill. July 8, 2020, No. 20 M 297), 2020 WL 5491763 at p. *4, 2020 U.S.Dist. Lexis 165185 at p. *9 [noting no controlling authority addressing constitutional validity of geofence warrants].) Furthermore, as the preceding analysis demonstrates, "the permissibility of geofence warrants is a complex topic, requiring a detailed, nuanced understanding and application of Fourth Amendment principles." (*Chatrie,* at p. 938.)

[31] **[32]** Meza and Meneses argue the good faith exception should not apply here because, instead of following the three steps described in the warrant, "Haas and Bailey disregarded the express terms set forth in the warrant, and essentially fashioned their own search warrant." While officers may not rely on the good faith exception when they have knowingly exceeded the scope of a warrant (see *Leon, supra*, 468 U.S. at p. 918, fn. 19, 104 S.Ct. 3405 [the good faith exception "assumes, of course, that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant"]; see also *People v. Nguyen* (2017) 12 Cal.App.5th 574, 586-587, 219 Cal.Rptr.3d 124), the manner of execution in this case (Google's filtering of the results at step one) narrowed, not expanded, the search authorized by the warrant. Rather than receiving a list of many thousands of anonymized devices from Google that could then be filtered and matched, law enforcement received only information about eight specific devices—as if only two rooms of a house were searched pursuant to a warrant that authorized searching the entire property.

Given the dearth of authority directly on point and the novelty of the particular surveillance technique at issue, the officers were not objectively unreasonable in believing the warrant was valid, even if the issue, upon close legal examination, is not a particularly close one. (See *People v. Rowland* (2022) 82 Cal.App.5th 1099, 1124, 299 Cal.Rptr.3d 206 [applying good faith exception where no California precedent existed on the issue]; *People v. Pressey* (2002) 102 Cal.App.4th 1178, 1191, 126 Cal.Rptr.2d 162 [same]; see also *United States v. Smith* (N.D.Miss. Feb. 10, 2023, No. 3:21-cr-107-SA), 2023 WL 1930747, at pp. *8–*9, 2023 U.S.Dist. Lexis 22944, at pp. *37-*38 [applying good faith exception to geofence warrant given lack of legal authority on the issue]; *Chatrie, supra,* 590 F.Supp.3d at p. 938 [same].) [14]

3. *The Geofence Warrant Did Not Violate CalECPA*

***13** Effective January 1, 2016, CalECPA requires law enforcement officials to obtain a warrant in order to compel production of electronic communication information and electronic device information from a service provider. [15] (§ 1546.1, subd. (b).) Covered information includes "information stored on or generated through the operation of an electronic device, including the current and prior locations of the device." (§ 1546, subd. (g).) Any warrant issued pursuant to CalECPA "shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, ... the target individuals or accounts" and "the applications or services covered." (§ 1546.1, subd. (d)(1).) A party "may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter." (§ 1546.4, subd. (a).) [16]

[33] Meza and Meneses first argue the geofence warrant in this case violated CalECPA because it "fails to specifically target individuals or accounts. No individual's name was included in the warrant, nor was any specific cell phone number, email address, or account information." Their argument ignores the plain language of the statute, which provides that a warrant shall describe with particularity the

information to be seized "as appropriate and reasonable." (§ 1546.1, subd. (d)(1).) The warrant in this case described the target individuals and accounts with the greatest degree of particularity available to investigators—individuals whose devices were located within the search boundaries at certain times. There is no requirement in the statute that a suspect's name or other identifying information be included in the warrant to ensure its validity. In fact, CalECPA specifically contemplates a scenario where there is "no identified target of a warrant" and provides that, in such an instance, because notice of the warrant cannot be served upon any individual, the law enforcement agency seeking the warrant must notify the California Department of Justice. (§ 1546.2, subd. (c).) Accordingly, the failure to specify an individual's name or other identifying information did not render the warrant invalid under CalECPA.

[34] Meza and Meneses next argue the warrant violated CalECPA because it did not specify the "applications and services covered" by the warrant. CalECPA does not define "applications and services"; and Meza and Meneses have not explained what they believe it means, what particular information they contend should have been included in the warrant, or how the warrant was ambiguous absent such unspecified information. The common sense meaning of the statute appears to be that, when law enforcement seeks to recover the content of electronic communications, such as emails or text messages, the warrant must specify, as appropriate and reasonable, the particular mail or text message applications and services from which law enforcement seeks to retrieve information. With a geofence warrant, however, the government is not seeking data or content related to a particular application or service. Rather, what is sought is the service provider's record of all electronic contact with that device, regardless of which applications or services originated the contact. Accordingly, the failure to name a particular application or service in this instance does not result in a violation of CalECPA.

***14 [35]** Finally, Meza and Meneses argue any constitutional infirmities in the warrant create an independent violation of CalECPA. [17] Meza and Meneses do not explain precisely how a constitutional violation is also a statutory violation. However, it appears they rely on CalECPA's requirement that a warrant must comply with all "provisions of California and federal law" (§ 1546.1, subd. (d)(3)) and its grant of standing to "any person" to "move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter" (§ 1546.4, subd. (a)). Those provisions do nothing more than expressly preserve an individual's existing rights under the federal Constitution. There is nothing in the cited language that, without more, converts a Fourth Amendment violation into a statutory violation.

DISPOSITION

The judgments are affirmed.

We concur:

SEGAL, J.

FEUER, J.

Dissenting Statement by Justice Liu

The Electronic Communications Privacy Act (CalECPA; Pen. Code, § 1546 et seq.) governs law enforcement's ability to "compel the production of or access to electronic communication information from a service provider." (*Id.*, § 1546.1, subd. (b).) "Any warrant for electronic information" must meet certain requirements: it must "describe with particularity the information to be seized" and "require that any information obtained ... that is unrelated to the objective of the warrant shall be sealed." (*Id.*, § 1546.1, subd. (d)(1), (2)). In addition, the warrant must "comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants." (*Id.*, § 1546.1, subd. (d)(3).)

Here, law enforcement used a geofence warrant — a " ' "reverse location search[ ]" ' " request — to access device location data gathered by Google. (*People v. Meza* (2023) 90 Cal.App.5th 520, 525, 307 Cal.Rptr.3d 235 (*Meza*).) The warrant directed Google to search certain location history data, produce an anonymized list of devices, and turn over identifying information for devices that law enforcement deemed relevant to the investigation. (*Id.* at pp. 529–530, 307 Cal.Rptr.3d 235.) This led to the identification of defendants Daniel Meza and Walter Meneses, whose cell phones, while "signed in to Google accounts connected to them[,] were in several of the same locations" as the victim. (*Id.* at p. 526, 307 Cal.Rptr.3d 235.) Meza and Meneses challenge the warrant and admission of the resulting evidence under the Fourth Amendment to the United States Constitution and CalECPA.

The Court of Appeal concluded the geofence warrant violated the Fourth Amendment because it "lacked the particularity required by the Fourth Amendment and was impermissibly overbroad." (*Meza, supra*, 90 Cal.App.5th at p. 526, 307 Cal.Rptr.3d 235.) It then held that the warrant did not violate CalECPA, rejecting an argument that the "constitutional infirmities in the warrant create an independent violation" of the statute. (*Meza*, at p. 546, 307 Cal.Rptr.3d 235.) The Court of Appeal's analysis was minimal. It reasoned that "nothing in the [statutory] language ..., without more, converts a Fourth Amendment violation into a statutory violation." (*Ibid.*)

It is not apparent what "more" is necessary here. Penal Code section 1546.1, subdivision (d)(3) requires all warrants to comply with "all other provisions of California and federal law," which includes the Fourth Amendment. CalECPA's incorporation of the Fourth Amendment's requirements seems unambiguous: a warrant that violates federal law also violates CalECPA. Consistent with this reading, the statute's remedy provision specifically references Fourth Amendment violations: "Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter." (Pen. Code, § 1546.4, subd. (a).)

***15** The Court of Appeal held that these "provisions do nothing more than expressly preserve an individual's existing rights under the federal Constitution." (*Meza, supra*, 90 Cal.App.5th at p. 546, 307 Cal.Rptr.3d 235.) But there is no need for a state statute to "expressly preserve" federal rights. An individual can always independently pursue a federal constitutional challenge, as Meza and Meneses did here. CalECPA did not purport to supplant the requirements of federal law; in fact, it would have been impermissible for the statute to do so. (See *Sibron v. New York* (1968) 392 U.S. 40, 60–61, 88 S.Ct. 1889, 20 L.Ed.2d 917 [a state "is, of course, free to develop its own law of search and seizure to meet the needs of local law enforcement" but "may not ... authorize police conduct which trenches upon Fourth Amendment rights"].) Interpreting these provisions as solely preserving existing federal rights appears to give them no effect.

The consequences of this decision are potentially significant. Despite finding that the warrant violated the Fourth Amendment, the Court of Appeal declined to apply the exclusionary rule under the good faith exception of *United States v. Leon* (1984) 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677. (*Meza, supra*, 90 Cal.App.5th at p. 544, 307 Cal.Rptr.3d 235.) It is not clear whether such an exception applies to violations of CalECPA, and there are plausible arguments on both sides of the question. (See Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act* (*CalECPA*) (2018) 33 Berkeley Tech. L.J. 131, 161 ["[T]he state procedures do not incorporate the expansive exceptions that courts have used to deny suppression remedies in Fourth Amendment cases under the doctrine of good faith."], fn. omitted; *Meza*, at p. 546, fn. 17, 307 Cal.Rptr.3d 235 [declining to reach the question]; cf. *People v. Jackson* (2005) 129 Cal.App.4th 129, 153–160, 28 Cal.Rptr.3d 136 [considering various factors in concluding that the good faith exception does not apply to evidence gathered in violation of California's wiretap law].) If the exception does not apply, then the identifying evidence would be suppressed under CalECPA, thus affecting the validity of Meza's and Meneses's convictions.

CalECPA is a "significant" statute that made "the law governing access to electronic communications by law enforcement in California ... much more protective of communications privacy." (Freiwald, *supra*, 33 Berkeley Tech. L.J. at p. 133.) Because I find questionable the Court of Appeal's interpretation of this important state law, and because of the practical importance of the issue, I would grant review.

I Concur:

EVANS, J.

All Citations

--- Cal.Rptr.3d ----, 2023 WL 5287224

Footnotes

1 Verizon Connect, *What Is A Geofence*? <https://www.verizonconnect.com/glossary/what-is-a-geofence/#:~:text=A% 20geofence% 20is%20a% 20virtual,straight% 20line% 20between% 20two% 20points> [as of April 13, 2023], archived at < https://perma.cc/A3A6-NPZ9>.

2 SecureMac, *What Are Geofence Warrants?* (Sept. 8, 2020) <https://www.securemac.com/blog/what-is-geofencing> [as of April 13, 2023], archived at <https://perma.cc/74XS-KWGZ>.

3 Owsley, *The Best Offense Is A Good Defense: Fourth Amendment Implications of Geofence Warrants* (2022) 50 Hofstra L.Rev. 829, 834; see also Brief of Amicus Curiae Google LLC in Support of Neither Party, filed December 20, 2019 in *United States v. Chatrie* (E.D.Va. 2019, No. 3:19-cr-00130-MHL) (Google Amicus Brief) ("Google has observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019").

4 Statutory references are to this code.

5 Our factual summary is based on the preliminary hearing transcript and the search warrant affidavit.

6 One such document was the Google Amicus Brief filed in *United States v. Chatrie* (E.D.Va. 2022) 590 F.Supp.3d 901, which was admitted as an exhibit without objection at the hearing. McInvaille also considered two declarations of Google employees filed in *United States v. Chatrie*, which the superior court received into evidence without objection. These documents describe Google's location data collection and storage procedures as well as its process for responding to warrants for location history data.

7 According to Google, a user must not only enable location tracking on his or her device but also must opt-in to having that location data saved. Specifically, Google "saves a record of the user's travels only when the user opts into [location history] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it." (Google Amicus Brief, *supra*, at p. 8.) Nevertheless, some reports indicate Google can track a user's location history even when the user has opted out of location reporting. (See *In re Search of Information that Is Stored at the Premises Controlled by Google LLC* (D.D.C. 2021) 579 F.Supp.3d 62, 70 & fn. 8.)

8 See generally *Chatrie, supra*, 590 F.Supp.3d at page 914 ("[I]n 2018, Google held both internal discussions with its counsel and external discussions with law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice ('CCIPS'), to develop internal procedures on how to respond to geofence warrants. 'To ensure privacy protections for Google users, ... Google instituted a policy of objecting to any warrant that failed to include de[-]identification and narrowing measures.' [Citation.] Seemingly developed as a result of Google's collaboration with CCIPS, this de-identification and narrowing 'protocol typically ... entails a three-step process' ").

9 Article I, section 13 of the California Constitution similarly provides, "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized." Notwithstanding this separate warrant requirement in the California Constitution, pursuant to article I, section 28, subdivision (f)(2), of the state Constitution (the Truth-in-Evidence provision), "evidence sought to be introduced at a criminal trial is subject to suppression as the fruit of an unconstitutional search and seizure 'only if exclusion is ... mandated by the federal exclusionary rule applicable to evidence seized in violation of the Fourth Amendment [of the United States Constitution].' " (*People v. Maikhio* (2011) 51 Cal.4th 1074, 1089, 126 Cal.Rptr.3d 74, 253 P.3d 247; accord, *In re Lance W.* (1985) 37 Cal.3d 873, 896, 210 Cal.Rptr. 631, 694 P.2d 744.)

This limitation on the suppression of unlawfully obtained evidence does not apply if the search violated state law and exclusion was authorized "by statute hereafter enacted by a two-thirds vote of the membership of each house of the Legislature." (Cal. Const., art. I, § 28, subd. (f)(2).)

10 As a threshold matter no warrant is required if an individual has no reasonable expectation of privacy in the place or thing searched. (See *People v. Camacho, supra,* 23 Cal.4th at pp. 830-831, 98 Cal.Rptr.2d 232, 3 P.3d 878.) As the Attorney General recognizes, the prosecutor did not argue this point in the trial court; and, thus, the issue is forfeited. (See *People v. Nottoli* (2011) 199 Cal.App.4th 531, 561, 130 Cal.Rptr.3d 884 ["[s]ince the prosecutor failed, in opposing the suppression motion, to assert that Barry had no reasonable expectation of privacy in the vehicle or cell phone, the People have forfeited that issue on review of the suppression ruling"].) Nevertheless, the United States Supreme Court has suggested that an individual has a right to privacy regarding his or her current and historical location. (See *Carpenter v. United States* (2018) —— U.S. ——, [138 S.Ct. 2206, 2219], 201 L.Ed.2d 507 [retrieval of wireless carrier cell tower data to determine suspect's location "invaded [suspect's] reasonable expectation of privacy in the whole of his physical movements"]; *Riley v. California* (2014) 573 U.S. 373, 395-396, 134 S.Ct. 2473, 189 L.Ed.2d 430 [citing location history data as one of the privacy interests implicated by search of a cell phone's contents].)

11 While not the only way to address unfettered law enforcement discretion at steps two and three, judicial oversight at those steps, not just prior to issuance of the warrant, would resolve many of the constitutional deficiencies discussed. (See, e.g., *In re Search of Information that Is Stored at the Premises Controlled by Google LLC* (D.D.C. 2021) 579 F.Supp.3d 62, 88-89 [granting geofence warrant application requiring law enforcement to seek second court authorization for additional information regarding anonymous users initially identified by Google; this process "eliminated law enforcement's discretion at step two by requiring it to return to the Court and justify any device deanonymization"].)

12 See Note, *Geofence Warrants and the Fourth Amendment* (2021) 134 Harv. L.Rev. 2508, 2510-2511 (whether geofence warrants are Fourth Amendment searches is an open question; "[o]n the one hand, the [Supreme] Court has recognized that, in certain circumstances, individuals have reasonable expectations of privacy in their location information"; "[o]n the other hand, there is a strong argument that the third party doctrine—which states that individuals have no reasonable expectation of privacy in information they voluntarily provide to third parties—applies to these warrants" (fn. omitted)).

13 Despite finding the geofence warrant invalid the *Chatrie* court ultimately denied the defendant's motion to suppress based on the good faith exception of *Leon, supra,* 468 U.S. 897, 104 S.Ct. 3405.

14 Meza and Meneses attempt to distinguish *Chatrie* because in that case the detective sought advice from prosecutors before applying for the geofence warrant. While such a practice is certainly prudent when dealing with a novel search technique and a lack of legal authority, we cannot say in this particular instance the failure to do so rendered law enforcement's reliance on the warrant objectively unreasonable.

15 Prior to passage of CalECPA, California law did not require law enforcement officials to obtain a warrant to access most electronic information. Proponents of CalECPA sought to update the law for "the digital age" and "properly safeguard the robust constitutional privacy and free speech rights of Californians, spur innovation, and support public safety by instituting clear warrant standards for government access to electronic information." (Sen. Com. on Public Safety, Analysis of Sen. Bill No. 178 (2015-2016 Reg. Sess.) Mar. 24, 2015; see also Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act* (*CalECPA*) (2018) 33 Berkeley Tech. L.J. 131, 143-147.)

16 Senate Bill No. 178 (Stats. 2015, ch. 651) was adopted by a greater-than-two-thirds vote by both the state Senate and Assembly. See footnote 9, above.

17 Establishing an independent CalECPA violation in addition to a Fourth Amendment violation is crucial to Meza and Meneses's position because they contend the *Leon* good faith exception is not applicable to a CalECPA violation. We need not address that issue.