CERTIFIED FOR PARTIAL PUBLICATION*

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FOURTH APPELLATE DISTRICT

DIVISION TWO

AHMAD RAHEEM PRICE,

Petitioner,

v.

THE SUPERIOR COURT OF RIVERSIDE COUNTY,

Respondent;

THE PEOPLE,

Real Party in Interest.

E078954

(Super.Ct.No. RIF2004183)

OPINION

ORIGINAL PROCEEDINGS; petition for writ of prohibition. John D. Molloy,

Judge. Petition denied.

Steven L. Harmon, Public Defender, and Lisa M. Larson, Deputy Public Defender,

for Petitioner.

^{*} Pursuant to California Rules of Court, rules 8.1105(b) and 8.1110, this opinion is certified for publication with the exception of sections V and VI.

No appearance for Respondent.

Michael A. Hestrin, District Attorney, Natalie M. Lough and W. Matthew Murray, Deputy District Attorneys, for Real Party in Interest.

I. INTRODUCTION

Defendant Ahmad Raheem Price petitions for a writ of prohibition, directing the superior court to grant his motion to set aside the information (Pen. Code, §§ 995, 999a)¹ charging him with the first degree, premeditated murder of Jovany R. on October 29, 2019 (§ 187, subd. (a); count 1), and unlawfully possessing a firearm on the same day (§ 29800; count 2). The information further alleges that Price personally and intentionally discharged a firearm causing the death in count 1 (§ 12022.53, subd. (d)), and that Price has two prior serious felony convictions and two prior strikes (§ 667, subds. (a)-(i)). We issued an order staying the criminal proceedings pending the resolution of the writ petition, along with an order to respondent superior court to show cause why the relief sought in the petition should not be granted.

At the preliminary hearing on the felony complaint, and as part of his section 995 motion to set aside the information, Price moved to quash, traverse, and suppress all evidence obtained pursuant to 11 search warrants for electronic information, including a geofence warrant to Google, LLC (Google). A geofence warrant, or "reverse-location" warrant, draws a virtual geographic fence around the location of a crime, on the date of the crime, and for a specified, limited time period encompassing the crime. Geofence

¹ Undesignated statutory references are to the Penal Code.

warrants allow law enforcement agencies to identify suspects and witnesses to crimes by obtaining location data and identifying information associated with electronic devices traversing the geofence and carried by the suspects or witnesses. Google stores location data transmitted from, and has identifying information associated with, electronic devices that use Google's Android operating system or any Google application. Price was identified as a suspect in the shooting of Jovany R. based on location data and identifying information returned pursuant to the geofence warrant.

In the suppression motion, Price claimed that the geofence warrant and several of the other 10 warrants for electronic information (1) failed to satisfy the Fourth Amendment's probable cause and particularity requirements; (2) had to be traversed based on material factual omissions in their affidavits; and (3) violated the particularity and notice requirements of the California Electronic Communications Privacy Act (CalECPA; §§ 1546 to 1546.5). Price also moved to suppress evidence that the gun used in the October 29, 2019 shooting death of Jovany R. was found in Price's vehicle during a January 18, 2020 parole search. Price claimed that the gun evidence was fruit of Price's unlawful detention for being lawfully parked on a private driveway.

The magistrate at the preliminary hearing denied the suppression motion in its entirety and held Price to answer the murder, unlawful possession, and enhancement allegations of the felony complaint, including a robbery-murder special circumstance allegation. (§ 190.2, subd. (a)(17)). In ruling on the section 995 motion to set aside the information, respondent superior court dismissed the robbery-murder special

circumstance allegation but denied the section 995 motion in all other respects and denied the renewed suppression motion in its entirety.²

In the writ petition, Price renews his Fourth Amendment, traversal, and CalECPA claims concerning the geofence warrant and other warrants for electronic information. He claims the geofence warrant evidence and its fruits, including the gun evidence, must be suppressed, along with the other warrant evidence. He maintains that, without any of the warrant evidence or the gun evidence, there is insufficient evidence to hold him to answer the charges and allegations in the information.

In the published portion of this opinion, we address Price's Fourth Amendment, traversal, and CalECPA claims concerning the geofence warrant. We conclude that the geofence warrant satisfied the probable cause and particularity requirements of the Fourth Amendment and was not overbroad; it was reasonably and narrowly drawn in geographic scope and time period to capture the location data of only suspects and witnesses to the shooting death of Jovany R, and to minimize the possibility of allowing the government to obtain the location data and identifying information for uninvolved individuals persons who were neither suspects nor witnesses to the shooting. We also conclude that the good faith exception to the warrant requirement precludes the suppression of the geofence warrant evidence and its fruits, even if the geofence warrant is invalid under the Fourth Amendment. Lastly, we conclude that CalECPA does not require the suppression of the geofence warrant evidence despite the government's violation of CalECPA's

² The People do not challenge respondent Superior Court of Riverside County's dismissal of the robbery-murder special circumstance allegation.

notice provisions (§ 1546.2). In the unpublished portion of this opinion, we reject Price's claims concerning the other 10 warrants and the gun evidence. Thus, we conclude that the suppression motion was properly denied in its entirety, deny the writ petition, and lift the order staying the criminal proceedings against Price.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. The Suppression Motion

1. Overview

On November 8, 9, and 10, 2021, Price's motion to suppress the geofence warrant evidence, the other warrant evidence, and the gun evidence was heard with the preliminary hearing on the felony complaint charging Price with the October 29, 2019 shooting and murder of Jovany R. and unlawful firearm possession. West Covina Police Officer Kyle Clifton testified about his investigatory stop and detention of Price in West Covina on January 18, 2020, and the subsequent parole search of Price's vehicle during which the gun used in the shooting of Jovany R. was found.³

Riverside County Sheriff's Investigator Ryan Deanne was the lead investigator in the shooting death of Jovany R. and the affiant for the geofence warrant. Deanne testified about the investigation, the geofence warrant, and three other warrants seeking Price's Google e-mail (Gmail) account data and cell phone records, issued after Price was identified as a suspect in the shooting based on location data and identifying information

³ We discuss Officer Clifton's testimony, and Price's claims concerning the lawfulness of his detention and the admissibility of the gun evidence, in the unpublished portion of this opinion, section VI.

obtained from Google pursuant to the geofence warrant.⁴ Deanne also testified about his observations at the scene of the shooting, and his interviews with other investigating officers and witnesses, including Jovany R.'s brother, Samuel R., who was with Jovany R. at the time of the shooting and witnessed the shooting.⁵

2. Investigator Ryan Deanne's Testimony

(a) *The shooting death of Jovany R.*

Jovany R. was shot and killed in the front porch area of his Jurupa Valley home on October 29, 2019. An autopsy confirmed that the death was a homicide and that Jovany R. died from gunshot wounds to his left leg, back, and head. The forensic pathologist who performed the autopsy did not ascertain the caliber of the bullets that killed Jovany R. An unloaded, .40-caliber gun was found in Jovany R.'s waistband after the shooting, but no .40-caliber casings were found on or near Jovany R.'s body or at the scene.

The home had a concrete front porch and patio, and an "L"-shaped walkway from the front porch to the driveway, which led to a garage. Six .45-caliber shell casings were found on the walkway and grassy area near the front porch, and there were possible bullet-strike marks near the front door. The garage and several rooms inside the house were being used to grow marijuana, indicating a "marijuana grow" on the property.

⁴ We discuss the other warrant evidence, and Price's claims concerning the other warrant evidence, in the unpublished portion of this opinion, Section V.

⁵ At the time that he testified in November 2021, Deanne had been a peace officer for over 15 years, and he had been assigned to the homicide unit of the Riverside County Sheriff's Department for two and one-half years.

Jovany R.'s brother, Samuel R., spoke to investigators after the shooting. Samuel R. said that he, Jovany R., and a friend, Edgar A., were socializing in the house during the evening of October 29, 2019, when the front doorbell rang or there was a knock at the door. Jovany R. answered the door, went outside, and spoke with the person at the door. Jovany R. came back inside and said that the person at the door said that his car had broken down and he needed assistance.⁶ Jovany R. then went into a bedroom, came out, grabbed a pair of jumper cables and a charging box, and again went outside through the front door. Samuel R. did not follow Jovany R. into the bedroom but followed Jovany R. outside because he was concerned about home invasion robberies.

As Samuel R. and Jovany R. walked outside through the front door, Samuel R. saw a black male adult, whom Samuel R. did not recognize, standing a short distance from the door with either a gun or a knife pointed at Jovany R.'s face. The male said, "Don't move." Samuel R. described the male as five feet nine or ten inches tall, middle aged, in his 30s, with a beard and a muscular, stocky build, wearing gray pants and a gray shirt, but wearing nothing on his head.

Just as the male said, "Don't move," a second black male adult, whom Samuel R. also did not recognize, came around the corner of the house from the garage area and stood near the corner of the house. Samuel R. described the second male as younger than the first, in his 20s, around five feet five or six inches tall, with a "skinny" build, and

⁶ The magistrate admitted Jovany R.'s hearsay statement to Samuel R.—that the person at the door said his car had broken down and he needed assistance—for the limited purpose of explaining Jovany R.'s actions after making the statement.

wearing a black beanie, a black sweater, and red sweatpants. The second black male did not say anything. After the first male said, "Don't move," and the second male appeared, Samuel R. and Jovany R. began stepping backward toward the front door, but they did not turn around. Samuel R. was pushing Jovany R. toward the door. Samuel R. then heard two gunshots, Jovany R. fell to the ground, and the two males ran away in separate directions. The second male ran north on Homestead, the street in front of the house. Samuel R. did not see the second male get into a vehicle. The first male ran to a silver car parked on Homestead in front of the house, then the car proceeded south on Homestead. Samuel R. could not see whether anyone other than the first male was in the silver car. Samuel R. did not report seeing that either of the two males had a cell phone.

After Jovany R. was shot, Samuel R. attempted to help Jovany R. and yelled to Edgar A. to call 911. Edgar A. did not witness the shooting. He stayed inside the house while Samuel R. and Jovany R. went outside; and after he heard gunshots, he hid in the garage. Neither of the two males, the homicide suspects, demanded money or marijuana, or made any reference to marijuana. "Don't move" were the only words anyone said after Jovany R. and Samuel R. went outside. Samuel R. did not know whether Jovany R. grabbed at the gun in his waistband, or that Jovany R. even had a gun on his person, until officers told Samuel R. they found the gun in Jovany R.'s waistband.

Samuel R. told Investigator Deanne that the marijuana being grown in the house was for personal and medicinal use, and he denied that either he or Jovany R. was selling the marijuana. Deanne believed Samuel R. and Jovany R. were selling marijuana, based on the large quantity of marijuana in the house and because Samuel R. and Jovany R. had

a social media account in which it appeared that they were advertising marijuana for sale. Deanne did not recall whether the address of the house on Homestead appeared on the social media account. Police confiscated the marijuana plants and did not find a marijuana grow permit. No significant amount of cash was found in the house, and nothing outside the house indicated that there was a large marijuana grow inside or that marijuana was being sold there.

(b) Further investigation and search warrants

Several days after the October 29, 2019 shooting death of Jovany R., investigators obtained surveillance video recordings from a gas station located east of the intersection of Homestead and Limonite, less than one-half of a mile from the scene of the shooting at the house on Homestead. The surveillance video showed a silver car heading east on Limonite, moments before it showed a patrol vehicle that was responding to the shooting heading west on Limonite toward Homestead. After receiving the surveillance videos, Investigator Deanne drafted the geofence warrant and supporting affidavit.

In his testimony in November 2021, Deanne explained that a geofence warrant creates a geographical fence around a particular location, typically in the form of a circle, rectangle, or square, using longitude and latitude points. The geofence warrant is directed to Google, and Google is asked to identify any electronic devices, including smartphones, that Google is tracking and that were located inside the geofence at or around the time of the crime. Google tracks the locations of smart phones and other devices that use at least one Google application (e.g., Google Maps), regardless of whether the device runs on the Google-supported Android or Apple-supported [iOS]

operating systems. Google does not track device locations while the device is turned off, but a Google application does not have to be in use on a device to allow Google to track the device through the Google application. Deanne also explained that a geofence warrant should be as specific as possible in terms of the date, time, and location of the crime, and the device data that the geofence warrant seeks. Deanne said, "If you know that the person [who] committed [the] crime took this pathway to and from the crime scene, you would want to include that pathway and the crime scene in your geographical fence."

Google has an online portal it calls LERS (law enforcement reporting system), where geofence warrants are uploaded and law enforcement agencies are required to follow a process established by Google to receive the data the warrant seeks. Google releases requested data in three stages. In stage one, Google identifies all devices located within the geofence area, or the geofence, by anonymized numbers known as "automated device identifiers" or "device IDs." The device IDs disguise the personal identities of the device users or subscribers. In stage two, law enforcement may ask Google to provide additional data, including location histories, outside the geofence, for devices identified in stage one. This location history data gives "a more expanded view" of the location and movements of the devices, or some of the devices, identified by anonymized device IDs in stage one. In stage three, law enforcement asks Google for information identifying the users or subscribers of the device IDs identified in stages one or two.

The geofence for the geofence warrant encompassed the front yard of Jovany R.'s house, including the front porch area where the shooting occurred, and the street in front

of the house (Homestead) for the lengths of two houses in each direction (north and south), between 10:00 p.m. and 10:22 p.m. on October 29, 2019—a 22-minute period. Multiple 911 calls about the shooting occurred during this period, including at 10:14 p.m. to 10:15 p.m. The geofence warrant was issued, ordered sealed, and served on November 7, 2019. In addition to sealing the warrant, the issuing magistrate granted the government a 90-day extension of the 90-day period for notifying the identified "target" of the warrant of the issuance of the warrant, pursuant to CalECPA. (§ 1546.2.)

Around January 29, 2020, Deanne received stage one information from Google, showing that five device IDs were located in the 22-minute geofence. Next, Deanne requested "stage two information" showing the locations of the five device IDs both before and after the 22-minute period, and Deanne received the stage two information in March 2020. The stage two information showed that two of the five device IDs were at the house on Homestead for five to seven minutes during the 22-minute period and later travelled east on Limonite, past the gas station where the surveillance video showed a silver car traveling east on Limonite after the shooting. Deanne then asked Google for stage three identifying information for the two device IDs that appeared to belong to the two suspects. On September 14, 2020, Deanne received stage three information, showing that the two device IDs were associated with a single device and two Gmail accounts one using the phrase "Product of Music" and the other, "Be Hood Music." Price's name was associated with both Gmail accounts, and the "recovery" phone number associated with both Gmail accounts ended in 4481. A Gmail account subscriber provides a "recovery" phone number to Google for security and password recovery purposes.

Deanne then instructed another investigator to prepare a warrant to Google for data related to Price's Gmail accounts, and a warrant to AT&T, the service provider, for data related to Price's 4481 number.

Using a mapping program and the location data received for the two device IDs associated with Price's two Gmail accounts, a crime analyst created a map showing a single device using Price's two Gmail accounts traveling on Limonite and other streets to Jovany R.'s house on Homestead, between 9:50 p.m. and 10:09 p.m. on October 29, 2019. A second map using the same Gmail account location data showed the device traveling to Price's home in West Covina between 10:20 p.m. and 10:58 p.m. on October 29. A third map showed the device traveling from Price's home in West Covina to a restaurant in Jurupa Valley, one to two miles from Jovany R.'s house, between 8:01 p.m. and 8:49 p.m. on October 29. A fourth map, created using call records for Price's 4481 number, was consistent with the program maps based on the Gmail account location data. The fourth map showed the device using the 4481 number traveling to and from Jovany R.'s house at the same times as the maps based on the Gmail account data.

After mapping the location data returned from the geofence warrant, the Gmail accounts warrant, and the 4481 call-records warrant, Deanne began looking into Price's background. Deanne discovered that, on November 6, 2019, eight days after the shooting, Price was driving a silver 2017 Ford Fusion when he was involved in a traffic collision in West Covina. Deanne compared three photographs: (1) a "stock" photograph of a 2017 Ford Fusion, (2) a screen shot of the silver car shown in the October 29 gas station video, and (3) a photograph of the vehicle Price was driving

during the November 6 collision, obtained using that vehicle's license plate number. Deanne believed that the silver car observed in the screen shot from the gas station video matched the description of a 2017 Ford Fusion.

After Deanne identified Price as a suspect in the murder, a criminal analyst made a six-pack photo lineup that included Price. When shown the lineup, Samuel R. excluded Price as the shooter and identified another male as the shooter. Deanne believed the photo of Price shown to Samuel R. was taken on January 18, 2020, but Deanne was unsure. Deanne also learned that West Covina police had arrested Price for unlawfully possessing a firearm on January 18, 2020. Deanne contacted the West Covina Police Department and learned that the firearm was a .45-caliber handgun, the same caliber as the six shell casings found at the scene of the October 29, 2019 shooting.

Deanne obtained the gun from the West Covina Police Department pursuant to a warrant and had the gun test-fired to compare the test casings to the .45-caliber casings found at the scene. A firearm examiner used a machine to compare the two sets of casings. Based on the first test results, the examiner concluded that the casings did not match. Deanne asked that the gun be retested, the examiner performed a second test, and concluded that the casings matched. It was discovered during the second test that the test casings were incorrectly put into the machine during the first test. A third test reconfirmed that the casings matched.

Deanne then obtained a second warrant to AT&T, referred to as a "ping data in real time warrant" seeking Price's real-time cell phone location data for the 4481 number, along with 4481 call records, for September 15, 2020 through November 25, 2020.

Deanne believed that Price was still using the 4481 number in September 2020 and wanted to track Price's location through the 4481 number.

Deanne then asked Price's parole officer to arrange a meeting with Price. In early December 2020, investigators tracked Price's 4481 phone in real time and saw that the phone traveled from Las Vegas to Pomona where Price was scheduled to meet with his parole officer. Price was arrested at the meeting. When Price was arrested, Deanne gave Price "service copies" of the four warrants issued during the investigation that sought electronic information "related to" Price-namely, the geofence warrant, the Gmail accounts warrant, the 4481 call-records warrant, and the 4481 ping-data warrant. The service copies included "everything except" the affidavits and probable cause statements of the warrants. When Deanne gave Price the service copies, Deanne told Price that the sheriff's department had received all of the information it sought in the four warrants and gave Price a verbal summary of the information received. On December 8, 2020, a felony complaint was filed charging Price with the murder of Jovany R. and unlawful firearm possession, and alleging firearm, prior conviction, and robbery-murder special circumstance enhancements.

3. The Contents of the Geofence Warrant and Affidavit

The geofence warrant sought "all identifying information" according to the Google "production protocol" for Google accounts reporting "location history data generated from devices that reported a location" within the geofence. As Deanne testified, the warrant limited the geofence to the front yard of Jovany R.'s home, where the shooting occurred, and the street in front of the home (Homestead) for the length of

two houses in each direction, where Samuel R. saw the two suspects flee in separate directions after the shooting. The street portion of the geofence on Homestead abutted the yards of 11 homes, including Jovany R.'s front yard. The warrant requested location data in the geofence between 10:00 p.m. and 10:22 p.m. on October 29, 2019, a 22-minute period encompassing the time of the shooting, according to 911 calls and the times officers responded to the scene of the shooting. The warrant included an aerial photograph of the geofence marked by latitude and longitude coordinates, and areas immediately around the geofence.

In accordance with the Google "production protocol," the warrant requested data in stages by directing Google to do the following: "1. Google shall query location history data based on the Initial Search Parameters described above [the area, date, and time period of the geofence]. [¶] 2. For each location point recorded within the Initial Search Parameters, Google shall produce an Anonymized List specifying a unique device identifier, timestamp, coordinates, display radius, and data source. [1] 3. The Examining Officer will then review the Anonymized List to identify a Target List of devices that fit a pattern described in this Affidavit. If the Examining Officer needs additional location information outside the Initial Search Parameters for specific devices in the Anonymized List to determine if they fit a pattern described in this Affidavit, the officer may submit an additional request to Google for additional location information within the listed time period. For instance, an account moving quickly through the target area may be excluded from the Target List if additional information suggests that the device is on a highway and not associated with the events described in this Affidavit.

4. For those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google [p]rovide identifying information, without additional legal service, as defined in 18 U.S.C. § 2703(c)(2) [name, address, etc.], for the Google Account associated with each identified device ID. [¶] 5. The examining officer may provide the Target List to Google. Upon receiving the Target List, Google shall provide the following subscriber information for the Google Account associated with each identified device: [name, street address, telephone number], email address or similar contact information provided by the subscriber to the provider to establish or maintain an account or communication channel."

The stated purpose of the warrant was to "authorize the examination of Google location history records from the time and place of the homicide to identify potential suspects and/or witnesses." Investigator Deanne signed the warrant affidavit, in which he described the circumstances of the shooting and averred that no suspects had been identified. Deanne also explained why there was probable cause to believe Google had electronic information that would identify the suspects or lead to their identification. Deanne averred based on his training and experience that, "most people in today's society" possess and carry "cellular phones and other connected" devices, which "may include global positioning systems (GPS) and other technology for determining a more precise location of the [phone or] device." Google uses an operating system known as Android for its mobile devices. According to a February 2018 study by a research company, approximately 99.9 percent of all smartphones were supported either by Google's Android operating system or Apple's iOS operating system, and 86 percent of

the 99.9 percent were Android-supported. All Android-supported devices have a Google account, and Apple iphones support Google applications, which also include a Google account. These Google applications include Google Search, Gmail, Google Maps, and Google Drive. Whenever a user activates a Google account, Google asks the user to provide a phone number for the account.

Google collects and retains location data on its server, the "'Sensorvault,' " from Android-operated devices and devices supporting Google applications, as long as the location services of the device are enabled. That is, Google collects location data "whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messag[e], internet access, or email access," and also when the user is not "interacting with the device" but Google applications are "running in the background." The location data is derived from several sources—GPS data, cell site/cell tower information, Bluetooth beacons, and Wi-Fi access points—and is "stored forever" unless the user deletes it.

Because most people use and carry a cell phone nearly all the time, and nearly all such devices are Android-operated or use Google applications and associated Google accounts, Deanne averred it was likely the two suspects were carrying at least one such device at the time of the shooting. Additionally, when multiple suspects are involved in criminal activity, they "typically" use cell phones to communicate with each other.

Deanne also explained how the warrant would be executed according to the Google production protocol. The initial device tags provided by Google would be provided in an anonymized list and would not include any "subscriber information"

identifying the device subscribers. The anonymized list of device tags would "allow investigators to see which Google device tags were present in the geographical area [the geofence area] prior to, during, and after the crime." Law enforcement would "review the Anonymized List to remove device tags that are not relevant to the investigation, such as device tags that were not in the location for a sufficient period of time." If law enforcement needed additional location information for a given device tag to determine whether the device was relevant to the investigation, it could ask Google to provide that information. Additional location "information provided by the extended timeframe and times when entering and exiting the geographical area" would "allow investigators to determine which device tags require further investigation and which ones do not," and would also "assist investigators in understanding a bigger geographic picture and timeline," which could identify witnesses and "inculpate or exculpate the account owners."

At Deanne's request, the issuing magistrate ordered the warrant, including its affidavit, statement of probable cause, return, and all documents related to the warrant sealed until further order of court. Deanne averred in the warrant that publicizing this information would "make it impossible to continue" the murder investigation. The issuing magistrate also granted Deanne's request for a 90-day delay in notifying the target of the warrant, contemporaneously with the service of the warrant on Google, pursuant to CalECPA. (§ 1546.2, subd. (b).) Deanne averred that the 90-day notice delay was "justified because providing prior notice to the target . . . would lead to an adverse result" in that it could "endanger the life or physical safety of an individual; lead

to flight from prosecution"; destruction of or tampering with evidence; witness intimidation; or "otherwise seriously jeopardize" the investigation. (§§ 1546, subd. (a) [defining " 'adverse result' " for CalECPA purposes], 1546.2, subd. (b) [authorizing delayed notice].) The warrant did not explain that there was no "identified target" of the warrant at the time the warrant was issued. (§ 1546, subd. (c).)

B. The Preliminary Hearing Magistrate's Rulings on the Suppression Motion

In denying the suppression motion at the preliminary hearing, the magistrate ruled that the geofence warrant was supported by probable cause to believe the suspects were carrying cell phones, and the warrant was not overbroad but was "narrowly tailored" in terms of its geographic scope and time frame to capture only the location data of the suspects and possible witnesses to the shooting. The magistrate concluded that the other 10 warrants for electronic information were also supported by probable cause and described the data sought with sufficient particularity; none were overbroad in terms of the nature or extent of the data they sought.

Regarding Price's traversal claims, the magistrate ruled that the evidence Price was complaining was omitted from the affidavits for the 11 warrants was immaterial, and "a mountain of evidence" and probable cause supported the warrants. The magistrate also rejected Price's claim that CalECPA required the suppression of all evidence obtained pursuant to a warrant that violates its provisions, including its particularity and notice requirements. (§§ 1546.1, subd. (d)(1) [particularity], 1546.2 [notice], 1546.4 [remedies].) The magistrate concluded that the remedy for a CalECPA violation is a *motion to suppress* the warrant evidence (§ 1546.4), and a court is not required to

suppress evidence based on "technical" CalECPA violations. The magistrate also denied Price's motion to suppress the gun evidence.

After denying the suppression motion, the magistrate found sufficient evidence to hold Price to answer all of the charges and enhancements alleged in the felony complaint. On November 22, 2021, an information was filed charging Price with the October 29, 2019 murder of Jovany R., unlawful firearm possession, and alleging prior conviction, firearm, and robbery-murder special circumstance enhancements.

C. The Renewed Suppression Motion and Section 995 Motion

In moving to set aside the information (§ 995), Price renewed the suppression motion he made at the preliminary hearing, including the motions to quash and traverse the 11 warrants, suppress the warrant evidence and its fruits, and suppress the gun evidence as the fruit of his unlawful detention on January 18, 2020. On April 21, 2022, respondent superior court issued a detailed order, dismissing the robbery-murder special circumstance allegation but denying the section 995 motion in all other respects and denying the renewed suppression motion in its entirety.

III. STANDARD OF REVIEW

At a preliminary hearing on a felony complaint, the defendant may move to suppress evidence that the defendant claims was obtained as a result of an invalid search or seizure. (*People v. Magee* (2011) 194 Cal.App.4th 178, 182-183; § 1538.5, subds. (a), (f))(1).) If the motion is denied and the defendant is held to answer, the defendant may renew the suppression motion in the superior court under the standards governing a

section 995 motion. (*People v. Magee*, at p. 182; § 1538.5, subd. (m).)⁷ In a section 995 proceeding, the superior court "merely reviews" the evidence presented at the preliminary hearing; it does not substitute its judgment on the weight of the evidence or resolve conflicts in the evidence. (*People v. McDonald* (2006) 137 Cal.App.4th 521, 529.) The role of the superior court " ' "is similar to that of an appellate court reviewing the sufficiency of the evidence to sustain a judgment and involves the determination of a legal issue only." '" (*Brewer v. Superior Court* (2017) 16 Cal.App.5th 1019, 1023.)

In reviewing a section 995 order, itself reviewing a magistrate's order denying a suppression motion at a preliminary hearing, " 'we, in effect, review the magistrate's decision directly, deferring to the magistrate's factual findings.' " (*People v. Kidd, supra,* 36 Cal.App.5th at p. 17.) " 'We must draw all presumptions in favor of the magistrate's factual determinations, and we must uphold the magistrate's express or implied findings if they are supported by substantial evidence.' " (*People v. Hawkins* (2012) 211 Cal.App.4th 194, 200.) But, like the superior court, we independently determine whether the search or seizure was reasonable. (*People v. Magee, supra,* 194 Cal.App.4th at p. 183; see § 1538.5, subd. (a).) That is, " '[w]e judge the legality of the search by

⁷ The defendant may also renew the defendant's preliminary hearing challenge of the validity of the search or seizure, or challenge of the validity of the search or seizure in the first instance, in "a special hearing relating to the validity of the search or seizure." (§ 1538.5, subd. (i)); *People v. Kidd* (2019) 36 Cal.App.5th 12, 19-20 & fn. 3, disapproved on other grounds in *People v. Tacardon* (2022) 14 Cal.5th 235, 245-247 (*Tacardon*); *People v. Superior Court* (*Cooper*) (2003) 114 Cal.App.4th 713, 717.) Price did not utilize the special hearing procedure. (§ 1538.5, subd. (i).)

"measur[ing] the facts, as found by the trier, against the constitutional standard of reasonableness." '" (*People v. Magee*, at p. 183.)

When a search warrant is challenged as unsupported by a showing of probable cause in the affidavit (U.S. Const., 4th Amend.), we review the probable cause determination of the magistrate who issued the warrant. "A magistrate's determination of probable cause is entitled to great deference by reviewing courts. [Citation.] A court reviewing the sufficiency of an affidavit on which a search warrant is issued, should not conduct a de novo review of the evidence. . . . (*Ibid.*) Rather, the [issuing] magistrate's determination of probable cause should be disturbed on review only if the affidavit fails as a matter of law to set forth sufficient competent evidence to support the magistrate's finding of probable cause." (*People v. McDaniels* (1994) 21 Cal.App.4th 1560, 1564.)

IV. THE GEOFENCE WARRANT

A. Fourth Amendment Claims

1. Fourth Amendment Principles, Overview

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides, "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.) The Fourth Amendment was intended to prevent, " the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'" (*Carpenter v. United States* (2018) 585 U.S.___,___

[138 S.Ct. 2206, 2213]; *Riley v. California* (2014) 573 U.S. 373, 403; *Steagald v. United States* (1981) 451 U.S. 204, 220 ["The central objectionable feature" of general warrants and writs of assistance was that they provided "no judicial check" on executing officials' discretion to decide where to search or whom or what to seize.].)

"To satisfy the demands of the Warrant Clause, a warrant must comply with two related but distinct rules. First, it must describe the place to be searched or things to be seized with sufficient particularity, taking account of 'the circumstances of the case and the types of items involved.' [Citation.] Second, it must be no broader than the probable cause on which it is based. [Citation.] The particularity rule and the probable cause rule serve a common purpose: to protect privacy by prohibiting 'a general, exploratory rummaging in a person['s] belongings.' [Citation.] Although the two rules serve the same ultimate purpose, they achieve the purpose in distinct ways." (*United States v. Weber* (9th Cir. 1990) 923 F.2d 1338, 1342.)

There is probable cause for a search if "there is a fair probability that evidence of a crime will be found in a particular place." (*Illinois v. Gates* (1983) 462 U.S. 213, 238.) The probable cause showing must be made in the warrant affidavit (*People v. Carrington* (2009) 47 Cal.4th 145, 161) and, as noted, the scope of the search must be "no broader than the probable cause on which [the warrant] is based" (*United States v. Weber, supra*, 923 F.3d at p. 1342; *Burrows v. Superior Court* (1974) 13 Cal.3d 238, 250 ["It is axiomatic that a warrant may not authorize a search broader than the facts supporting its issuance."]). A warrant is unconstitutionally overbroad if it describes the place to be searched in broader terms than is justified by the probable cause showing. (*United States*

v. Snow (D.AZ, Oct. 9, 2019, CR 18-1796-TUC-JGZ) 2019 U.S. Dist. Lexis 230128, p. *11.)

The particularity requirement—that a warrant particularly describe the place to be searched and the persons or things to be seized—renders a general, exploratory search impossible by preventing " 'the seizure of one thing under a warrant describing another' " and leaving " 'nothing to the discretion of the officer executing the warrant.' " (Stanford v. Texas (1965) 379 U.S. 476, 485.) The particularity requirement prevents the government from exercising "unbridled authority" under the warrant. (Id. at pp. 481, 485-486; Maryland v. Garrison (1987) 480 U.S. 79, 84 ["By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] 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. Frank (1985) 38 Cal.3d 711, 726 ["The vice of an overbroad warrant is that it invites the police to treat it merely as an excuse to conduct an unconstitutional general search."]; United States v. Sanchez-Jara (7th Cir. 2018) 889 F.3d 418, 421 [A warrant cannot be "an open-ended authorization for public officials to rummage where they please in order to see what turns up."].)

In determining whether a warrant is sufficiently particular in describing the place to be searched or the things to be seized, courts look to "such factors as the purpose for which the warrant was issued, the nature of the items to which it is directed, and the total circumstances surrounding the case." (*People v. Rogers* (1986) 187 Cal.App.3d 1001,

1008.) Neither "complete precision" nor "near certainty" is required. (*People v. Amador*(2000) 24 Cal.4th 387, 392; *People v Hepner* (1994) 21 Cal.App.4th 761, 775-776.)

2. Fourth Amendment Case Law on Geofence Warrants

When the geofence warrant in this case was issued on November 7, 2019, "there were no published cases anywhere in the country, let alone in California, analyzing the constitutionality of geofence warrants." (*People v. Meza* (2023) 90 Cal.App.5th 520, 526, review filed May 22, 2023, S280089 (*Meza*).) Since July 2020, several published federal district court decisions have addressed Fourth Amendment challenges to geofence warrants, both in the context of considering geofence warrant applications and in ruling on motions to suppress geofence warrant evidence.⁸

⁸ The federal court decisions considering geofence warrant applications are: *In re* Search of Info. Stored at Premises Controlled by Google (N.D. Ill., July 8, 2020, No. 20M297) 2020 U.S.Dist. Lexis 165185 (Pharma I) [denying application], followed by In re Search of Info. Stored at Premises Controlled by Google (N.D. Ill., 2020) 481 F.Supp.3d 730 (Pharma II) [same]; and In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation (N.D. Ill., 2020) 497 F.Supp.3d 345 (Arson Investigation) [granting application]; In re Search of Info. That Is Stored at the Premises Controlled by Google LLC (D. Kan., June 4, 2021) 542 F.Supp.3d 1153 (Kansas Federal Crimes) [denying application]; In re Search of Info. Stored at Premises Controlled by Google (D.D.C., Dec. 30, 2021) 579 F.Supp.3d 62 (D.C. Federal Crimes) [granting application]; and In re Search of Info. That is Stored At Premises Controlled by Google (S.D. Tx., Feb. 14, 2023, No. 2:22-mj-01325) 2023 U.S. Dist. LEXIS 33651 (Texas Federal Crimes) [granting application]. See In re Search of Info. Stored at Premises Controlled by Google (Va. Cir., Feb. 24, 2022, No. KM-2022-79) 2022 Va. Cir. Lexis 12 [denying application]. The federal court decisions considering motions to suppress geofence warrant evidence are: United States v. Chatrie (E.D. Va. 2022) 590 F.Supp.3d 901 (Chatrie), United States v. Rhine (D.D.C., Jan. 24, 2023, No. 21-0687) 2023 U.S.Dist. Lexis 12308 (Rhine); United States v. Smith (N.D.Miss., Feb. 10, 2023, No. 3:21-cr-107-SA) 2023 U.S.Dist. Lexis 22944 (Smith); and United States v. Carpenter (M.D.Fl., Feb. 28, 2023, No. 8:21-cr-309-VMC-MRM) 2023 U.S.Dist. Lexis 64948 (Carpenter).

Although we are not bound by the decisions of lower federal courts on questions of federal law, such decisions are " " "persuasive and entitled to great weight" ' " when, as here, they are " 'both numerous and consistent.' " (*People v. Nguyen* (2022) 82 Cal.App.5th 888, 897.) We are also guided by *Meza*, to date the only California Court of Appeal decision to address the constitutionality of a geofence warrant. (*Meza, supra*, 90 Cal.App.5th at pp. 536-543.) The California Supreme Court and United States Supreme Court have yet to rule on the Fourth Amendment constitutionality of a geofence warrant.

3. The Geofence Affidavit Showed Probable Cause to Believe the Suspects'

Identities Would be Revealed Through the Geofence Search⁹

Price first claims that the geofence warrant is invalid because its affidavit failed to show probable cause to believe that evidence of a crime, namely, the suspects' identities, would be found through the geofence search. (*Illinois v. Gates, supra*, 462 U.S. at

⁹ The government's intrusion into a place where an individual has a reasonable expectation of privacy—an expectation society is prepared to recognize as reasonable—is a "search" that triggers the Warrant Clause of the Fourth Amendment. (Carpenter v. United States, supra, 138 S.Ct. at pp. 2211-2213, 2217 & fn. 3 [warrant required to access at least seven days of "cell site location information" (CSLI) maintained by cell phone service provider]; Riley v. California, supra, 573 U.S. at p. 403 [warrant required for search incident to arrest of suspect's cell phone contents]; United States v. Jones (2012) 565 U.S. 400, 404-405 [warrant required to install GPS tracking device on vehicle to track its movements over 28 days].) The United States Supreme Court has not determined whether individuals have a reasonable expectation of privacy in their electronic device location data, even for short periods of time. (See Geofence Warrants and the Fourth Amendment (2021) 134 Harv. L. Rev. 2508, 2509-2510 [It is "an open question" whether "geofence warrants are Fourth Amendment searches."].) We assume for purposes of our discussion of Price's Fourth Amendment claims that the search for location data and identifying information, as authorized by the geofence warrant, constituted a "search" within the meaning of the Fourth Amendment.

p. 238.) Price claims the warrant affidavit failed to show probable cause to believe (1) the suspects were carrying cell phones, given that the affidavit was "devoid of any facts that someone saw" either of the suspects with a cell phone, and, therefore, (2) that Google would have location data and identifying information revealing the suspects' identities.

"The question facing a reviewing court asked to determine whether probable cause supported the issuance of the warrant is whether the [issuing] magistrate had a substantial basis for concluding a fair probability existed that a search would uncover wrongdoing. [Citations.] "The task of the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.' " (*People v. Kraft* (2000) 23 Cal.4th 978, 1040-1041; *People v. Hulland* (2003) 110 Cal.App.4th 1646, 1651.)

Here, the suspects' identities was the evidence that the geofence warrant sought to uncover. For two reasons, the warrant affidavit gave the issuing magistrate a substantial basis for concluding there was a fair probability the geofence warrant search would reveal the suspects' identities. First, the affiant, Investigator Deanne, averred that in his experience people who plan and commit crimes together use cell phones to communicate, and that "most people in today's society" possess and carry "cellular phones and other ... devices," which "may include global positioning systems (GPS) and other technology for determining a more precise location of the [phone or] device." These statements, together with the evidence that the suspects acted in concert in committing the shooting,

gave the issuing magistrate a substantial basis for concluding there was a fair probability the suspects were carrying cell phones at the time of the shooting. Thus, it was unnecessary for the affidavit to show that a witness saw either suspect with a cell phone. (*Arson Investigation, supra*, 497 F.Supp.3d at pp. 355-356.)

It is also a matter of indisputable common knowledge that most people carry cell phones virtually all the time, and courts may take judicial notice of "facts and propositions that are of such common knowledge . . . that they cannot reasonably be the subject of dispute." (Evid. Code, § 452, subd. (g).) In 2018, the United States Supreme Court observed that individuals "compulsively carry cell phones with them all the time." (Carpenter v. United States, supra, 138 S.Ct. at p. 2218 ["While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time."]; see Riley v. California, supra, 573 U.S. at p. 384 ["[M]odern 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."].) Other courts have followed suit in recognizing that nearly everyone regularly carries a cell phone. (United States v. James (8th Cir. 2021) 3 F.4th 1102, 1105 ["Even if nobody knew for sure whether the [suspect] 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.' "]; D.C. Federal Crimes, supra, 579 F.Supp.3d at p. 78 ["The core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business."].) The common knowledge that most people carry cell

phones gave the issuing magistrate a substantial basis for concluding there was a fair probability that the suspects were carrying cell phones at the time of the shooting.

Second, the affidavit explained why there was a fair probability that the suspects' cell phones were sending location data to Google, and that Google had location data and identifying information associated with the suspects' cell phones or devices that would reveal the suspects' identities. The affidavit cited a February 2018 study showing that around 99.9 percent of all smartphones were supported by Google's Android operating system or Apple's iOS operating system. The affidavit explained that all Android-supported devices have a Google account; the use of a Google application also requires a Google account; Apple iphones, like Google's Android devices, support Google applications; and a Google account cannot be activated without providing Google with a name and phone number for the Google account. Also, Google collects and retains location data from all Android-operated devices and devices using Google applications, as long as the device's location services are enabled. The location data is "stored forever" unless the user deletes it.

Although this explanation of how Google obtains and retains location data and identifying information did not show it was certain that Google would have location data and identifying information revealing the suspects' identities, the explanation demonstrated a fair probability this was the case, and this fair probability was sufficient. (*Arson Investigation, supra*, 497 F.Supp.3d at pp. 355-356.) The affidavit provided a substantial basis for the issuing magistrate to conclude there was a fair probability that the suspects were carrying cell phones and would be identified through location data and

identifying information through the geofence search. Thus, the affidavit showed probable cause to believe the geofence search would reveal the suspects' identities.

Arson Investigation is instructive. There, the court granted a geofence warrant application despite there being "no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense," and no "additional evidence that perpetrators or witnesses of the crime used Google applications or operating systems that would store location data." (*Arson Investigation, supra,* 497 F.Supp.3d at pp. 355-356, 363.) The court reasoned that an agent's training and experience can provide information necessary to establish probable cause in an affidavit, that "probable cause does not require conclusive evidence that links a particular place or item to a crime," and that " '[t]he Fourth Amendment does not require certainty that a search will uncover the sought-after evidence; a fair probability is enough." (*Ibid.*)

Applying these principles, the court found that the warrant affidavit showed a fair probability to believe the suspects in the crimes under investigation were carrying cell phones, and "that location data at Google will contain evidence of the arson crime[s], namely the identities of perpetrators and witnesses to the crime[s]." (*Arson Investigation, supra*, 497 F.Supp.3d. at p. 356.) Other courts have found sufficient probable cause based on similar showings. (*Meza, supra,* 90 Cal.App.5th at pp. 536-537; *D.C. Federal Crimes, supra,* 579 F.Supp.3d at pp. 78-80; but see *Kansas Federal Crimes, supra,* 542 F.Supp.3d at pp. 1155-1157 [denying geofence warrant application as "too vague and generic to establish a fair probability" that the suspect or any witnesses would be identified through the proposed geofence search].) Similarly here, the warrant affidavit

showed a fair probability that (1) the suspects were carrying cell phones, (2) the phones were used a Google application, and, therefore, (3) Google would have location data and identifying information revealing the suspects' identities.

4. The Geofence Warrant Was Not Overbroad

Price next claims the geofence warrant failed to satisfy the probable cause and particularity requirements of the Fourth Amendment because: (1) the warrant affidavit did not show probable cause to believe every individual or device user likely to be located in the geofence was a suspect or witness to the shooting of Jovany R., and (2) the affidavit was insufficiently particular in describing the individuals and information to be searched and seized because Google's multi-step production protocol, the process followed in executing the warrant, is overbroad and unconstitutional on its face.

Again, *Arson Investigation* is instructive. The case illustrates that, if a geofence warrant is narrowly tailored, in its initial search parameters, or geographic scope and time period, to maximize the probability it will capture only suspects and witnesses, and to minimize searches of location data and identifying information of individuals for whom there is no probable cause to believe were suspects or witnesses (uninvolved individuals), then the discretion afforded to the executing officer by Google's multi-step production protocol will be constitutionally immaterial. (*Arson Investigation, supra*, 497 F.Supp.3d at pp. 360-363.) As we explain, the geofence warrant here fits this description.

In *Arson Investigation*, the government sought a geofence warrant to identify two suspects in a series of arsons involving multiple vehicle fires on two commercial lots, separated by roadways, in the City of Chicago. (*Arson Investigation, supra*,

497 F.Supp.3d at p. 351.) The arsons occurred during the early morning hours (around 2:00 a.m.) on two days in July and December 2019. (*Id.* at pp. 351-353.) The geographical areas of the proposed geofences focused on each lot, a roadway between the two lots, and part of another roadway near one lot. The time periods of the proposed geofences were 17 to 37 minutes in length and were narrowly focused on the times the suspects were believed to be at the lots committing the arsons and driving on the roadways before, after, and between the arsons. (*Id.* at pp. 351-352, 358.) The proposed geofences included some areas where uninvolved individuals may have been located, even during the early morning time periods: the roadways, two garages, a trailer, and a mixed-use building with an apartment. (*Id.* at p. 351, 357.)

The court explained that a geofence warrant must be "particular in time, location, and scope." (*Arson Investigation, supra*, 497 F.Supp.3d at pp. 353, 356.) That is, the warrant must be narrowly crafted, in time and geographic scope, to "minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses." (*Ibid.*) But the warrant does not have to eliminate every possibility that it will capture location data and identifying information of individuals for whom there is no probable cause to believe are suspects or witnesses to the crimes. (*Id.* at pp. 360-361.) Instead, the time and geographic scope of the geofence are judged by a reasonableness standard. (*Id.* at pp. 361.)

"[T]he Fourth Amendment deals in probabilities and reasonableness, and not exactness and pinpoint accuracy." (*Arson Investigation, supra*, 497 F.Supp.3d at p. 361.)

" 'Hence, the touchstone of reasonableness under the Fourth Amendment is sufficient probability, not certainty.' " (*Ibid.*) Thus, in assessing whether a geofence warrant passes Fourth Amendment scrutiny, "[t]he 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." (*Id.* at p. 362.)

The court noted it is not unusual for "one uninvolved individual's privacy rights [to be] indirectly impacted by a search" (Arson Investigation, supra, 497 F.Supp.3d at p. 361.) "[W]hen a court authorizes the search of a house, the entire house is subject to the search, ... such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children." (Ibid.) And, "when a court authorizes the search of an individual's email account," the search "includes private emails sent by non-perpetrators that were not intended to be seen by the government . . . but are nonetheless viewed by government agents in the search for evidence of the crime." (Ibid.) Searches of cell phones reveal "calendar entries of meetings, events, and text messages with uninvolved individuals" and pictures identifying the locations of these individuals. (Ibid.) Thus, "it is nearly impossible to pinpoint a search where only the perpetrators' 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." (Id. at pp. 361-362.)

The court concluded that the proposed geofence warrant described the places to be searched with sufficient particularity "because it narrowly identifie[d] the place[s] by

time and location," and it was "not overbroad in scope." (*Arson Investigation, supra*, 497 F.Supp.3d at p. 357.) The court treated physical location and "scope" as distinct, but in discussing the scope of the proposed warrant, the court discussed how investigators had worked to narrow the *geographic* scope of the warrant to exclude areas where uninvolved individuals could be located. (*Id.* at pp. 355-358.) The proposed geofences excluded residences and commercial buildings along the roadways, and surveillance videos showed few vehicles other than the suspect vehicles on the roadways near the times of the arsons. (*Id.* at pp. 358-359.) Thus, the government "satisfied overbreadth considerations by ensuring" there was "probable cause that location data of perpetrators, co-conspirators and witnesses will be collected from Google, and that the scope of the warrant would not result in the collection of a broad sweep of data from uninvolved individuals for which there is no probable cause." (*Ibid.*)¹⁰

The court next addressed the Google production protocol and found it "of no matter" to the constitutionality of the warrant under the Fourth Amendment, given that the government had "established probable cause to seize all location and subscriber data within the geofence locations." (*Arson Investigation, supra*, 497 F.Supp.3d at p. 362.) In light of the probable cause showing, it was immaterial to the constitutionality of the

¹⁰ The court acknowledged that location data has a margin of error of around 20 meters that could cause devices outside of a geofence to appear to be inside, and vice versa. (*Arson Investigation, supra*, 497 F.Supp.3d at p. 360.) But the court said the margin of error did not invalidate the warrant because "only reasonableness is required, not surgical precision. A margin of error, in light of the remarkable accuracy of Google location data, is reasonable given the nature of the evidence being sought and what is possible with the technology at issue." (*Id.* at p. 361.)

warrant whether the government chose to seize all location data and subscriber information for all devices located in the geofences. (See *ibid*.) The court acknowledged, however, that "a constitutionally permissible warrant does not leave open the opportunity for the government agent to use his discretion in conducting a search or seizure." (*Ibid*., citing *Stanford v. Texas, supra*, 379 U.S. at pp. 485-486.) Thus, the court did not sanction the Fourth Amendment constitutionality of the multi-step protocol in cases where no probable cause is shown to seize all location data and identifying information for all devices located in the geofences. (*Arson Investigation*, at p. 362.)

Here, the geofence warrant was a model of particularity in geographic scope and time period. (*Arson Investigation, supra*, 497 F.Supp.3d at pp. 357-358.) The "initial search parameters" specified a "target location" and a "date and time period." Pursuant to Google's multi-step production protocol, the warrant sought location data for a 22-minute period, between 10:00 p.m. and 10:22 p.m., on October 29, 2019—the date and time period encompassing the shooting. Like the warrant application in *Arson Investigation*, the warrant sought location data "tailored and specific to the time of the [crime] only." (*Id.* at p. 357.)

The target location was likewise narrowly tailored to "minimize the potential for capturing location data for uninvolved individuals." (*Arson Investigation, supra*, 497 F.Supp.3d at p. 353.) The target location was limited to the front yard of Jovany R.'s house, where the shooting occurred, and the street in front of the house, for the length of two houses in each direction, where the two suspects were seen fleeing after the shooting. Thus, the target location was "narrowly crafted to ensure that location data, with a fair

probability, [would] capture evidence of the crime only." (*Id.* at p. 357.) Additionally, because the warrant sought first-stage location data after 10:00 p.m. in a suburban, residential neighborhood, it was likely that any individuals traversing the geofence were either suspects or witnesses to the shooting. (*Id.* at p. 358.) The initial time and location parameters of the warrant were reasonably specific; in fact, they were as narrowly tailored as they could have been to capture *only* the location data and identifying information of the suspects and potential witnesses to the shooting.

Given the narrowly tailored initial search (time and location) parameters of the warrant, the multi-step production protocol, which, as applied in executing the warrant, was constitutionally immaterial to the extent it authorized a search for location data and identifying information associated with devices located outside the geofence, at step two of the production protocol. In his testimony at the preliminary hearing, Investigator Deanne explained how the geofence warrant was executed and what information he received at each step of the production protocol.¹¹

The stage-one information, the anonymized list, showed five device IDs in the geofence during the 22-minute period, and that two of the five device IDs were at Jovany R.'s house for five to seven minutes during the 22-minute period. At stage two, Deanne requested and obtained additional location data for the two device IDs, showing where the two device IDs travelled after they were in the geofence. The stage-two information

¹¹ In his testimony, Investigator Deanne described the Google production protocol as a three-stage process. The warrant affidavit described the process in five steps, but the affidavit's description is consistent with Investigator's Deanne's description of the three-stage process.

showed that the two device IDs "ultimately" traveled east on Limonite, past the gas station where surveillance video showed a silver car, similar to the car Samuel R. said the shooter left in after the shooting, traveling east on Limonite after the shooting.

Thus, at stage two, Deanne received location data for the two device IDs outside of the initial time and location parameters, or the initial search parameters, of the geofence. Deanne then requested stage-three identifying information for the two device IDs and discovered they were associated with a single device and two Gmail accounts, both associated with Price.

The stage-two information that Deanne was authorized to receive under the production protocol did not render the warrant insufficiently particular under the Fourth Amendment. As in *Arson Investigation*, the warrant showed probable cause to seize all location data and identifying information for all devices traversing the geofence. (*Arson Investigation, supra*, 497 F.Supp.3d at p. 362.) And, because the additional location data that Deanne was authorized to receive at stage two was based on the location data produced at stage one, the Google production protocol, as applied, did not vest Deanne with discretion to conduct a search and seizure unsupported by the probable cause showing in the warrant. (*Ibid; Stanford v. Texas, supra*, 379 U.S. at pp. 481, 485-486.)

Price does not challenge the warrant affidavit's showing of probable cause to believe every individual who was likely to be located in the geofence was a suspect or a witness to the shooting. (*Pharma II, supra*, 481 F.Supp.3d at pp. 751-753 [comparing geofence warrants to " 'all persons' " warrants that require probable cause to believe " 'all persons present' " in the place to be searched participated in criminal activity].) It

is difficult to imagine how the warrant could have been more narrowly tailored to focus on identifying only the suspects and minimizing the potential for seizing location data and identifying information associated with devices carried by uninvolved individuals. (*Arson Investigation, supra*, 497 F.Supp.3d at p. 356.)

Relying on *Chatrie, supra*, 590 F.Supp.3d 901, Price argues that Google's threestep production protocol renders the warrant insufficiently particular under the Fourth Amendment. *Chatrie* is distinguishable. Unlike the warrant in this case and the approved warrant application in *Arson Investigation, Chatrie* involved a geofence warrant that lacked "particularized probable cause" to believe every individual in the geofence was a suspect or witness to the crime under investigation. (*Chatrie*, at pp. 929-930; *Pharma II, supra*, 481 F.Supp.3d at pp. 751-753.) Thus, the warrant in *Chatrie* was overbroad in the first place, before the Google production protocol allowed the executing officer discretion to obtain location data and identifying information for individuals traveling outside the geofence.

In *Chatrie*, the court considered a motion to suppress evidence obtained pursuant to a geofence warrant. (*Chatrie, supra*, 590 F.Supp.3d at p. 906.) The court ultimately denied the suppression motion based on the good faith exception to the exclusionary rule. (*Id.* at pp. 905, 937-940.) But the court concluded that the geofence warrant was invalid because it lacked both "particularized probable cause" and sufficient particularity under Fourth Amendment standards. (*Id.* at pp. 927-935.) The court heard extensive evidence on the suppression motion, including testimony and declarations from Google employees, describing Google's three-stage production protocol, and Google's policies in

implementing the protocol. (*Id.* at pp. 906-907, 914-917.) Google also filed an amicus brief in the case. (See *id.* at pp. 906-907 & fn. 5.) According to the record in *Chatrie*, Google received its first geofence warrant in 2016, and, in 2019, Google received "'around 9,000 total geofence requests.'" (*Id.* at p. 914.)

Chatrie includes an in-depth discussion of location data, including how Google collects and stores location data and the margin of error for location data. (*Id.* at pp. 905-913.) The record in *Chatrie* shows that Google works with law enforcement to limit the additional location data and identifying information that Google produces at stages two and three of the production protocol, but there were no practical limitations on the additional location data and identifying information that Google would produce pursuant to the protocol. (*Id.* at pp. 916-917, 934-935.)

Through the warrant in *Chatrie*, the government was seeking to identify a single suspect in a bank robbery. (*Chatrie*, *supra*, 590 F.Supp.3d at p. 916.) Surveillance video showed the suspect entering the bank building holding a cell phone. (*Id.* at p. 917.) The geofence was circular, with a diameter of 300 meters—longer than three football fields "in an urban environment," and included a church. (*Id.* at p. 918.) "All told, the geofence encompassed 17.5 acres." (*Ibid.*) The warrant sought location data for every device present within the geofence for one full hour, on the day of the robbery, pursuant to Google's three-step production protocol. (*Id.* at pp. 918-919.)

Chatrie first explained that the warrant was not supported by sufficient probable cause because it did not show probable cause to believe that *every individual* or Google account holder in the geofence was a suspect in the robbery. (*Chatrie, supra,*

590 F.Supp.3d at pp. 926-929.) Warrants that "authorize the search of every person within a particular area must establish probable cause to search every one of those persons." (*Id.* at p. 927.) That is, such warrants "must establish probable cause that is 'particularized with respect to the person to be searched or seized.'" (*Id.* at p. 929, quoting *Maryland v. Pringle* (2003) 540 U.S. 366, 371; accord *Pharma II, supra*, 481 F.Supp.3d at p. 751-753, citing *Ybarra v. Illinois* (1979) 444 U.S. 85, 91 [" '[A] warrant to search "all persons present" for evidence of a crime may only be obtained when there is reason to believe that *all* those present will be participants in the suspected criminal activity '"].)

The warrant in *Chatrie* further authorized the government to obtain location data "for yet another hour" for devices that traveled outside the geofence, "with no geographical restrictions" on the additional location data, and with no showing that all or even a substantial number of the individuals to be searched had participated in or witnessed the crime. (*Chatrie, supra,* 590 F.Supp.3d at p. 929.) The warrant "swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." (*Id.* at pp. 929-930.) Under the Fourth Amendment, it was unreasonable to request so much location data. (*Id.* at p. 930.)¹²

¹² The overbroad geofence warrant in *Chatrie* is similar to the overbroad geofence warrant applications in *Pharma I*, *Pharma II*, and *Kansas Federal Crimes*. In these cases, the warrant applications were denied because they would have authorized the government to search the location data and identifying information of large numbers of uninvolved individuals for whom there was no probable cause to believe were suspects or witnesses to the crimes under investigation. (*Pharma I, supra*, 2020 U.S.Dist. Lexis 165185 at pp. *7-*8; *Pharma II, supra*, 481 F.Supp.3d at pp. 742-745; *Kansas Federal [footnote continued on next page]*

The *Chatrie* court rejected the government's argument that the Google three-step production protocol "cure[d] any defects with the warrant's particularized probable cause." (Chatrie, supra, 590 F.Supp.3d at pp. 933-934.) Observing that the particularity requirement " 'leaves the executing officer with no discretion as to what to seize' " (id. at p. 934), the court concluded that steps two and three of the production protocol gave the government "unbridled discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users" or minimize the amount of location data and identifying information obtained for uninvolved individuals (*ibid*.). The warrant contained no "objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny." (Ibid.) Instead, the warrant gave the government "unchecked discretion to seize more intrusive and personal data with each round of requests-without ever needing to return to a neutral and detached magistrate for approval." (Ibid.) Thus, the court concluded that steps two and three of the protocol did not "supply this warrant with particularized probable cause, as these steps independently fail under the Fourth Amendment's particularity requirement." (Id. at p. 935.)

Crimes, *supra*, 542 F.Supp.3d at p. 1157.) In contrast, the warrant applications in *D.C. Federal Crimes* and *Texas Federal Crimes*, and the warrants in *Rhine* and *Smith*, are more like the warrant application in *Arson Investigation* and the warrant in this case: they were not overbroad; they did not "have the potential of sweeping up the location data of large numbers of uninvolved persons"; and they were " 'confined to the breadth of the probable cause that support[ed]" them. (*D.C. Federal Crimes, supra*, 579 F.Supp.3d at pp. 81, 85; *Rhine, supra*, 2023 U.S. Dist.Lexis 12308 at pp. *95-*98; *Smith*, *supra*, 2023 U.S.Dist. Lexis 22944 at pp. *18-*24; *Texas Federal Crimes, supra*, 2023 U.S.Dist. Lexis 33651 at pp. *9,*33-*40.)

Price argues that the geofence warrant suffers from the same particularity deficiency as the geofence warrant in *Chatrie*. He argues that, at steps two and three of the Google production protocol, the warrant gave the executing officer unbridled or unchecked discretion to demand additional location data for devices traveling beyond the initial time and location parameters of the geofence and identifying information for all devices identified in step one, without any judicial oversight at stages two and three.

But as Arson Investigation demonstrates, these potentially overbroad aspects of the Google production protocol are constitutionally immaterial when, as here, the warrant shows probable cause to believe that all persons, or nearly all persons, likely to be located in the geofence (the initial time and location parameters of the search) are suspects or witnesses to the crime or crimes under investigation. (Arson Investigation, supra, 479 F.Supp.3d at pp. 362-363.) "[T]he Constitution 'is not so exacting' as to require the 'eliminat[ion of] all discretion of the officers executing the warrant.'" (D.C. Federal Crimes, supra, 579 F.Supp.3d at p. 76.) The degree of required particularity " 'turns on what was realistic or possible in this investigation," " and " 'a broader sweep' can be lawful 'when a reasonable investigation cannot produce a more particular description' of the things to be seized prior to obtaining and executing the warrant." (Ibid.) "Ultimately, '[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed to promote legitimate governmental interests." '" (Ibid.) The geofence warrant in this case satisfied the Fourth Amendment standard of reasonableness.

B. Traversal Claims

A motion to traverse a warrant challenges the completeness and truthfulness of the warrant affidavit's probable cause showing. (Franks v. Delaware (1978) 438 U.S. 154, 155-156.) Generally, in order to traverse a warrant, the defendant must show that "(1) the affidavit included a false statement made 'knowingly and intentionally, or with reckless disregard for the truth,' and (2) 'the allegedly false statement is necessary to the finding of probable cause." (People. v. Hobbs (1994) 7 Cal.4th 948, 974, quoting Franks v. Delaware at pp. 155-156.) If the defendant makes this showing, " 'the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." (*People v. Lazarus* (2015) 238 Cal.App.4th 734, 768, quoting Franks v. Delaware, at pp. 155-156.)

Likewise, a defendant who challenges a warrant based on factual omissions in the affidavit must show that the omissions were material to the probable cause determination. (*People v. Panah* (2005) 35 Cal.4th 395, 456.) Facts omitted from a warrant affidavit are "not material" if "there is no 'substantial possibility they would have altered a reasonable magistrate's probable cause determination,' and their omission did not 'make the affidavit[s] *substantially misleading*.'" (*People v. Eubanks* (2011) 53 Cal.4th 110, 136.) "We review the denial of a *Franks* hearing de novo." (*People v. Panah*, at p. 457.)

Price claims the geofence warrant affidavit omitted material facts showing there was no evidence that the two murder suspects knew about the marijuana grow in Jovany R.'s house. The affidavit stated, "Deputies conducted a safety sweep of the residence and located what appeared to be a marijuana grow with numerous marijuana plants in varying stages of maturation, as well as large amounts of processed marijuana throughout the residence. [¶] Based on the statement the suspects made prior to the shooting ["Don't move"] and the large amounts of marijuana within the residence, it appears the suspects had knowledge there would be large amounts of marijuana at the residence." Price notes the affidavit failed to state that "the home looked normal and the marijuana grow was not visible from outside of the home," and that the affidavit did not point to any evidence (besides the shooter's "Don't Move" statement) that the two suspects knew about the marijuana grow.

The magistrate at the preliminary hearing, and the superior court in ruling on the section 995 motion, found these omissions immaterial to the issuing magistrates' probable cause determination for all of the 11 challenged warrants, including the geofence warrant. On de novo review, we agree that these omissions were immaterial. Whether the suspects knew there was a marijuana grow in the house is relevant to whether the suspects had a motive for the shooting (CALCRIM No. 370), but motive is not an element of murder. (§§ 187-189.) Even if the affidavit had explained that the marijuana grow was not visible from the outside of the house or that there was no direct evidence the suspects knew there was a marijuana grow in the house or garage, the

affidavit showed probable cause to believe Jovany R. was murdered by two unknown suspects and that Google had information that would reveal the suspects' identities.¹³ C. *The Good Faith Exception to the Exclusionary Rule Precludes Suppression of the Geofence Warrant Evidence and Its Fruits*

The exclusionary rule is not a personal constitutional right; nor is it designed to "'redress the injury' occasioned by an unconstitutional search." (*Davis v. United States* (2011) 564 U.S. 229, 236 (*Davis*); *Chatrie, supra*, 590 F.Supp.3d at p. 937.) It is "'a judicially created remedy designed to safeguard Fourth Amendment rights'" by deterring "police misconduct" rather than by punishing "the errors of judges and magistrates." (*United States v. Leon* (1984) 468 U.S. 897, 906, 909, 916 (*Leon*); *Herring v. United States* (2009) 555 U.S. 135, 144 [The rule "serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."].) Given that the purpose of the rule "is to deter future Fourth Amendment violations" by law enforcement officers, "[w]here suppression fails to yield appreciable deterrence,' exclusion is 'clearly... unwarranted.'" (*Davis*, at pp. 236-237.)

In *Leon*, the high 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, supra*,

¹³ Price also claims the geofence warrant affidavit should be traversed because it did not state that a gun was found on Jovany R.'s person after the shooting. This is not so. The affidavit stated, "deputies . . . located a Beretta .40-caliber handgun on the victim's person."

238 Cal.App.4th at p. 766, quoting *Leon*, supra, 468 U.S. at pp. 920, 922; *Meza*, *supra*, 90 CalApp.5th at p. 543) Thus, under the good faith exception, the "exclusionary rule does not bar the use in the prosecution's case-in-chief of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause." (*People v. Lim* (2000) 85 Cal.App.4th 1289, 1296, citing *Leon*, at p. 922.)

There are four "limited situations" in which reasonable, good faith reliance on the warrant cannot not be established and suppression remains appropriate: "(i) the issuing magistrate was misled by information that the officer knew or should have known was false; (ii) the magistrate 'wholly abandoned his judicial role'; (iii) the affidavit was ' "so lacking in indicia of probable cause" ' that it would be ' "entirely unreasonable " ' for an officer to believe such cause existed; and (iv) the warrant was so facially deficient that the executing officer could not reasonably presume it to be valid." (*People v. Camarella* (1991) 54 Cal.3d 592, 596, quoting *Leon, supra*, 468 U.S. at p. 923. Price suggests the third and fourth limited situations apply.

We review the application of the good faith exception de novo, applying "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. Lazarus, supra,* 238 Cal.App.4th at pp. 766-767.) In other words, we ask whether a reasonably well trained officer " 'would have *known* that his affidavit failed to establish probable cause and that he should not have applied for the warrant.'" (*People v. Camarella, supra,*

54 Cal.3d at pp. 605-606.) "[T]he government has the burden to prove facts warranting application of the good faith exception." (*People v. Willis* (2002) 28 Cal.4th 22, 37.)

When the warrant was issued on November 7, 2019, "geofence warrants were still a novel investigative tool," and "there were no published cases anywhere in the country, let alone in California, analyzing the constitutionality of geofence warrants." (*Meza*, *supra*, 90 Cal.App.5th at p. 544.) And, although *Pharma I* and *Pharma II*, were issued in July and August 2020, before Deanne received stage three identifying information from Google on September 14, 2020, these cases did not reasonably indicate that the warrant was invalid or that Deanne should have obtained a further warrant before obtaining the stage two or stage three information from Google. (*Pharma I, supra*, 2020 U.S.Dist. Lexis 165185; *Pharma II, supra*, 481 F.Supp.3d 730.) The cases involved significantly overbroad geofence warrant applications that would have allowed the government to seize location data and identifying information for numerous individuals who had no connection to the crimes under investigation. In contrast, the geofence warrant here was both narrowly drawn *and executed* to exclude such data.

Thus, from the time the warrant was issued through its execution, a well-trained officer in Investigator Deanne's position had no reason to believe the warrant affidavit failed to establish probable cause, that Deanne should not have applied for the warrant, or that Deanne should have sought a further warrant before seeking stage two or stage three information from Google. Nor was the warrant so facially deficient, at any time during its execution, that a well-trained officer could not have reasonably presumed it to be valid. The record shows Investigator Deanne acted in good faith in drafting the warrant,

in relying on the issuing magistrate's probable cause determination, and in seeking and obtaining from Google only so much location data and identifying information as was reasonably necessary to identify the suspects and possible witnesses to the shooting. Thus, even if the geofence warrant is invalid under the Fourth Amendment, the good faith exception applies. No deterrent purpose would be served by suppressing the geofence warrant evidence or its fruits.¹⁴

D. CalECPA Claims

Price claims the geofence warrant violated CalECPA's particularity requirement (§ 1546.1, subd. (d)(1)) and, in executing the warrant, the Riverside County Sheriff's Department failed to give notice of the warrant in accordance with the notice provisions of CalECPA (§ 1546.2). For these violations, Price claims that the CalECPA's remedy provision requires the suppression of the warrant evidence and its fruits. (§ 1546.4.)

1. <u>CalECPA Applies to Geofence Warrants</u>¹⁵

Subject to exceptions not applicable here, CalECPA requires a government entity to obtain a search warrant (§ 1523 et seq.) to do any of the following: (1) "Compel the

¹⁴ Other courts applied the good faith exception to geofence warrant evidence based in part on (1) the novelty of geofence warrants as investigative tools, and (2) the lack of controlling authority addressing the constitutionality of geofence warrants at the time the warrants were issued and executed. (*Meza, supra,* 90 Cal.App.5th at pp. 543-545; *Chatrie, supra,* 590 F.Supp.3d at pp. 937-938; *Carpenter, supra,* 2023 U.S.Dist. Lexis 64948 at pp. *33-*34; *Smith, supra,* U.S.Dist. Lexis 22944 at pp. *36-*38; see *Rhine, supra,* 2023 U.S.Dist. Lexis 12308 at pp *108-*109.)

¹⁵ CalECPA was enacted effective January 1, 2016 (Stats. 2015, ch. 651, § 1) and was most recently amended effective January 1, 2017 (Stats. 2016, ch. 541, § 3.5). For an extensive discussion of the history, purpose, and provisions of CalECPA, see *[footnote continued on next page]*

production of or access to electronic communication information from a service provider," (2) "Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device," or (3) "Access electronic device information by means of physical interaction or electronic communication with the electronic device." (§ 1546.1, subds. (a)-(c).)¹⁶

CalECPA does not address geofence warrants specifically (§§ 1546 to 1546.5), but it applies to geofence warrants. In the words of CalEPCA, a geofence warrant seeks to compel the production of, or access to, electronic communication information from a service provider, and to compel the production of or access to electronic device information from anyone other than the authorized possessor of an electronic device.

Freiwald, At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA) (2018) 33 Berkeley Tech. L.J. 131 (hereafter Freiwald).

¹⁶ CalECPA defines several terms for purposes of its provisions. (§ 1546, subd. (a).) A "'service provider' means a person or entity offering an electronic communication service." (§ 1546, subd. (j).) "'Electronic communication' means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system." (§ 1546, subd. (c).) "'Electronic communication service' means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as intermediary in the transmission of electronic communications, or stores electronic communication information." (§ 1546, subd. (e).)

"'Electronic communication information' means "any information about an electronic communication or the use of an electronic communication service," including "the location of the sender or recipients at any point during the communication." (§ 1546, subd (d).) "Subscriber information" is specifically excluded from the definition of " electronic communication information.' " (*Ibid.*) " '[E]lectronic device information' means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device." (§ 1546, subd. (g).) " 'Electronic information." (§1546, subd. (h).)

(§ 1546.1, subd. (b).) A geofence warrant also seeks to access electronic device information by means of electronic communication with the device. (§ 1546.1, subd. (c).)

2. <u>The Geofence Warrant Did Not Violate CalECPA's Particularity Requirement</u>

CalECPA requires "[a]ny warrant for electronic information" to "describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and types of information sought." (§ 1546.1, subd. (d)(1); see § 1525.) Price claims the geofence warrant violated this particularity requirement because it did not specify "the target individual or accounts, the applications or services covered," or sufficiently describe "the types of information sought." (§ 1546.1, subd. (d)(1).) As we explain, these arguments disregard the plain language of section 1546.1, subdivision (d)(1), and the types of information the geofence warrant sought.

The language of section 1546.1, subdivision (d)(1), is plain and unambiguous and controls our interpretation of the statute. (*People v. King* (2006) 38 Cal.4th 617, 622 [" '[I]f the plain, commonsense meaning of a statute's words is unambiguous, the plain meaning controls.' "].) The statute only requires a warrant for electronic information to describe the information it seeks by "*specifying, as appropriate and reasonable*, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought" (§ 1546.1, subd. (d)(1), italics added.) Thus, not every warrant for electronic information must describe the information it seeks in

terms of each of the four categories of information listed in the statute. The warrant is only required to include such descriptions "as appropriate and reasonable." $(Ibid.)^{17}$

And here, it was not "appropriate and reasonable" for the geofence warrant to specify "the target individuals or accounts." (\$1546.1, subd. (d)(1).) A geofence warrant *seeks to identify* target individuals through location data generated from, and accounts and identifying information associated with, devices located in the geofence. The identities of the "target individuals" and their "accounts" with the service provider are unknown to the agency executing a geofence warrant. Thus, it was not "appropriate and reasonable" for the sheriff's department to specify "the target individuals or accounts" in describing the information sought in the geofence warrant.¹⁸

Price next argues that the geofence warrant violated CalECPA's particularity requirement by not specifying the "applications or services covered" by the warrant. (§ 1546.1, subd. (d)(1).) Price points out that the warrant directed Google "to query all location data within the geofence for the specified time *without reference to the*

¹⁷ Section 1546.1, subdivision (d), expressly contemplates that a "court may determine that it is not appropriate to specify time periods" in a warrant to access electronic device information through physical interaction with or electronic communication with a device (§ 1546.1, subd. (c)) "because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched" (§ 1546.1, subd. (d)(1)).

¹⁸ As noted in *Meza*, "CalECPA specifially contemplates a scenario where there is 'no identified target of a warrant.'" (*Meza, supra,* 90 Cal.App.5th at pp. 545-546.) When there is no identified target, CalECPA allows the entity executing the warrant to serve the warrant on the Department of Justice (§ 1546.2, subd. (c)) "because notice of the warrant cannot be served upon any individual." (*Meza,* at p. 546.) Thus, "the failure to specify an individual's name or other identifying information" does not render a geofence warrant invalid under CalECPA. (*Meza,* at p. 546.)

applications or services utilized to provide that data to Google," and that Investigator Deanne "admitted he had no idea what applications or services might be in use on the unknown target's device that would produce the location data sought."

This argument confuses the electronic information the warrant sought (location data emitted from and identifying information associated with devices in the geofence) with applications or services that the devices or the service provider (Google) used to obtain, store, and retrieve the location data and identifying information. These applications and services were merely incidental to the "type of information sought," the location data and identifying information. As the Meza court explained: "With a geofence warrant, . . . 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." (Meza, supra, 90 Cal.App.5th at p. 546 [rejecting claim of CalECPA particularity violation].) Thus, it was not appropriate and reasonable for the geofence warrant to specify the applications or services that the devices or Google used to obtain, store, and retrieve "types of information sought," the location data and identifying information. (§ 1546.2, subd. (d)(1).)

Price also claims that the geofence warrant insufficiently described "the types of information" sought (§ 1546.1, subd. (d)(1)), but Price does not explain what types of information the warrant sought that it failed to sufficiently describe, or how the warrant was unclear or ambiguous in describing the types of information it sought. The warrant included a detailed description of the types of information it sought, summarized here as

location data and identifying information associated with devices found to be traversing the geofence (specified by date, time, and geographical location), to be produced in accordance with Google's production protocol. There is no evidence that Google misinterpreted the types of information the warrant sought. Thus, Price has not shown that the warrant insufficiently described the types of information sought. (*Ibid*.)

Price further suggests that any warrant for electronic information that violates the Fourth Amendment's particularity requirement necessarily, and independently, violates CalECPA's particularity requirement. (§ 1546.1, subd. (d)(1).) Price does not explain how a Fourth Amendment particularity infirmity in a warrant necessarily violates section 1546.1, subdivision (d)(1) (Meza, supra, 90 Cal.App.5th at pp. 545-546 [rejecting similar claim]), and nothing in the language of the statute (\S 1546.2, subd. (d)(1)) supports Price's interpretation. Price also suggests that CalECPA's remedies provision (§ 1546.4, subd. (a)), which allows "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 [CalECPA]," means that a Fourth Amendment particularity violation also violates CalECPA's particularity requirement. (§ 1546.4, subd. (a), italics added.) The language of the remedies provision (§ 1546.4, subd. (a)) does not support this interpretation. To the contrary, the remedies provision refers to Fourth Amendment and CalECPA violations as separate violations, by its use of the disjunctive term "or."

(§ 1546.4, subd. (a).) The remedies provision does "nothing more than expressly preserve an individual's existing rights under the federal Constitution." (*Meza*, at p 546.)

3. <u>CalECPA's Notice Provisions</u>

(a) Notice to identified targets

Section 1546.2 requires a government entity that executes a warrant for electronic information to "*serve* upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, *the identified targets of the warrant* ..., *a notice* that informs the recipient that information about the recipient has been compelled or obtained, and states with reasonable specificity the nature of the government investigation under which the information is sought." (§ 1546.2, subd. (a)(1), italics added.) The notice must include a copy of the warrant and must be "provided contemporaneously with the execution of [the] warrant." (*Ibid.*)

(b) Delayed notice to identified targets

"[T]he government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an *adverse result*, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days." (§ 1546.2, subd. (b)(1), italics added.) An " 'adverse result' " means "[d]anger to the life or physical safety of an individual," "[f]light from prosecution," "[d]estruction of or tampering with evidence," "[i]ntimidation of potential witnesses," or "[s]erious jeopardy

to an investigation or undue delay of a trial." (§ 1546, subd. (a).) The court may grant successive extensions of the notice delay period, of up to 90 days for each extension, based on a continued showing of an adverse result. (§ 1546.2, subd. (b)(2).)

(c) *Identified target to be served following delayed notice period*

Upon the expiration of the delayed notice period, including extensions, the government entity is required to serve the identified target or targets of the warrant with all of the information described in section 1546.2, subdivision (a)(1) [notice of the warrant, including the nature of the investigation, and a copy of the warrant], together with copies of or a summary of the information obtained pursuant to the warrant, "including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual." (§ 1546.2, subd. (b)(3).)

(d) Service on the California Department of Justice

If there is no identified target of a warrant, then within three days of the execution of the warrant, the government entity is required to "submit to Department of Justice" the information described in section 1546.2, subdivision (a)—notice of the warrant, including the nature of the investigation, and a copy of the warrant (§ 1546.2, subd. (c)). If an order delaying notice of the warrant has been issued (§ 1546.2, subd. (b)(1)-(2)), then, upon the expiration of the notice delay period, including extensions, the government is required to serve the department with notice of the warrant, including the nature of the investigation, a copy of the warrant, and a copy or summary of all electronic information

obtained pursuant to the warrant. (§ 1546.2, subd. (c).) The department is required to "publish all those reports on its Internet Web site within 90 days of receipt," but it "may redact names or other personal identifying information from the reports." (*Ibid.*)

4. <u>The CalECPA Notice Violations</u>

In the geofence warrant, the People sought an order delaying the People's obligation to serve "identified targets" of the warrant with notice of the warrant under CalECPA for a period of 90 days. (§ 1546.2, subds. (a), (b)(2).) The warrant claimed the delay was justified because "providing prior notice to the target/ party" could lead to all of the adverse results listed in section 1546, subdivision (a); that is, it could endanger lives or physical safety, lead to flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, and it could seriously jeopardize the investigation. The issuing magistrate found "reason to believe that contemporaneous notification of the existence" of the warrant "may have an adverse result on the on-going criminal investigation" and granted the 90-day notification delay in issuing the warrant on November 7, 2019.¹⁹ (§ 1546.2, subd. (b)(2).)

¹⁹ The warrant ordered Google to "delay notification of the subscribers or to any other person, for a period of 90 days unless otherwise directed by the court," but the warrant did not expressly grant the People's request for a 90-day order delaying notification of identified targets of the warrant with notice of the warrant. (§ 1546.2, subds. (a), (b)(2).) The omission in the order must have been inadvertent, and the parties agree that the requested 90-day notification delay was granted. CalECPA contemplates that "an order delaying notification *and* prohibiting the party providing information from notifying any other party that information has been sought" will be made in the same order. (§ 1546.2, subd. (b)(2), italics added.) An order prohibiting the party providing information from disclosing that the information is being sought under the warrant would be ineffective without an order delaying notification of the target parties, and vice versa.

The People did not seek any extensions of the order delaying notice; thus, the 90day notice delay period expired on February 5, 2020. (§ 1546.2, subd. (b)(2).) There were no "identified targets" of the warrant from the time it was issued on November 7, 2019 until September 14, 2020, when Investigator Deanne received the identifying information linking Price to the shooting. But, on or around January 29, 2020, during the 90-day notice delay period, Deanne received the anonymized list of five device IDs from Google, the stage one information. Deanne received the stage two information, showing two device IDs traveling outside the geofence, in March 2020.

Thus, by February 6, 2020, upon the expiration of the 90-day notice delay period, the People were required to serve the Department of Justice with the information listed in section 1546.2, subdivsion (b)(3) (notice of the warrant including the nature of the investigation and a copy of the warrant), together with the stage one information, in the form of "a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual." (§ 1546.2, subds. (a), (b)(3).) By failing to submit this information to the Department of Justice by February 6, 2020, the People violated CalECPA's notice requirements. (§ 1546.2, subd. (c).)

The People concede Price was not properly served with notice of the warrant, or the information obtained pursuant to the warrant (stage one, two, and three information) when Price was arrested in December 2020. (§ 1546.2, subds. (a), (b)(3), (c).) At that

time, Investigator Deanne gave Price what Deanne called a "service copy" of the warrant, without the affidavit and probable cause statement, and gave Price a verbal summary of the geofence information that the sheriff's department had obtained pursuant to the warrant. The service copy and verbal summaries did not include all of the information with which Price was required to be served, once he was identified as a target of the warrant. (§ 1546.2, subd. (b)(3).) In the absence of an order extending the 90-day notice delay period, the government was required to notify Price of the warrant, the investigation, and the information obtained pursuant to the warrant, when the government identified Price as a target on September 14, 2020. (§ 1546.2, subds. (a), (b)(3), (c).)²⁰

5. <u>CalECPA Does Not Require the Suppression of Electronic Information</u>

Section 1546.4 specifies remedies for CalECPA violations. (§ 1546.4, subds. (a)-

(c).) As pertinent, the statute provides: "Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment . . . or of this chapter [(CalECPA; §§ 1546-1546.4)].^[21] The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) through (q), inclusive of Section 1538.5." (§ 1546.4, subd. (a).)

Price claims that section 1546.4, subdivision (a), is an "express suppression

²⁰ Section 1546.2, subdivision (b)(3), requires "the identified targets" to be served with notice of the warrant and any information obtained pursuant to the warrant "[u]pon expiration of the period of delay of the notification." (*Ibid.*) We interpret this provision to mean that identified targets must be served as soon as they are identified, if they are identified when no notice delay period is in effect.

²¹ Chapter 3.6 of title 12 of part 2 of the Penal Code comprises CalECPA (§§ 1546 to 1546.5).

requirement" which *requires* any electronic information obtained or retained in violation of CalECPA to be suppressed in a criminal proceeding. This interpretation of the statute is inconsistent with its plain language, which governs our interpretation. (*People v. King*, *supra*, 38 Cal.4th at p. 622; *Khan v. Los Angeles City Employees' Retirement System* (2010) 187 Cal.App.4th 98, 106.) The statute does not require the suppression of any electronic information. Rather, it *authorizes* any person in a trial, hearing, or proceeding to *move to suppress* any electronic information obtained or retained in violation of the Fourth Amendment or CalECPA. (§ 1546.4, subd. (a).) Its only directive is that the motion "be made, determined, and be subject to review" in accordance with the procedures set forth in section 1538.5, subdivisions (b) through (q)—the procedures governing suppression motions in criminal proceedings. (§ 1538.5.)

Interpreting section 1546.4, subdivision (a), as requiring courts to suppress electronic information obtained or retained in violation of CalECPA would be inconsistent with the plain language of similar CalECPA provisions, subdivisions (b) and (c) of section 1546.4. Subdivision (b) authorizes the Attorney General to bring a civil action to compel a government entity to comply with CalECPA. Subdivision (c) authorizes, "[a]n individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with [CalECPA], or the California Constitution or the United States Constitution," or "any other recipient of the warrant, order, or other legal process," to "petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of [CalECPA], or the California Constitution, or the United States Constitution." (§ 1546.4, subd. (c).)

Subdivisions (a), (b), and (c) of section 1546.4 are in pari materia—they each deal with electronic evidence obtained or retained in violation of CalECPA. Thus, they should be construed consistently with each other and according to their terms. (*Apartment Assn. of Los Angeles County, Inc. v. City of Los Angeles* (2009)

173 Cal.App.4th 13, 22.) [Statutes in pari materia should be " 'construed together' " and consistently with each other.].) None of these provisions direct a court to impose a particular remedy for a CalECPA violation; they leave the determination of the appropriate remedy to the court considering the suppression motion, civil action, or petition alleging the CalECPA violation.

Price suggests that section 1546.4, subdivision (a), requires a court to suppress electronic information obtained in violation of CalECPA because CalECPA was enacted by over two-thirds vote of each house of the Legislature, and is therefore excepted from the Right to Truth-in-Evidence provision of the California Constitution (Cal. Const., art. I, § 28, subd. (f)(2).) The Right to Truth-in-Evidence provision prohibits the suppression of relevant evidence in a criminal proceeding to an extent not compelled by the federal Constitution, unless the exclusion is authorized by a statute enacted by twothirds supermajorities in both houses of the Legislature. (*People v. Guzman* (2019) 8 Cal.5th 673, 679; *In re Lance W.* (1985) 37 Cal.3d 873, 886-887.)

In the summary of the bill that enacted CalECPA, the Legislative Counsel's Digest advised: "Because this bill *would exclude evidence* obtained or retained in violation of its provisions in a criminal proceeding, it requires a 2/3 vote of the Legislature." (Legis. Counsel's Dig., Sen. Bill. No. 178 (2015-2016 Reg. Sess.), ch. 651, italics added.) Price

points to this advisory in arguing that the Legislature intended section 1546.4, subdivision (a), to require the exclusion in criminal proceedings of evidence obtained or retained in violation of the Fourth Amendment or CalECPA. (See § 1546.4, subd. (a).) Again, the argument conflates a court's authority to suppress evidence based on a CalECPA violation (§§ 1538.5, 1546.4, subd. (a)), with a statutory directive to suppress such evidence. By *authorizing* the suppression of electronic evidence based on a CalECPA violation, section 1546.4, subdivision (a), *authorizes* the suppression of evidence to an extent not required by the federal Constitution. But nothing in CalECPA *requires* the suppression of electronic information in a criminal proceeding.

Price argues that the good faith exception to the exclusionary rule, which applies to Fourth Amendment violations (*Leon, supra*, 468 U.S. at p. 922), does not apply to electronic information obtained or retained in violation of CalECPA because section 1546.4, subdivision (a), overrides the good faith exception by requiring the suppression of the electronic evidence obtained or retained in violation of CalECPA. Nothing in subdivision (a) supports this interpretation. Subdivision (a) does not mention the good faith exception or prohibit its application to CalECPA violations. (§ 1546.4, subd (a).) As respondent superior court noted, "[i]nsofar as [Price's] claims encompass the argument that CalECPA does not permit good faith reliance on the warrant, [Price] has failed to show that the Legislature intended such a sweeping change to this well-established rule without express clarity. The Legislature is presumed to know existing law, including case law [citation], and nothing in CalECPA suggests that the legislation was intended to vitiate the rule of *Leon* and its progeny."

6. Suppression Is Not an Appropriate Remedy for the CalECPA Notice Errors

Given our conclusion that the superior court was not required to suppress the geofence warrant evidence and its fruits based on the CalECPA notice errors (§§ 1546.2, 1546.4), the next question we must determine is whether suppression of the geofence warrant evidence and its fruits is an appropriate remedy for the CalECPA notice violations. Section 1546.4 does not address what circumstances may justify the suppression of electronic information obtained pursuant to a warrant that violates the notice provisions of CalECPA. But in denying the renewed suppression motion, the superior court found guidance in the way courts have analyzed motions to suppress intercepted wire or electronic communications, and evidence derived from those communications, based on the government's violation of the reporting requirements for the wiretap order. (§ 629.72.) The wiretap context is instructive.

In *People v. Roberts* (2010) 184 Cal.App.4th 1149 (*Roberts*), the defendants moved to suppress evidence obtained pursuant to a wiretap order (§§ 629.52, 1538.5), on the ground the government failed to timely file periodic reports with the court overseeing the order in accordance with former section 629.60 (*Roberts*, at pp. 1178-1183). At the time the order was in effect, section 629.60 required the government to file reports with the court at intervals of not less than six days. (See *Roberts*, at p. 1179.)²²

²² Section 629.60 was amended effective January 1, 2011 to require the reports to be filed with the court "not less than one for each period of 10 days, commencing with the signing of the order" (Stats. 2010, ch. 707, § 8.) In 2019, the wiretap statutes (§§ 629.50 to 629.86) were repealed effective January 1, 2025. (§ 629.98; Stats. 2019, ch. 607, § 1.) CalECPA allows a government entity to obtain a wiretap order (§ 629.50 et *[footnote continued on next page]*

Section 629.72 authorizes a motion to suppress wiretap evidence. It mirrors section 1546.4, subdivision (a), in that it provides: "Any person in any trial, hearing, or proceeding, may move to suppress some or all of the contents of any intercepted wire or electronic communications, or evidence derived therefrom, only on the basis that the contents or evidence were obtained in violation of the Fourth Amendment of the United States Constitution or of this chapter [(§§ 629.50-629.98)]. The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in Section 1538.5." (§ 629.72.)

In determining whether the government's failure to timely file the six-day reports (§ 629.60) merited suppression of the wiretap evidence under section 629.72, *Roberts* applied the framework articulated in *People v. Jackson* (2005) 129 Cal.App.4th 129, 149 (*Jackson*) (*Roberts, supra*, 184 Cal.App.4th at p. 1183). Under the *Jackson* framework, "the defendant has the burden to show the evidence was obtained in violation of the Fourth Amendment or a provision of the Act, and that provision was intended to play a central role in the authorization and execution of wiretaps. The burden then shifts to the state to show the statutory purpose of the violated provision was achieved in spite of the error." (*Roberts*, at p. 1183, citing *Jackson*, at p. 160.)

The *Roberts* court concluded that "the timely filing requirement" of section 629.60 played "a central role in the wiretap statutory scheme," and the defendants met their burden of showing that the wiretap evidence was obtained in violation of section 629.60.

seq.), as an alternative to a warrant, to access electronic device information (1546.1, subd. (c)(2)).

(*Roberts, supra*, 184 Cal.App.4th at pp. 1184-1185.) "A central role," the court explained, "is one that affects the legality of the authorization or the execution of the wiretaps." (*Id.* at p. 1185.) Section 629.60 affected the legality of the wiretap order and the execution of the wiretaps because it "prescribe[d] timely and ongoing judicial oversight" of the order and "mandate[d] immediate termination of the wiretap" if "the judge [overseeing the wiretaps]" found that "progress ha[d] not been made, the [government's] explanation for the lack of progress [was] not satisfactory," or there was "no need" for "continued interception." (*Roberts*, at p. 1185.)

The court also concluded, however, that the government met its burden of showing that the purpose of section 629.60 was achieved despite the untimely filing of the wiretap reports. (*Roberts, supra*, 184 Cal.App.4th at pp. 1185-1186.) The court reasoned that the supervising judge *would not have* terminated the wiretap if the reports had been timely filed. (*Id.* at p. 1185.) The record showed that the government informed the supervising judge about developments in the case, and the judge "made the appropriate findings of necessity" to continue the wiretap order. (*Id.* at pp. 1185-1186.) Thus, the purpose of the reporting provision (§ 629.60) was achieved, despite the government's statutory violations in failing to timely file reports (*id.* at p. 1186).

Price has met his burden of making the necessary two-prong showing under the *Jackson* framework. (*Roberts, supra*, 184 Cal.App.4th at pp. 1183; *Jackson, supra*, 129 Cal.App.4th at p. 149.) He has shown that the government violated the notice provisions of CalECPA by failing to timely submit to the Department of Justice and serve Price with notice of the warrant, the nature of the investigation, and the copies or

summaries of the electronic information obtained. (§ 1546.2.) He has also shown that CalECPA's notice provisions play a central role in serving the purpose of CalECPA, which is to allow identified targets of warrants and others to protect the privacy of electronic information. (See Freiwald, *supra*, 33 *Berkeley Tech. L.J.* at pp. 133, 143-144.)

But the People have met their burden of showing that the CalECPA notice violations did not undermine the purpose of the CalECPA notice provisions. (*Roberts*, *supra*, at pp. 1185-1186.) The warrant was ordered sealed when it was issued on November 7, 2019, and it remained sealed until August 24, 2021, after Price filed his motion to suppress evidence at the preliminary hearing. The court also granted the government a 90-day delay in giving notice of the warrant under CalECPA. (§ 1546.2, subd. (b).) In light of the sealing order, the 90-day notice delay order, and the nature of the investigation, including that the warrant sought to identify two unknown murder suspects, a court would have granted successive 90-day extensions of the initial 90-day notice delay period (§ 1546.2, subd (b)), at least through the time of Price's arrest in December 2020, if the People had sought the extensions.

Notifying the Department of Justice or Price of the warrant, the nature of the investigation, and the electronic information obtained pursuant to the warrant at any time before Price was arrested in December 2020 may have seriously jeopardized the murder investigation and led to other adverse results. (§ 1546, subd. (a).) For the same reasons the magistrate ordered the warrant sealed, the magistrate would have granted the further extension requests. Because the notice violations did not undermine the purpose of the

notice provisions, the notice violations do not justify suppressing the geofence warrant evidence or its fruits. (*Roberts, supra*, 184 Cal.App.4th at p. 1185.)

V.

THE OTHER WARRANT EVIDENCE

Price claims the other 10 warrants seeking electronic information are invalid for the same reasons he argues the geofence warrant is invalid: (1) the warrants lacked sufficient probable cause and particularity under the Fourth Amendment; (2) the warrants violated CalECPA's particularity and notice requirements; and (3) the supporting affidavits for the warrants omitted material facts, requiring traversal.²³

A. Additional Background

Here, we list all 11 of the challenged warrants in chronological order, by their dates of issuance, beginning with the geofence warrant issued on November 7, 2019, and we summarize the electronic information sought in each warrant.²⁴

1. The geofence warrant, to Google for location data and identifying information pursuant to Google's production protocol, for devices located in the geofence specified in the geofence warrant, issued on November 7, 2019 (RI1107201919);

²³ Price originally moved to suppress evidence obtained pursuant to 15 warrants, but Price withdrew his motion as to four of the 15 warrants in his reply to the opposition to his original suppression motion at the preliminary hearing. Between October 30, 2019 and November 25, 2020, 19 warrants were issued in the Jovany R. murder investigation.

²⁴ When Price was arrested, Deanne gave Price "service copies" of the warrants listed as items 1, 6, 7, and 10. The 11 warrants were ordered sealed when each warrant was issued, and each warrant was ordered unsealed on August 26, 2021, after Price filed his motion to suppress evidence at the preliminary hearing.

2. To Google for "any search" on "any and all Google applications" for several variations of Jovany R.'s address on Homestead, between October 22, 2019 and October 30, 2019; issued on November 7, 2019 (RI1107201918);

3. To Facebook for all account information for Jovany R.'s user IDs and profiles between April 29, 2019 and January 6, 2020; issued on January 6, 2020 (RI106202013);

4. To Instagram for "all data" related to Jovany R.'s two Instagram accounts, between April 29, 2019 and January 6, 2020; issued on January 6, 2020 (RI106202012);

5. To Google for "all records" associated with three Gmail accounts in the names of two suspects in unrelated robberies (K.W. and T. H.), between June 1, 2019 and January 1, 2020; issued on May 8, 2020 (RI051120201) ("0201");

 To AT&T Wireless for "all records" associated with Price's cell phone number "4481" between August 1, 2019 and September 15, 2020; issued on September 15, 2020 (RI0915202024);

7. To Google for "all records" related to two Gmail accounts associated with Price, between August 1, 2019 and September 15, 2020; issued on September 15, 2020 (RI0915202023);

8. To AT&T for "all records" related to two phone numbers believed to be associated with Price's brother, C. Price, between August 1, 2019 and November 5, 2020; issued on November 5, 2020 (RI1105202017);

9. To T-Mobile for "all records" associated with a phone number believed to be associated with G. Contreras between August 1, 2019 and November 17, 2020; issued on November 17, 2020 (RI111820201);

 To AT&T for "all records" associated with Price's "4481" phone number for September 15 through November 25, 2020; issued on November 25, 2020 (RI12012024) ("2024");

11. To Apple for "all data" and content concerning an iphone found on Price at the time of his December 4, 2020 arrest, between January 1, 2019 and December 4, 2020; issued on December 4, 2020 (RI120820209) ("0209").

B. Under CalECPA, Price Has Standing To Challenge the Validity of All 11 Warrants

As a preliminary matter, we observe that CalECPA confers standing on Price to challenge the validity of all 11 warrants, on Fourth Amendment and CalECPA grounds, including the six warrants that targeted electronic information of persons other than Price, and that, therefore, did not implicate Price's Fourth Amendment rights.

Federal law provides that "'Fourth Amendment rights are personal' and 'may not be vicariously asserted.' [Citations.] A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." (*Rakas v. Illinois* (1978) 439 U.S. 128, 133-134.) Thus, to have standing to challenge a search on Fourth Amendment grounds, a defendant must establish a reasonable expectation of privacy in the area searched. (*In re Rudy F.* (2004) 117 Cal.App.4th 1124, 1131; *Rawlings v. Kentucky* (1980) 448 U.S. 98, 104-105.)

Under federal law, Price cannot establish a reasonable expectation of privacy in the areas searched pursuant to at least six of the 11 warrants—the warrants listed above as items 2, 3, 4, 5, 9, and 10. These warrants sought electronic information generated by persons other than Price (e.g., Jovany R.'s Gmail account data), in which Price had no reasonable expectation of privacy. Thus, Price lacks Fourth Amendment standing to challenge the six warrants under federal, Fourth Amendment law.²⁵

But under CalECPA, Price has standing to challenge the validity of all 11 warrants on Fourth Amendment *and* CalECPA grounds. As we have discussed, section 1564.4, subdivision (a), authorizes "[a]ny person in a trial, hearing, or proceeding" 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*." (Italics added.) Price is a person in a trial, hearing, or proceeding, and each of the 11 challenged warrants sought "electronic information," as CalECPA defines the term. (§ 1546, subd. (h).) CalECPA does not require Price to have a reasonable expectation of privacy in the electronic information sought in the 11 warrants in order to have standing to file a motion to suppress the information under CalECPA. (§ 1546.4, subd. (a).)

²⁵ We assumed for purposes of our analysis of Price's Fourth Amendment challenges to the geofence warrant that Price had a reasonable expectation of privacy in the location data and identifying information sought in the warrant, and, therefore, the warrant authorized a search within the meaning of the Fourth Amendment. Other courts have treated this issue as forfeited or implicitly conceded by the government, in the context of a defendant's Fourth Amendment challenge to a geofence warrant, when, as here, the government sought the warrant and does not claim the warrant did not authorize a search. (See, e.g., *Chatrie, Meza.*)

The Right to Truth-in-Evidence provision of our state Constitution (Cal. Const., art. I, § 28, subd. (f)(2)) does not require us to follow the federal law of Fourth Amendment standing. Originally enacted in 1982, the provision states: "Except as provided by statute hereafter enacted by a two-thirds vote of the membership in each house of the Legislature, relevant evidence shall not be excluded in any criminal proceeding including pretrial and post conviction motions and hearings" (*Ibid.*; *People v. Guzman, supra*, 8 Cal.5th at p. 679.) Absent such a statute, the Right to Truth-in-Evidence provision prohibits relevant evidence from being excluded in a criminal proceeding, "except to the extent that exclusion remains federally compelled." (*In re Lance W., supra*, 37 Cal.3d at pp. 886-887.)

CalECPA was enacted by over a two-thirds vote of the membership of each house of our state Legislature. Thus, CalECPA is excepted from the Right to Truth-in-Evidence provision of our state Constitution. (Cal. Const., art. I, § 28, subd. (d)(2).) In authorizing "[a]ny person, in a trial, hearing, or proceeding" to make a motion "to suppress evidence obtained or retained in violation of" any person's Fourth Amendment rights or of CalECPA, section 1546.4, subdivision (a), confers standing on Price to challenge the validity of the 11 warrants on both Fourth Amendment and CalECPA grounds. C. *Price Has Forfeited Most of His Challenges to the Other 10 Warrants*

A party forfeits a claim on appeal if the party fails to support the claim "with cogent argument, legal authority or specific citations to the record on appeal." (*United Grand Corp. v. Malibu Hillbillies, LLC* (2019) 36 Cal.App.5th 142, 153.) "We may and do 'disregard conclusory arguments that are not supported by pertinent legal authority or

fail to disclose the reasoning by which the appellant reached the conclusions he wants us to adopt.' " (*Ibid.*) "In order to demonstrate error, an appellant must supply the reviewing court with some cogent argument supported by legal analysis and citation to the record." (*City of Santa Maria v. Adam* (2012) 211 Cal.App.4th 266, 286-287.)

Price has forfeited most of his Fourth Amendment and CalECPA claims concerning 10 of the warrants (except the geofence warrant) because his petition does not explain the factual and legal bases of most of his claims. For example, Price does not explain why any of the warrants, other than the geofence warrant, lacked probable cause or particularity under the Fourth Amendment. Price only generally asserts that the other 10 warrants were overbroad in the electronic information the warrants sought.

In his original and renewed suppression motions, Price raised specific challenges to the other 10 warrants. But Price does not sufficiently articulate most of these claims in his writ petition. Nor does he explain how the superior court's extensive analysis of his claims regarding the other 10 warrants was incorrect. Thus, we do not revisit these claims here. We would only be rehashing the superior court's analysis of the claims.

Nonetheless, we have reviewed the contents of the other 10 warrants and find no Fourth Amendment probable cause or particularity infirmities in the electronic information sought. Each warrant also specified, as reasonable and appropriate, "the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought" in accordance with CalECPA's particularity provision. (§ 1546.1, subd. (d)(1).) And, to the extent notice of the other 10 warrants was not given in accordance with CalECPA (§ 1546.2), the purpose of CalECPA's notice

provisions was not undermined, for the same reasons it was not undermined in connection with the geofence warrant.

Through all 11 warrants, investigators were trying to identify the two unknown suspects in the murder of Jovany R. or find evidence linking a suspect to the murder. All 11 warrants were sealed when issued and remained sealed until after Price filed his original suppression motion. Sealing the warrants until the investigation was completed and Price was arrested was necessary to prevent adverse results, including serious jeopardy to the investigation. (§§ 1546, subd. (a), 1546.2, subd. (b)(1)-(2).) Thus, a court would have extended the notification periods for each warrant, through Price's December 2020 arrest, had the People sought the extensions.

D. Price's Traversal Claims Concerning the Other 10 Warrants Lack Merit

Price has preserved his claim that the other 10 warrants must be traversed based on the failure of their affidavits to explain that (1) the marijuana grow inside Jovany R.'s house was not visible from the outside, and (2) there was no evidence the suspects knew about the marijuana grow. As with the geofence warrant, however, these omissions were immaterial to the issuing magistrates' probable cause determination for each warrant.

Price raises another traversal claim concerning warrant 0201 (listed above as item no. 5), which sought records for three Gmail accounts belonging to two suspects in unrelated robberies, K.W. and T.H. This warrant was issued on May 8, 2020, and sought the Gmail account data for K.W. and T.J. for a seven-month period, June 1, 2019 through January 1, 2020. Price claims the government engaged in "warrant laundering" to obtain this warrant. He points out that the government first sought a warrant for the same Gmail

account data on January 22, 2020, for the period of June 1, 2019 through January 1, 2020, and this warrant was issued but the issuing magistrate restricted the time period to 60 days. The government did not serve this warrant, and, on January 28, 2020, the government went to another magistrate who issued a second warrant (0205) for the originally requested period of January 1, 2019 through January 1, 2020. This warrant (0205) was served and the government received the data, but Price claims "two specifically listed officers didn't download that data." Then, on May 8, 2020, the government obtained warrant 0201 for the same Gmail account data, for the seven-month period of June 1, 2019 through January 1, 2020. The May 8, 2020 warrant (0201) mentioned the seven-month, January 28, 2020 warrant (0205), but it did not mention the 60-day, January 22, 2020 warrant.

Price claims the failure to mention the 60-day January 22, 2020 warrant in the affidavit for the seven-month, May 8, 2020 warrant (0201) was a material omission. We disagree. Although we agree that the magistrate should have been apprised of both prior warrants, we do not view the omission as material. As the superior court explained in rejecting this claim, the omission had no bearing on the probable cause showing for the May 8, 2020 warrant. The affidavit for the May 8 warrant showed probable cause to believe that seven months of Gmail account data for the two suspects in the unrelated robberies, from June 1, 2019 through January 1, 2020, rather than 60 days of such Gmail account data, would reveal evidence of the murder and help law enforcement identify the suspects, or rule out K.W. and T.H. as suspects. As the superior court explained: "Whether the first magistrate limited the timeframe does not impact whether another

magistrate believed a larger timeframe was constitutionally permissible. Reasonable persons may disagree about these [timeframe] issues, and the finding of one magistrate does not mean the finding of another is invalid or that the second magistrate would necessarily have agreed with the first."

VI. THE GUN EVIDENCE

Price claims the gun evidence should have been suppressed as a product of his unlawful detention in West Covina on January 18, 2020. We disagree.

A. Additional Background

1. Officer Kyle Clifton's Preliminary Hearing/Suppression Motion Testimony

Around 3:40 p.m. on January 18, 2020, Officer Clifton was on patrol in West Covina, driving a marked police car, when he drove by the "California Parkette," a suburban park that "backs up" to a water company. The officer was familiar with the area from patrolling it and noticed something unusual: a vehicle parked in the water company's private driveway. The driveway was adjacent to the park and led to a gate to the water company. The vehicle, a blue Ford Fusion, appeared to be unoccupied. It was parked on the right side of the driveway, next to a grassy area of the park, and facing a gate to the water company.

Officer Clifton testified he believed the vehicle was parked in violation of Vehicle Code section 22500, subdivision (e)(1), which he understood prohibited "blocking a driveway." The officer parked his patrol car around 15 to 20 feet behind and around one foot to the left of the vehicle. He then walked to the driver's side window of the vehicle, which was down. He did not recall whether he had his hand on his gun as he approached

the vehicle. He noticed a male in the driver's seat, whom he identified in court as Price. He then noticed a female in the front passenger seat. He asked Price how Price's day was going and whether Price was willing to speak with him, and Price said yes. He then asked Price what Price was doing at the park. Price said he was looking for directions and wanted to show his female passenger a video on his phone.

As he was speaking with Price, Officer Clifton noticed "a strong odor of marijuana emitting from the vehicle." The officer then asked Price whether the officer could have Price's driver's license, and Price said, "yes." As Price was handing the officer his driver's license, the officer asked Price whether there was any marijuana in the vehicle. Price said, "yes," and showed the officer a bag of marijuana. Price had "bloodshot, watery eyes," which made the officer suspect Price was under the influence of marijuana. Next, the officer asked Price whether Price was on parole or probation. Price said he was on parole for assault with a deadly weapon.

Officer Clifton then stepped away from the vehicle to perform a records check to determine whether Price was on parole. After verifying that Price was on parole, either on his phone or through his patrol car radio, the officer stepped back to the vehicle and asked Price whether there were any other drugs or weapons in the vehicle. Price said there were not. The officer then stepped away from the vehicle to "have" Price step out of the vehicle. The officer did not recall asking or ordering Price to step out of the vehicle.

Before Price stepped out of the vehicle, the vehicle suddenly lurched forward, toward the gate to the water company and away from Officer Clifton. The officer

stepped behind the driver's side door of his patrol car for "cover." Price quickly stopped the vehicle, reversed it a few feet to where it had been parked, put his hands in the air through the driver's side window, and called to the officer that he did not know his vehicle was still in drive. Around this time, Officer Clifton's partner pulled up in a second marked patrol car and parked on the street in front of the park. After the second officer arrived, Price and his female passenger were ordered out of the vehicle and taken into custody.

Next, Officer Clifton conducted a parole search of Price's vehicle. The officer found a loaded .45-caliber handgun "in plain view" on the front passenger seat. The gun was in the firing position and its safety was "off." In the center console, the officer found the bag of marijuana Price had shown him. The officer took the marijuana and booked the gun into evidence.

Later on January 18, 2020, Officer Clifton wrote a report of the incident, his first of two reports. The officer testified he mistakenly wrote in his original report that the vehicle was parked in a "parking lot" rather than in a driveway because he was "exhausted" after working an overtime shift. The officer also wrote in his original report, and testified, that he contacted Price and the female passenger in a "consensual manner," that is, in a "politer, more professional way" for "de-escalation and to gain a little bit more cooperation with the driver."

On August 9, 2021, Price filed a motion to suppress the warrant evidence and the gun evidence—the evidence that the gun used in the October 29, 2019 shooting death of Jovany R. was found in Price's vehicle during the January 18, 2020 parole search of the

vehicle. After the suppression motion was filed, a deputy district attorney and Investigator Deanne contacted Officer Clifton and questioned him about his original report. Officer Clifton then wrote a supplemental report, dated August 25, 2021, to correct his January 18, 2020 original report, and to provide further details about the driveway and his "consensual encounter" with Price. Officer Clifton denied that anyone told him what to write in his supplemental report, and he affirmed that the information in the supplemental report was based on his observations and recollections of the January 18, 2020 incident.

In his supplemental report, Officer Clifton wrote that the vehicle was parked in a driveway, not in a parking lot, and that the officer returned to the driveway and measured it for the supplemental report. The driveway was 17 feet wide and 80 feet long, measured from the street in front of the driveway to the "water supply facility['s]" wrought iron gate. Price's vehicle was parked one foot from the right side of the driveway, facing the gate to the water supply facility. The officer knew that only large commercial trucks typically used the driveway to enter and exit the facility, and Price's vehicle was blocking the trucks' access to and from the facility.

In his original report, Officer Clifton did not mention Vehicle Code section 22500 or state that he intended to issue a citation to the driver for violating the statute when he approached the vehicle. The officer first mentioned Vehicle Code section 22500 in his supplemental report. The officer testified that when he approached the vehicle, he intended to "at least" advise its occupant of the Vehicle Code section 22500, subsection (e)(1) violation, or issue a citation for the violation. But he did not do either of these

things, because his intentions changed after he verified that Price was on parole and found the gun in Price's vehicle during the parole search. When asked why he did not tell Price that Price was not allowed to park in the driveway, Officer Clifton testified that he "did not have to."

There were no signs posted along the driveway, prohibiting parking on or in the driveway. The officer also did not look for or find any "pipes or joints or anything that would . . . account for the smell of burning marijuana." The officer initially testified he could not tell whether the vehicle was running when he approached it, but he later testified that the vehicle was running, and he did not recall that its engine was turned off before it lurched forward. The officer also testified that he did not recall the precise sequence of events when he first testified, but his recollection of events was refreshed after he reviewed his original and supplemental reports.

2. <u>The Magistrate's Rulings on the Motion To Suppress the Gun Evidence</u>

The magistrate at the preliminary hearing denied the motion to suppress the gun evidence after concluding that Price was lawfully detained in the water company's driveway before the parole search of his vehicle. Thus, the magistrate ruled that the gun found during the parole search of the vehicle and the ballistics evidence showing that the gun was the same gun used in the shooting death of Jovany R., were not required to be suppressed as the fruits of an unlawful detention.

The magistrate concluded that Price's vehicle was parked on a private driveway (Veh. Code, § 490), and that Price was detained when Officer Clifton parked his patrol car behind Price's vehicle. The magistrate also ruled that the detention was lawful—it

did not violate the Fourth Amendment—because the officer had reason to suspect that the vehicle was parked "on" the driveway in violation of Vehicle Code section § 22500, subdivision (e)(1), which prohibits parking "*in front of* a public or private driveway." (Italics added.) The magistrate rejected Price's argument that the vehicle was lawfully parked "on" or "in" rather than "in front of" the driveway and, therefore, that Price was unlawfully detained. The magistrate also concluded that "everything" Officer Clifton did after he approached Price's vehicle was "reasonable" and did not violate the Fourth Amendment.

B. The Motion To Suppress the Gun Evidence Was Properly Denied

Price claims the motion to suppress the gun evidence was erroneously denied because the parole search, during which the gun used in the shooting was found in Price's vehicle, was the fruit of Price's unlawful detention. Price claims he was unlawfully detained without an articulable, reasonable suspicion that he had committed or was committing a crime, when Officer Clifton approached him in his parked vehicle. Price claims his vehicle was lawfully parked "in" or "on" the private driveway of the water supply company, and he was therefore not violating Vehicle Code section 22500, subdivision (e)(1), which only prohibits parking "in front of" a driveway. Price also claims Officer Clifton violated Price's Fourth Amendment rights by "demanding" to see Price's identification, asking Price whether there was any marijuana in the vehicle, asking Price whether he was on probation or parole, then "ordering" Price to step out of the

vehicle. Lastly, Price claims the magistrate should have discredited all of Officer Clifton's testimony as contradictory and inherently unreliable.²⁶

1. Legal Principles

The Fourth Amendment guarantees " '[t]he right of the people' " to be free from unreasonable searches and seizures. (*People v. Camacho* (2000) 23 Cal.4th 824, 829.) For purposes of the Fourth Amendment, police " ' "contacts" ' " or " ' "interactions" ' " with individuals fall into three broad categories: "consensual encounters, detentions, and arrests, with consensual encounters being the least intrusive, and arrests the most intrusive, of these contacts." (*People v. Gutierrez* (2018) 21 Cal.App.5th 1146, 1152.)

"Consensual encounters do not trigger Fourth Amendment scrutiny." (*In re Manuel G.* (1997) 16 Cal.4th 805, 821.) " '[L]aw enforcement officers may approach someone on the street or in another public place and converse if the person is willing to do so' without having any 'articulable suspicion of criminal activity. ' " (*People v. Parrott* (2017) 10 Cal.App.5th 485, 492.) "[A] detention does not occur when a police officer merely approaches an individual on the street and asks a few questions." (*In re Manuel G.*, at p. 821, citing *Florida v. Bostick* (1991) 501 U.S. 429, 434.) But a motorist is detained when an officer approaches the motorist in a parked car and, in view of the

²⁶ Price represents that the Los Angeles County District Attorney did not file an unlawful firearm possession charge against Price based on Price's unlawful possession of the gun found during the January 18, 2020 parole search, "presumably because [the Los Angeles County District Attorney] could not overcome the Fourth Amendment violation." We are unaware of the Los Angeles County District Attorney's reasons, if any, for not filing the unlawful possession charge, and its failure to file or prosecute the charge does not affect our analysis of the lawfulness of the detention.

circumstances, a reasonable person in the motorist's position would not feel free to leave or otherwise terminate the encounter. (*People v. Brown* (2015) 61 Cal.4th 968, 975-977.) Evidence may be suppressed if it is the "fruit" of an unlawful detention. (*Brewer v. Superior Court, supra*, 16 Cal.App.5th at pp. 1023-1025.)

2. Price Was Lawfully Detained

The magistrate concluded, and the People do not dispute, that Price was detained when Officer Clifton parked his patrol car around 15 to 20 feet behind, and one foot to the left of, Price's parked vehicle, and approached the vehicle, ostensibly to speak with its driver or occupants. Whether an individual had been detained is a legal question subject to our de novo review. (*Tacardon, supra*, 14 Cal.5th at pp. 254-255.) In determining whether a detention occurred, we defer to the magistrate's factual findings if substantial evidence supports them and the record shows the magistrate performed the function of weighing the evidence concerning the detention. (*Id.* at pp. 255-256.)

The record shows the magistrate weighed Officer Clifton's testimony about the circumstances surrounding the officer's investigation of Price's parked vehicle and detention of Price. Based on this evidence, the magistrate concluded that a detention occurred when the officer parked his patrol car behind Price's vehicle because it would have taken "herculean efforts to get out [of the driveway] past the police officer." That is, to leave the driveway, Price would have had to drive his vehicle forward, turn his vehicle around, and drive around the officer's patrol car. Substantial evidence shows Price was detained when the officer parked his patrol car behind Price's vehicle. The officer parked 15 to 20 feet behind and one foot to the left of the vehicle, indicating to

any reasonable driver of the vehicle that the driver was not free to leave or terminate the encounter.

In *Tacardon*, our Supreme Court emphasized that, "merely walking up to someone in a parked car is not a detention." (*Tacardon, supra*, 14 Cal.5th at p. 241.) Something more is required: the officer must, "by means of physical force or a show of authority" in some way, restrain the liberty of an individual. (*Ibid.*, citing *People v. Brown* (2015) 61 Cal.4th 968, 974.) " 'In situations involving a show of authority, a person is seized "if 'in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave' " or " 'otherwise terminate the encounter' "....'" (*Tacardon*, at p. 241, italics added.)

In determining whether a detention occurred, courts are required to consider the totality of the circumstances, including "the use of a patrol car to block movement." (*Tarcardon, supra*, 14 Cal.5th at p. 242, citing *Michigan v. Chesternut* (1988) 486 U.S. 567, 575.) The facts are reviewed objectively; the officer's state of mind is not relevant " 'except insofar as his overt actions would communicate that state of mind,' " and the individual citizen's subjective state of mind or belief is also not relevant. (*Tacardon*, at p. 242.) Here, the facts, viewed objectively, show Price was detained when Officer Clifton parked his patrol car 15 to 20 feet behind and one foot to the left of Price's vehicle. Under the totality of the circumstances, parking the patrol car behind and to the left of the vehicle was a sufficient show of authority to turn what might have been a consensual encounter into a detention. The way the officer parked his patrol car

reasonably indicated to any occupants of Price's vehicle that the occupants were not free to leave and terminate the encounter with the officer.

Price claims his detention violated his Fourth Amendment rights because there was no reason to suspect he was committing a crime by parking his vehicle on or in the private driveway. Detentions are "seizures of an individual which are strictly limited in duration, scope and purpose, and which may be undertaken by the police 'if there is an articulable suspicion that a person has committed or is about to commit a crime.' " (*Wilson v. Superior Court* (1983) 34 Cal.3d 777, 784.) The suspected crime may be a misdemeanor or a traffic violation. (*Atwater v. City of Lago Vista* (2001) 532 U.S. 318, 354 [upholding warrantless arrest based on probable cause of misdemeanor seat belt violation]; *Arkansas v. Sullivan* (2001) 532 U.S. 769, 771-772 [upholding traffic stop and detention for speeding and tinted windshield violations].)

The articulable suspicion requirement is also measured by an objective standard, not by the detaining officer's subjective state of mind at the time of the detention. (*People v. Kidd, supra*, 36 Cal.App.5th at p. 22; *People v. Conway* (1994) 25 Cal.App.4th 385, 388-389 [" '[T]he fact that the officer does not have the state of mind which is hypothecated by the reasons which provide the legal justification for the officer's action does not invalidate the action taken as long as the circumstances, viewed objectively, justify that action.' "].) The objectively reasonable suspicion necessary to justify a detention is "'… less demanding than that for probable cause' and can be established by 'considerably less than proof of wrongdoing by a preponderance of the evidence.' " (*People v. Souza* (1994) 9 Cal.4th 224, 230.)

A misdemeanor trespass is committed by willfully driving a vehicle upon real property belonging to another and known not to be open to the general public, without the consent of the property owner. (§ 602, subd. (n).) Officer Clifton had an objectively reasonable suspicion that Price was trespassing on the private driveway by parking his vehicle on or in the driveway. (*Ibid.*) The facts known to the officer when he decided to investigate the parked vehicle, and why it was parked there, supported a reasonable suspicion that the driver of the parked vehicle was committing a misdemeanor trespass by parking the vehicle on the driveway without the driveway owner's permission.

Officer Clifton testified that he was familiar with the area and had seen large, commercial water trucks using the driveway to enter and exit the dirt area behind the water company gate. The officer knew the driveway belonged to the water company and that the driveway was not part of the adjoining park. On the other side of the park, there was a parking area for park visitors. The officer believed that members of the public were not authorized to park vehicles on the driveway. Although there was enough room on the driveway to allow passenger vehicles to drive around Price's parked vehicle, the vehicle would have prevented the water company's large, commercial trucks from using the driveway. Even though there were no signs posted near or along the driveway prohibiting parking or trespassing, the officer's testimony showed that it was reasonably apparent that the driveway was a private driveway not open to the general public.²⁷

²⁷ The posting of signs prohibiting trespassing is not an element of a trespass in violation of section 602, subdivision (n); rather, the real property driven upon must be "known not to be open to the general public." (Cf. § 602, subd. (h)(1) [trespass is *[footnote continued on next page]*

Price claims Officer Clifton's suspicion that Price was violating Vehicle Code section 22500, subdivision (e)(1), did not justify the detention because Price was not violating the statute by parking on or in, rather than in front of, the driveway. Officer Clifton testified he stopped to investigate the parked vehicle because he suspected it was parked in violation of Vehicle Code section 22500, subdivision (e)(1). The statute prohibits parking "in front of" a public or private driveway, but it does not expressly prohibit parking "in" or "on" a driveway. (Veh. Code, §22500, subd. (e)(1).) It provides: "A person shall not stop, park, or leave standing any vehicle whether attended or unattended, except when necessary to avoid conflict with other traffic or in compliance with the directions of a peace officer or official traffic control device, in any of the following places: \dots [¶] \dots [¶] (e)(1) In front of a public or private driveway. \dots " (*Ibid.*) Vehicle Code section 490 defines a " 'private road or driveway'" as "a way or place in private ownership and used for vehicular travel by the owner and those having express or implied permission from the owner but not by other members of the public."

Both the magistrate at the preliminary hearing, who heard the officer's testimony and ruled on the original suppression motion, and respondent superior court, in ruling on the renewed suppression motion as part of the Penal Code section 995 motion, concluded that Vehicle Code section 22500, subdivision (e)(1), applies when a car is parked "in" or "on" a driveway. The magistrate and court reasoned that Vehicle Code section 22500,

committed by "[e]ntering upon lands . . . owned by any other person without the license of the owner or legal occupant, *where signs forbidding trespass are displayed*, and whereon cattle . . . or any other animal, is being raised" (Italics added.)].)

subdivision (e)(1), is intended to prevent vehicles from blocking driveways, and a vehicle is necessarily blocking part of a driveway when it is parked in or on the driveway. Thus, the magistrate and superior court ruled that Price was lawfully detained based on the officer's reasonable suspicion that Price was parked in or on the driveway in violation of Vehicle Code section 22500, subdivision (e)(1).

It is unnecessary for this court to determine whether Vehicle Code section 22500, subdivision (e)(1), prohibits parking in or on a driveway, in addition to parking in front of a driveway, and, therefore, the officer had reason to suspect Price's vehicle was parked in violation of the statute, justifying the detention. It is immaterial that Officer Clifton believed the driver was violating Vehicle Code section 22500, subdivision (e)(1), by being parked in or on the driveway. Everything the officer saw concerning the parked vehicle supported an objectively reasonable suspicion that the vehicle's driver was committing a misdemeanor trespass by parking the vehicle on or in the driveway without its owner's permission. (Pen. Code, § 602, subd. (n).) "[A]n officer's reliance on the wrong statute [to justify a detention] does not render the officer's actions unlawful if there is a right statute that applies to the defendant's conduct." (*In re Justin K.* (2002) 98 Cal.App.4th 695, 700.)

3. Officer Clifton's Actions During the Detention Were Lawful

Price claims that, when Officer Clifton approached Price's vehicle and smelled marijuana, the officer violated the Fourth Amendment by "demanding" to see Price's identification, asking Price whether there was marijuana in the car, asking Price whether

he was on parole or probation, and ordering Price to step out of the vehicle. We conclude that none of the officer's actions violated Price's Fourth Amendment rights.

At the beginning of the detention, as Officer Clifton was speaking with Price, and before the officer noticed the smell of marijuana in the vehicle and that Price had bloodshot and watery eyes, the officer was justified in asking or "demanding" to see Price's identification or driver's license, based on the officer's reasonable suspicion that Price's vehicle was unlawfully parked on the driveway. (*People v. Saunders* (2006) 38 Cal.4th 1129, 1135 [When there is reason to suspect a vehicle or its occupant is subject to seizure for violation of the law, "the vehicle may be stopped and the driver detained in order to check his or her driver's license and the vehicle's registration."]; *People v. Tully* (2012) 54 Cal.4th 952, 980 [Upon demand of a police officer, every motorist must present for examination the motorist's driver's license and vehicle registration card.].)

Officer Clifton was also justified in asking Price whether there was marijuana in the vehicle, after the officer smelled marijuana in the vehicle and noticed Price had blood shot and watery eyes. The officer testified that, as Price was handing Price's driver's license to the officer, the officer noticed "a strong odor of marijuana emitting from the vehicle," then asked Price whether there was any marijuana in the vehicle. Price said, "yes," and showed the officer a bag of marijuana. Around this time, the officer noticed that Price's eyes were bloodshot and watery, which made the officer suspect that Price was under the influence of marijuana.

As Price points out, the presence of a small quantity of marijuana in a vehicle, *by itself*, does not constitute probable cause to search the vehicle for contraband, given that the possession of 28.5 grams or less of marijuana by a person age 21 years or older is no longer a crime. (*People v. Hall* (2020) 57 Cal.App.5th 946, 952 ["[T]he lawful possession of marijuana in a vehicle, by itself, cannot justify a warrantless car search."]; *People v. Johnson* (2020) 50 Cal.App.5th 620, 629 ["[E]vidence of marijuana in a car does not provide certainty the car contains contraband."]; Health & Saf. Code, § 11362.1, subds. (a)(1), (a)(4) [authorizing possession, use, and transportation by persons 21 years of age or older of less than 28.5 grams of cannabis], subd. (c) ["no conduct deemed lawful by this section shall constitute the basis for detention, search, or arrest"].)

But this case does not involve the apparent lawful possession of marijuana in a vehicle without probable cause to believe the driver had committed or was committing a crime. When Officer Clifton noticed "a strong odor of marijuana emitting from the vehicle" *and* that Price had bloodshot and watery eyes, the officer had *probable cause* to believe Price was committing two crimes: (1) driving under the influence of marijuana (Veh. Code, § 23152, subd. (f)), and (2) driving with an open container of marijuana in the vehicle (Veh. Code, § 23222, subd. (b); *People v Johnson, supra*, 50 Cal.App.5th at p. 630; *People v. Fews* (2018) 27 Cal.App.5th 553, 563).

In any event, the officer did not violate Price's Fourth Amendment rights by asking Price whether there was any marijuana in the vehicle, and whether Price was on probation or parole. "Questioning during the routine traffic stop on a subject unrelated to the purpose of the stop is not itself a Fourth Amendment violation. Mere questioning is

neither a search nor a seizure. [Citation.] While the traffic detainee is under no obligation to answer unrelated questions, the Constitution does not prohibit law enforcement officers from asking." (*People v. Brown* (1998) 62 Cal.App.4th 493, 499.)

Next, in response to the officer's question whether Price was on probation or parole, Price said he was on parole for assault with a deadly weapon. The officer then stepped away from Price's vehicle to verify that Price was on parole, and after doing so, stepped back to the vehicle, ostensibly ordered Price to step out of the vehicle, and asked Price whether there were any other drugs or weapons in the vehicle. The officer's order to Price to step out of the vehicle was justified after the officer verified that Price was on parole and subject to a parole search condition. (§ 3067, subd. (b)(3); *People v. Delrio* (2020) 45 Cal.App.5th 965, 970-971.) A parole search condition subjects a parolee to a search "at any time of the day or night, with or without a search warrant or with or without cause." (§ 3067, subd. (b)(3).) During the subsequent parole search of the vehicle, a loaded .45-caliber handgun was found "in plain view" on the front passenger seat. The ballistics test later showed that the gun was the gun used to shoot and kill Jovany R. on October 29, 2019.

4. No Part of Officer's Clifton's Testimony Must Be Discredited

Price claims the magistrate at the preliminary hearing abused his discretion in crediting any part of Officer Clifton's testimony. He claims the officer's testimony was contradictory in many respects and was therefore not trustworthy or credible as a whole. He points out that, after the original motion to suppress the gun evidence was filed on August 9, 2021, and the officer spoke with Investigator Deanne and a prosecutor, the

officer wrote a second, supplemental report, stating for the first time that he approached Price's vehicle based on his suspicion that Price was violating Vehicle Code section 22500, subdivision (e)(1). Price claims the officer's supplemental report contradicted his original report because the original report did not mention Vehicle Code section 22500, subdivision (e)(1), as a basis for the investigatory stop. Instead, the original report stated that the officer approached Price's vehicle to engage in a "consensual encounter."

" ' In a suppression motion, "the power to judge the credibility of witnesses, resolve any conflicts in the testimony, weigh the evidence and draw factual inferences, is vested in the trial court." ' " (*People v. Vannesse* (2018) 23 Cal.App.5th 440, 445.) " ' "To warrant the rejection of the statements given by a witness who has been believed by a trial court, there must exist either a physical impossibility that [the statements] are true, or [the statements'] falsity must be apparent without resorting to inferences or deductions." ' " (*People v. Ennis* (2010) 190 Cal.App.4th 721, 728; see *Zemek v. Superior Court* (2020) 44 Cal.App.5th 535, 546.)

Here, there is no basis for this court to discredit the officer's testimony because none of the testimony was physically impossible or false on its face. For example, nothing in the officer's supplemental report was physically impossible or facially untrue in light of the officer's original report and testimony as a whole.

5. <u>Conclusion</u>

In sum, the January 18, 2020 parole search of Price's vehicle, during which the gun used in the October 29, 2019 shooting death of Jovany R. was found, was not the

fruit of an unlawful detention. (Brewer v. Superior Court, supra, 16 Cal.App.5th at

pp. 1023-1025.) Thus, the motion to suppress the gun evidence was properly denied.

VII. DISPOSITION

The petition for a writ of prohibition is denied. The order staying the criminal proceedings against Price is lifted.

CERTIFIED FOR PARTIAL PUBLICATION

FIELDS

J.

We concur:

MILLER

Acting P.J.

MENETREZ

J.