**SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES**

 **SEARCH WARRANT APPLICATION**

**STAGE THREE – GEOFENCE – SERVICE PROVIDER**

I, Click or tap here to enter text. am the affiant in this matter. I declare, under penalty of perjury, that all information in this application is true, to the best of my knowledge. Unless otherwise indicated, information obtained from any other identified individual, or entity, is believed by me to be true. Based upon this information, I apply for this search warrant because I believe that I have probable cause to search the person, location, entity or thing listed herein, and seize the items listed herein, pursuant to Penal Code section 1524, as indicated below, and I further swear and attest that nothing sought in this application pertains to an investigation into a “prohibited violation” as that term is defined in Penal Code section 629.51.

[ ]  The property was stolen or embezzled. (1524 (a)(1)).

[ ] The property or things were used as the means of committing a felony. (1524 (a)(2)).

[ ] The property or things to be seized are in the possession of any person with the intent to use them as a means of committing a public offense, or in the possession of another to whom that person may have delivered them for the purpose of concealing them or preventing them from being discovered. (1524 (a)(3)).

[ ] The property or things to be seized consist of an item or constitute evidence that tends to show a felony has been committed or tends to show that a particular person has committed a felony. (1524 (a)(4)).

[ ]  The property or things to be seized consist of evidence that tends to show that a violation of PC 311.3 or 311.11 has occurred or is occurring. (1524 (a)(5)).

[ ]  There is a warrant to arrest the person. (1524 (a)(6)).

[ ] Click or tap here to enter text.

[ ] Click or tap here to enter text.

[ ] Click or tap here to enter text.

I also request the following orders based on the information contained herein:

[ ]  **Evidence Code 1040 Sealing Order** [ ]  **90 day notification delay by government agency** [ ]  **Evidence Code 1041 (Hobbs) Sealing Order** [ ]  **Non-disclosure and 90 day Delay of Notification by Service Provider** [ ]  **Immediate compliance is required** [ ]  **Delay Return until 10 days after Receipt of Data** [ ]  **Seal Page 5 pursuant to Evidence Code 1040** [ ]  **Seal all documents until Gov’t Code 7923.615 disclosure is required.** [ ]  **Night Service**

Click or tap here to enter text.Click or tap to enter a date. Click or tap here to enter text.

(Affiant/Declarant signature) (Date) (Violation(s) suspected)

**SEARCH WARRANT**

**STATE OF CALIFORNIA, COUNTY OF LOS ANGELES**

The People of the State of California to any Law Enforcement Officer in the County of Los Angeles, designated as a PEACE OFFICER by PC 830 et seq., and who has qualified pursuant to PC 832:

Proof, by the affidavit contained within the incorporated application; that there is Probable Cause to believe that the items described herein may be found at the location set forth herein, I find that it is seizable pursuant to PC 1524, and THEREFORE:

YOU are COMMANDED to SEARCH the location, person, entity, or thing as set forth herein, for the property, data or things as set forth herein, and to SEIZE those things, and retain those things in your custody, subject to further orders of the court as set forth in Penal Code section 1536.

This Search Warrant, which incorporates by reference, all included/attached documents, was submitted to me and I find Probable Cause to issue, and I do issue, this Search Warrant, and I make the additional orders listed below. If not set forth below, the time and date of issuance shall be the timestamp for the document as posted to the online portal or emailed to the applicant.

(All references to “PC” or “EC” are references to the California Penal Code or California Evidence Code, respectively)

Unless expressly ordered otherwise within this Search Warrant, all parties, entities, and “service providers” [as that term is described in PC 1546 (j)]; shall comply with, and are subject to, Penal Code sections 1524 *et seq*.; and 1546 et *seq*.

“Service Provider(s)” includes all cellphone carriers, websites, social media sites, email service providers, remote computing services, and all other entities providing electronic communications or electronic storage.

Service Provider shall provide the items listed herein as “Item to be searched/seized” and verify the authenticity of any electronic information it produces pursuant to Penal Code 1546.1(d)(3).

Pursuant to Penal Code sections 1524.3 (c) and 1546.1 (d)(2), any information obtained through the execution of this warrant that is unrelated to its objective shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by PC 1054.1 and 1054.7.

If the Peace Officer executing the warrant is present, including virtually or online, and is being **assisted** by other persons, as provided by **PC 1530**, the service provider must then provide, the information sought in this warrant to the assisting agency or person(s).

I also GRANT the following check-marked COURT ORDERS. Any Order that is NOT checked is Denied at this time.

“Sealed Portion” is ordered Sealed [ ]  **EC 1040** (and/or) [ ]  **EC 1041** (*Hobbs*). [ ] Warrant may be served anytime, **day or night**.

[ ] Page 5 is ordered **Sealed** pursuant to EC 1040. [ ] Immediate compliance is required.

[ ] The **Service Provider** and employees shall **NOT notify** the subscriber or disclose any information about this warrant to the subscriber or any other person, other than to those necessary to comply with this warrant, for **90 days**.

[ ]  **Peace Officers** executing this warrant may **delay** PC 1546.2 **notification** to the identified target(s) for **90 days**.

[ ]  Return shall be within 10 days of receipt of data or information.

[ ] All information in this document is ordered **SEALED** until disclosure is required by Gov’t Code 7923.615 or Penal Code 1546.2.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date & Time Signature & Printed Name

 Judge of the Superior Court of Los Angeles County

ADDITIONAL REQUESTS

[ ]  **I request night service based on the information from Page \_\_\_ Line \_\_\_ through and including Page \_\_\_ Line \_\_\_\_.**

[ ]  **I request that page 5 be sealed as Official Information pursuant to Evidence Code section 1040.**

[ ]  **I request that the information contained within the section identified as “Sealed Portion” and/or contained within Page \_\_\_\_ Line \_\_\_ through Page \_\_\_ Line \_\_\_\_, inclusive, to be SEALED pursuant to Evidence Code Section** [ ]  **1041 (*Hobbs*) because the information would identify or tend to identify the confidential informant(s) and/or pursuant to Evidence Code section** [ ]  **1040 as “official information” based on the information contained within Page \_\_\_ Line \_\_\_ through Page \_\_\_\_ Line \_\_\_**

[ ]  **To preserve the integrity of the investigation, I request that all information in this Application & Warrant and the Return be SEALED until disclosure is required by Government Code 7923.615, or the arrest of the suspect(s), whichever is sooner.**

[ ]  **I request that the Service Provider, and employees thereof, be Ordered Not to Disclose any information about this search warrant to the subscriber, or any other person and to Delay other required Notification to the subscriber for 90 days due to the information contained within Page \_\_\_\_ Line \_\_\_\_\_ through Page \_\_\_\_ Line \_\_\_\_.**

[ ]  **I also request the delay of PC 1546.2 Notification by law enforcement or other government agency for the same reasons.**

[ ]  **I request that the Return be Delayed until 10 days after receipt of the information based on the information contained within Page \_\_\_ Line \_\_\_ through Page \_\_\_ Line \_\_\_.**

[ ]  **I have listed other requests on Appendix A.**

**PENAL CODE 1546.1(d)(2)**

Investigating officers and any assisting personnel, acting under the direction of the investigating officers, are authorized to access all data to determine if the data contains the items as described herein. Those items that are within the scope of this warrant may be copied and retained by investigating officers. Items that are not within the scope of this warrant will be sealed and retained by the investigating officers pending any future court order or to comply with discovery requirements.

**DELAY OF SEARCH WARRANT RETURN**

It has been your Affiant’s experience that it takes telecommunications companies and Internet service providers considerable time beyond the statutory, 10-day, search warrant return period, to search for, compile, and provide the materials sought in this search warrant. Therefore, your Affiant may request permission to return this search warrant ***within 10 days from the date that all materials are received*** from these companies.

**NON-DISCLOSURE AND DELAY OF NOTIFICATION**

It is your Affiant’s experience that notification to affected and/or targeted parties of the existence of a search warrant and/or on-going police investigation affords individuals an opportunity and/or may cause them to destroy or delete evidence, change patterns of behavior, notify co-conspirators, and/or flee from apprehension and prosecution. Notification can jeopardize an investigation and hamper the efforts of law enforcement to seize evidence and/or individuals in a timely manner. I, therefore, request that the Service Provider be ordered not to disclose to the subscriber, or any other person except those necessary to comply with this search warrant, the existence of this search warrant or investigation, and to also be ordered to delay any other required notification for 90 days. I also request that any government agency which is required to provide notification, be allowed to delay such notification for 90 days.

**NIGHT SERVICE**

Your Affiant may request that night service be authorized allowing service of the Search Warrant to Service Provider’s Subpoena Compliance at any time, day or night, because, based on my training and experience, I know that most Service Providers have Law Enforcement Compliance Analysts on duty 24 hours a day, 7 days a week to process requests. This Search Warrant will be sent to the telecommunication companies via e-mail, FAX, an online portal, or other electronic means. Service of this warrant will not involve law enforcement officers making a physical entry into a business or any other structure.

**SCOPE OF SEARCH**

The first two stages of the Geofence involved in this case utilized Service Provider’s historical location data to identify the individuals responsible for the crime(s) described in the Statement of Probable Cause. By discovering the devices near the crime scene, your affiant expected to be able to identify possible suspects involved in the crime. This Stage 3 application seeks to obtain identifying information on the devices which were identified by the Stage 2 search warrant.

**STORED DATA AVAILABLE TO SERVICE PROVIDER**

Modern smartphones usually have GPS capability to navigate from place to place. Some factory-installed and user-installed applications utilize this capability to provide directions or other information.

Anyone who owns a smartphone with a search application transmits real-time location information to cell towers. As such, service providers have access to information as to the location of their subscribers based on the cellphone transmitting to cell towers.

The Service Provider is able to translate the IMEI and/or other numeric or alphanumeric Device ID to a specific subscriber. This warrant seeks subscriber identification.

**SMARTPHONE PREVALENCE**

In recent years, smartphones have been almost universally adopted by the American public, and as such it is rare to find a person who does not have their smartphone readily accessible.

As of 2021, according to a Pew Research survey, 85% of Americans possessed a smartphone. As such, a high probability exists that the suspect(s) in this case were in possession of smartphones.

As is now generally known, acquisition of cellphones without providing accurate subscriber identification is commonplace especially among outlaws. As such, information that identifies the method of payment to service providers, including bank account information, location of device purchase, etc. is necessary to properly identify the actual user of a device.

**INTEGRITY OF AN INVESTIGATION**

Information gathered in an investigation often needs to be temporarily withheld from the public to protect against false confessions, avoid flight from prosecution or creation of false evidence or alibis, and protect the safety of potential witnesses. Therefore, in addition to any other order to seal, I request that, as an exception to Penal Code 1534(a), that this document and the Return, be temporarily sealed and not made public until disclosure is required by Government Code section 7923.615 or Penal Code section 1546.2.

**GEOFENCE PRODUCTION PROTOCOL/ANALYSIS PROCESS**

The process to obtain reverse location search data, commonly referred to as a geofence, from a Service Provider, is broken down into a three-stage process. The primary purpose of this is to protect the privacy interests of subscribers. In the first two stages of the process, the information is anonymous. The only data provided by the Service Provider in the first two stages are Device IDs and the location history of those Device IDs based on the limited Initial Search Parameters.

A Device ID is a numeric or alphanumeric string of characters, assigned by the Service Provider to a device to uniquely identify it to Service Provider. The Device ID is meaningless to anyone other than Service Provider. It cannot be used to identify an individual, or an individual’s device, without further information from the Service Provider. This is done purposely to protect the identity of the Service Provider account holder. No account holder information, such as name, date of birth, email address, phone number, device information, or any other personal information is provided in Stage 1 or Stage 2.

In **Stage 1**, Service Provider responds to the search warrant for Device IDs and location history data based on the Initial Search Parameters. Once that data is obtained, it will be compared with the information that is already known about the suspect and potential witnesses to the crime. The primary purpose of this comparison is to eliminate Device IDs that do not comport to the facts of the case. It is not uncommon in a warrant such as this to receive numerous Device IDs in Stage 1. Most of the Device IDs detected in Stage 1 are eliminated during the analysis. If the devices detected is sufficiently limited, a Stage 3 warrant may be sought.

**Stage 2** in the process is also a search warrant. In Stage 2, a warrant is written for an expanded time frame or other parameters for the small number of Device IDs that were not eliminated in the analysis of Stage 1 data. An additional time frame is usually about an hour before and after the Initial Search Parameters. Importantly, there is no subscriber identity data provided in Stage 2. At this point in the process, law enforcement is still not in possession of any data that could identify the Device ID account holder. Stage 2 provides additional contextual data to determine if the Device IDs requested in Stage 2 are actually relevant to the investigation. The Stage 2 Device IDs are analyzed in a similar way to that of the Stage 1 Device IDs, except there is more information to work with to better determine if the Device ID should be eliminated from further scrutiny.

**Stage 3** is also a search warrant. In Stage 3, based on the probable cause gathered in Stages 1 and 2, the basic subscriber information for the Device IDs that were narrowed down from Stage 2 would be requested. It is not until Stage 3 that any identifying information of a Service Provider account holder is disclosed to law enforcement.

**This warrant is Stage 3 in the process.** This warrant is based on the information received in the previous Stage(s).

Stage 1 results received from Service Provider, related to a search warrant previously authored by the undersigned and granted by Los Angeles County Superior Court Judge \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which was served to Service Provider on Click or tap to enter a date. .

On Click or tap to enter a date. Service Provider, provided responsive data specific to initial search parameters, whichcontained anonymous Device IDs, date and timestamp when the anonymous Device IDs appeared, along with geo-location (coordinates of latitude and longitude), source (WiFi or GPS), and accuracy radius.

Stage 2 results received from Service Provider, related to a search warrant previously authored by the undersigned and authorized by Los Angeles County Superior Court Judge \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which was served to Service Provider, on Click or tap to enter a date. .

On Click or tap to enter a date., Service Provider, provided responsive data specific to initial search parameters, whichcontained anonymous Device IDs, date and timestamp when the anonymous Device IDs appeared, along with geo-location (coordinates of latitude and longitude), source (WiFi or GPS), and accuracy radius.

**YOU ARE THEREFORE COMMANDED TO SEARCH:**

Service Provider

**FOR THE FOLLOWING PROPERTY:**Click or tap here to enter text.

Records pertaining to the following:

Stage 1 Service Provider Reference Number: \_\_\_\_\_\_\_\_\_\_\_\_\_

Stage 2 Service Provider Reference Number: \_\_\_\_\_\_\_\_\_\_\_\_\_

**IT IS ORDERED** Service Provider, shall provide identifying information for the Service Provider accounts associated with each identified anonymous Device IDs, listed below, to include subscriber’s name, street address, telephone number(s), email addresses, services and Service Provider services subscribed to, the account created date, Terms of Service IP address and associated date and time, any SMS number(s), any nickname used, the Service Provider Account ID, and the last six (6) months of IP history, to include the date and time, IP addresses and type of activity, and any other information provided by the subscriber to the service provider to establish or maintain an account or communications channel. The Device IDs have been identified as relevant pursuant to the ongoing investigation through extensive mapping and analysis of the already provided records from Stage 1 and Stage 2.

**Anonymous IDs:** Click or tap here to enter text.

**Location 1**

Date/Time: Click or tap here to enter text.

**Location 2**

Date/Time:Click or tap here to enter text.

**APPENDIX A**

**STATEMENT OF EXPERTISE**

**STATEMENT OF PROBABLE CAUSE**