



Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Honorable John P. Vander Feer
Presiding Judge
Superior Court of California
County of San Bernardino
San Bernardino Justice Center
247 W. Third Street, 11th Floor
San Bernardino, CA 92415-0240

May 16, 2019

Dear Judge Vander Feer:

We are writing on behalf of the Electronic Frontier Foundation to ask that the Court review and unseal 22 of its files that, from what we can tell, are indefinitely and completely sealed in violation of the Penal Code and Rule of Court 2.551. The San Bernardino Sheriff's Department has informed us that these files relate to search warrants authorizing electronic searches under Penal Code § 1546.1 and pen-register/trap-trace orders issued under Penal Code § 638.52. The statutory schemes governing these warrants and orders allow sealing only until they are executed or expire, respectively. *See* Penal Code §§ 1534(a), 638.52(g).¹ Thus, these files should long ago have been unsealed under these provisions. Nevertheless, it appears that, at the request of the Sheriff's Department, these court files remain completely sealed until further order of the Court.

We therefore ask that the Court review the files listed in the attached Exhibit A to determine whether they are properly sealed and to unseal any of them – or any parts of them – that do not meet the criteria for sealing. *See* Rule of Court 2.551(h) (authorizing Court to unseal records sua sponte after notice to affected parties).

We also ask that the Court take steps to ensure that any future sealing orders in these types of matters comport with statutory and constitutional requirements.

1. Background

The California Electronic Communications Privacy Act (CalECPA) requires law-enforcement agencies to obtain a search warrant or wiretap order before they “[a]ccess electronic device information by means of physical interaction or electronic communication with the electronic device,” unless one of the statute’s enumerated exceptions applies. §§ 1546.1(a)(3), (c); *see* 2015 stats. ch. 651, codified at Penal Code § 1546 *et seq.* The Penal Code similarly requires the police to obtain a court order before installing a pen register or trap-and-trace device. *See* §§ 638.51, 638.52(g).

¹ All unspecified statutory references are to the Penal Code.

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Both of these statutes generally require that, if the government knows the identity of the target of the search, it must provide that person with notice, a variety of specified information, and a copy of the court order when it executes one of these orders. §§ 1546.2(a), 638.54. If the government does not know the identity of the target, it must instead report this same information to the California Department of Justice within three days of the termination of the pen-register or trap-and-trace order or execution of the warrant. §§ 638.54(c), 1546.2(c). The Department must then post this information on its Open Justice website within 90 days after redacting whatever “names or other personal identifying information” it deems appropriate. *See id.*; *see also* California Department of Justice, Electronic Search Warrant Notifications at <https://openjustice.doj.ca.gov/data>.

Both statutes allow the police to request court authorization to delay this notice for renewable periods of 90 days if they can show a need to do so. §§ 638.54(b), 1546.2. After these periods expire, they must then send the requisite notice to the target or, if the target is unknown, to the Department of Justice for publication on its website. §§ 638.54(b)(3), 1546.2(c).

In August 2018, the Electronic Frontier Foundation (EFF) sent the Sheriff’s Department a request for copies of six warrants and orders issued under these provisions, as well as the related search warrant numbers and supporting affidavits. After that Department refused to provide these records, EFF brought suit in this Court under the Public Records Act, Gov’t Code § 6250 *et seq.* *See* Case No. CivDS-1827591.

In the course of this litigation, the Sheriff’s Department has provided the search warrant numbers of these six warrants,² but refuses to provide the warrants themselves, asserting among other things, that it cannot do so because they have all been indefinitely sealed by this Court.

EFF has since requested 18 other warrants pertaining to electronic searches that the Sheriff’s department obtained under similar circumstances from this Court. The Department has provided two of them but has refused to provide the rest, again on the grounds that they are sealed. The two warrants that it did provide both contain sealing requests that were denied by the issuing magistrates: warrant numbers VVSW18-1048 and VVSW18-1286. It thus appears that the Sheriff’s Department requests indefinite sealing orders as part of every application for a warrant or court order under these statutes.

² The warrant numbers are SBSW 17-0615, SBSW 17-0694, SBSW 17-0695, SBSW 17-0834, SBSW 17-0890, and SBSW 17-0892. The Sheriff’s Department has informed us that these warrants are in some way connected to San Bernardino Superior Court case numbers FSB18002619, FSB18002622, and FSB18002623, all of which appear to have been consolidated for trial.

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

The warrants/orders at issue are listed in Exhibit A to this letter. All of these warrants and orders were issued in 2017 and 2018, and the fact that they are listed on the Department of Justice website indicates that they have been executed or expired.

Although the sealing orders prevent us from reviewing information about the proffered justification for sealing, or even if any such justification was asserted, we believe that these files should be unsealed, in whole or in part, for the following reasons.

2. Pen Register or Trap and Trace Orders Must Be Disclosed After They Expire

Some of the files at issue apparently involve orders “authorizing or approving the installation and use of a pen register or trap and trace device,” which are methods of obtaining routing and dialing information for telephone calls and other electronic communications, respectively. *See* §§ 638.52(a), 638.51 (definitions). These orders may be issued for periods of up to 60 days, and extended for additional 60-day periods if there is continuing probable cause to do so. *See* §§ 638.52(e), 638.52(f).

Until recently, a magistrate issuing these types of orders was required to “direct that the order be sealed until otherwise ordered” by the Court. *See* § 638.52(g) (2016). These indefinite sealing orders may well have violated the First Amendment. *See in re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 880-887 (S.D. Tex. 2008) (holding that the First Amendment prohibits indefinite sealing of electronic-surveillance orders). The Legislature addressed this problem in 2016 by changing this provision so that it now requires that “[a]n order or extension order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that the order be sealed until the order, including any extension, expires.” *See* § 638.52(g) (amended by 2016 Cal. Stats. ch. 511 §§ 1, 6). This legislative history and the language of the amended statute make it clear that these sealing orders must now expire when the underlying order does, particularly given the constitutional requirement that the statute be read so as to promote public access. *See* Cal. Const. art. I, § 3(b)(2); *Overstock.com, Inc. v. Goldman Sachs Grp., Inc.*, 231 Cal. App. 4th 471, 495 (2014) (“[W]e must interpret the sealed records rules broadly to further the public’s right of access” to court records). But it appears that the warrant application forms submitted by the Sheriff’s Department fail to comply with this statutory change; though it may well be that the issuing magistrates in many of these cases were not aware of this statutory non-compliance.

Law enforcement must provide notice to the target, if known, within 30 days of the expiration of the order. § 638.54(a). The issuing court may grant delays of this period under certain conditions. *Id.* If there is no identified target, the agency must provide notice to the Department of Justice after the order and any authorized delay periods expire; the Department must then post information about the order on its website within 90 days. § 638.54(c). Information

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

about all of the orders in question appears on the Department's website, which shows that they have been executed and that any non-disclosure order has expired.

3. Executed Search Warrants Become Public Ten Days After They are Issued

Many of the orders in question authorize the use of a cell-site simulator. These devices, commonly known as Stingrays (a brand name), masquerade as cell-phone towers and allow law enforcement to locate specific cell phones by diverting these phones' signals to the simulator, rather than to the carrier's real tower. They can also be used to determine the unique international-mobile-subscriber identifiers (IMSI) of unknown devices.

Law enforcement must obtain a special kind of search warrant under CalECPA before deploying a cell-site simulator. *See* §§ 1546.1(a)(3), 1546.1(c). Warrants issued under CalECPA must comply with specific particularity and notice requirements mandated by statute and aimed to improve public oversight and transparency. § 1546.1(d). They must also comply with § 1534, which makes all warrants and related documents public 10 days after they are issued, assuming they have been executed:

A search warrant shall be executed and returned within 10 days after date of issuance.... The documents and records of the court relating to the warrant need not be open to the public until the execution and return of the warrant or the expiration of the 10-day period after issuance. Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record.
§ 1534(a).

As with pen registers, the police must provide information about these warrants to the target, if known, after execution; if the target is unknown, they must provide the information to the Department of Justice, which then posts it on its website. § 1546.2. Although the police may apply to the court for authorization to delay notice for up to 90 days at a time, the fact that information about these warrants was posted on the Department of Justice website shows that any such periods have long since expired. *See* § 1546.2(c).

4. The Court should examine these warrant files and unseal any parts of them that are not properly sealed

"Since orders to seal court records implicate the public's right of access under the First Amendment, they inherently are subject to ongoing judicial scrutiny, including at the trial court level." *In re Marriage of Nicholas*, 186 Cal. App. 4th 1566, 1575 (2010). Thus, the "court on its own motion may move ... to unseal a record" "entirely or in part." Rule of Court 2.551(h)(2), (5). "If the court proposes to order a record unsealed on its own motion, the court must give notice to the parties stating the reason for unsealing the record. Unless otherwise ordered by the court, any

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

party may serve and file an opposition within 10 days after the notice is provided and any other party may file a response within 5 days after the filing of an opposition.” *Id.* 2.551(h)(3). “No showing of changed circumstances is necessary on a motion to unseal” brought under this Rule. *In re Marriage of Nicholas*, 186 Cal. App. 4th at 1577. To the contrary, any party seeking to restrict access has a “continuing burden” to show that the materials currently meet the standards for sealing. *Id.* at 1576. A different judge may unseal records sealed by another judge of the court. *Id.* at 1577-78. “These Rules apply to civil and criminal cases.” Rule 2.550 advisory committee comment; see *People v. Jackson*, 128 Cal. App. 4th 1009, 1022 (2005) (motion to unseal search warrants under prior rule).

The Court may order the records “unsealed entirely or in part.” Rule 2.551(h)(5). If redaction of a record is sufficient, sealing the entire record is improper. See Rule 2.551(h)(4); Rule 2.550(e)(1)(B); *People v. Hobbs*, 7 Cal. 4th 948, 972 (1994); *In re Marriage of Burkle*, 135 Cal. App. 4th 1045, 1067 (2006). The California Constitutional right of access requires that these Rules be read so as to promote public access. See *Overstock.com*, 231 Cal. App. 4th at 495; Cal. Const. art. I, § 3(b)(2); see also *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d at 880-887.

Because we do not have access to the sealed materials, we cannot know whether parts of them are properly sealed; but for the following reasons it seems almost certain that much of the material should be unsealed.

5. Sealing is proper only in narrow circumstances authorized by statute or the state or federal constitutions

Because the statutes governing these court files make them open to the public after the expiration of a pen-register/trap trace order or the execution of a search warrant, the Court must unseal this material unless some other statute or constitutional provision authorizes continued sealing. To assist the court in making this determination, we next discuss some of the provisions that could justify continued sealing.

The Court may partially seal an affidavit as necessary to protect the identity of a confidential informant, which is protected under Evidence Code § 1041. *Hobbs*, 7 Cal. 4th at 972-78. But “[a]ny portions of the sealed materials which, if disclosed, would *not* reveal or tend to reveal the informant’s identity must be made public.” *Id.* at 963 (emphasis added). These same rules apply when the government asks to withhold information in warrant materials that have yet to result in a prosecution under Evidence Code § 1040, which applies when the government proves that “disclosure of the information is against the public interest because there is a necessity for preserving the confidentiality of the information that outweighs the necessity for disclosure in the interest of justice.” Evid. Code § 1040(b)(2); see *PSC Geothermal Servs. Co. v. Superior*

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Court, 25 Cal. App. 4th 1697, 1714-15 (1994) (superior court erred by failing to consider whether redacting, rather than completely sealing, affidavit would sufficiently protect official information).

In addition, affidavits and related materials may be sealed in whole or in part as necessary to protect a criminal defendants' Sixth Amendment right to a fair trial and minor victims' right to privacy, so long as the sealing orders comply with former Rule of Court 243.1, now Rule 5.550, which itself incorporates the requirements of the First Amendment. *Jackson*, 128 Cal. App. 4th at 1022. *Jackson* involved a media request in the child-sex-abuse trial of pop star Michael Jackson to unseal documents, including search warrant affidavits, returns, and inventories, but not the warrants themselves. *See id.* The Court of Appeal held that under both the First Amendment and the Rules of Court, the public's right of access to these materials

may be denied only if the court, after notice and hearing, makes four supported findings: (i) there exists an overriding ... interest supporting closure and/or sealing; (ii) there is a substantial probability ... that the interest will be prejudiced absent closure and/or sealing; (iii) the proposed closure and/or sealing is narrowly tailored to serve the overriding interest; and (iv) there is no less restrictive means of achieving the overriding interest.³

The court went on to hold that because the search warrant affidavits, returns, and inventories contained "highly prejudicial" "details of the crimes alleged," "combined with the celebrity of the defendant," and the "torrent of pretrial publicity," sealing them was appropriate because doing so was necessary to protect the Defendant's Sixth Amendment rights and the privacy rights of minors who had allegedly been the subject of sex abuse. *See Jackson*. at 1023, 1025. This unique combination of factors distinguished the case from others where sealing was inappropriate. *See id.* at 1024 ("[T]he combination of celebrity status, the crimes alleged and the ongoing criminal investigation that justifies sealing."); *cf. id.* at 1014 (noting "sui generis nature of [the] case").⁴ Even so, the court held that continued sealing of the indictment was improper. *Id.* at 2018.

³ *Id.* (citing *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 20 Cal. 4th 1178, 1217-18 (1999)); *see also Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 607 (1982) (access restrictions must be "necessitated by a compelling governmental interest, and . . . narrowly tailored to serve that interest").

⁴ Although Rule 2.550 cannot in itself authorize sealing orders and warrants that are declared open by statute, the right to privacy protected by Article I § 1 of the California Constitution could of course override the statute. *See Cal. Court Reporters Ass'n. v. Judicial Council of Cal.*, 39 Cal. App. 4th 15, 21-22, 33-34 (1995) (Rules of Court must be consistent with statutes).

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Jackson thus illustrates the unusual case in which sealing may be appropriate; but it is highly doubtful that these factors would apply to all – or even most – of the electronic search warrants obtained by the San Bernardino Sheriff's Department. In any event, the public's right of access to the requested materials cannot be denied under *Jackson* unless the court makes the four required factual findings. *See NBC Subsidiary*, 20 Cal. 4th at 1217-18.

6. These files should be completely or partially unsealed

We believe that an examination of the materials will show that they should be unsealed under these rules, at least in part because:

- a. The fact that information about these warrants and orders is available on the Department of Justice website indicates that any period for which the governing statutes authorize sealing has long since expired. These statutes therefore make them public unless some other statute or constitutional provision overrides that presumption.
- b. There can be no justification for sealing boilerplate parts of the files such as the outdated indefinite sealing orders or other parts containing general legal propositions, unrelated to any specific case, that were presented to the court. This information cannot be privileged and, because it does not relate to any individual case, cannot implicate any constitutional right. Moreover, there is no compelling interest that justifies sealing these materials. Both the Penal Code and the First Amendment therefore require that they be unsealed.
- c. For these same reasons, there cannot be any justification for sealing the orders authorizing Defendants to delay sending notification to the targets or the DOJ, along with the dates that those orders were issued and when they expired. The court will have to determine whether any of the facts presented to support these delayed-notification orders should continue to be sealed under *Hobbs* or *Jackson*. But the remainder of these documents must be unsealed.
- d. We are not aware of any precedent authorizing a court to seal a warrant or judicial order (as opposed to the supporting affidavit) after it has expired or been executed. This makes sense because it seems unlikely that a search warrant would itself contain much, if any, information that would meet the standards for sealing under *Hobbs* or *Jackson*: warrants do not generally contain the names of informants or the type of information that would jeopardize the right to a fair trial or constitute such a severe infringement on personal privacy so as to merit sealing. And there is an extremely significant countervailing public interest in government transparency and accountability by allowing the public to see how and why courts are authorizing the police to conduct digital searches.

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

- e. Information that has already been disclosed cannot be sealed because “there is no justification for sealing records that contain only facts already known or available to the public.” *H.B. Fuller Co. v. Doe*, 151 Cal. App. 4th 879, 898 (2007); *see Jackson*, 128 Cal. App. 4th at 1028. It seems likely that much of the information in the sealed documents has been revealed in the course of criminal proceedings, either in discovery provided to the defense without any sort of protective order or in the preliminary hearings, trials, or other evidentiary hearings.
- f. Summary sealing of the entirety of the requested search warrants and supporting materials is not narrowly tailored to serve any legitimate government interest in sealing.

7. Some of the Court’s files may be erroneously designated as sealed

We note one final concern: a boilerplate checkbox on the second page of one of the warrants that we did obtain from the Sheriff’s Department indicates that it is sealed until further order of the Court, even though the issuing magistrate specifically refused the requested sealing order. *Compare* VVSW18-1048 at 2 ¶ 9 (box apparently checked by Sheriff’s Department purporting to seal all records “unless further ordered by the Court”) *with id.* at 2 (magistrate refused to approve sealing) (attached as Exhibit B to this letter). Because it appears that this application is a standard template and that the Sheriff’s Department always asks that these orders be sealed, this may lead to confusion and to the erroneous withholding from the public of files that a judge of this Court has refused to seal.

8. Conclusion

For these reasons, we ask the Court take the following steps to ensure that the public has access to this Court’s judicial records as required by law:

- a. Review the files specified in Exhibit A to determine whether they are in fact sealed.
- b. Unseal any files or parts of files that are not properly sealed under Rule of Court 2.551(h) and the standards discussed above.
- c. Take whatever steps are necessary to ensure that similar files – both in the past and in the future – are open to the public as required by law.



Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Thank you for your kind consideration and please advise us as to your position on this issue on or before June 5, 2019. If you or your colleagues or staff should have any questions or concerns you would like to discuss, please do not hesitate to contact us.

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'Michael T. Risher'.

for Michael T. Risher (CA State Bar No. 191627)
Law Office of Michael T. Risher
2081 Center St. #154
Berkeley CA 94702
Email: michael@risherlaw.com
T: (510) 689-1657
F: (510) 225-0941

Stephanie J. Lacambra (CA State Bar No. 232517)
David Greene (CA State Bar No. 160107)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
T: (415) 436-9333 x130
F: (415) 436-9993
Email: stephanie@eff.org; davidg@eff.org

cc:
Miles Kowalski (CA State Bar No. 257269)
Deputy County Counsel
Michelle D. Blakemore (CA State Bar No. 110474)
County Counsel
Office of County Counsel
385 North Arrowhead Avenue, 4th Floor
San Bernardino, CA 92415-0140
T: (909) 387-5455
F: (909) 387-4381
Email: Miles.Kowalski@cc.sbcounty.gov



Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Exhibit A: Search Warrants to be Unsealed

1. SBSW 18-0259
2. SBSW 18-0256
3. SBSW 18-0269
4. SBSW 18-0275
5. SBSW 18-0278
6. SBSW 18-0281
7. SBSW 18-0292
8. SBSW 18-0298
9. SBSW 18-0293
10. SBSW 18-0302
11. SBSW 18-0297
12. VVSW 18-0164
13. SBSW 18-0849
14. SBSW 18-0850
15. VVSW 18-1051
16. VVSW 18-1047
17. SBSW 17-0615
18. SBSW 17-0694
19. SBSW 17-0695
20. SBSW 17-0834
21. SBSW 17-0890
22. SBSW 17-0892



Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Exhibit B: Search Warrant No. VVSW18-1048

VVSW 18-1048

STATE OF CALIFORNIA, COUNTY OF SAN BERNARDINO

RETURN TO SEARCH WARRANT

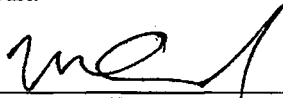
The following property was taken from AT&T Cell phone [REDACTED] and seized pursuant to Penal Code Section 1524 by virtue of a Search Warrant dated 05/21/2018, and executed by the Honorable Judge D. Harris of the Superior/Municipal Court, Victorville Judicial District, County of San Bernardino, State of California.

ITEMS SEIZED:

1.) Digital Records

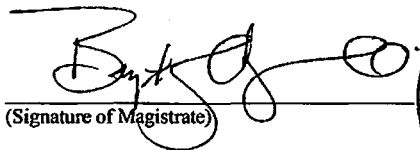
I, Deputy Michael Corral of the San Bernardino County Sheriff's Department, by whom this Search Warrant was executed, do swear that the above inventory contains a true and detailed account of all the property taken by me under this warrant.

It is further requested that for the purpose of retaining custody of this property and conducting further investigation and/or analysis of the property seized, that the court order the San Bernardino County Sheriff's Department to retain the property until it is brought before the court for hearing or other disposition, and/or that the San Bernardino County Sheriff's Department release the property to appropriate investigators, victims, and/or laboratories for further investigation and analysis without further order of this court.



(Signature of Affiant)

Deputy Sheriff, San Bernardino County Sheriff's Department



(Signature of Magistrate)

Judge of the Superior/Municipal Court, Victorville Judicial District, County of San Bernardino, State of California



FILED
SUPERIOR COURT OF CALIFORNIA
COUNTY OF SAN BERNARDINO
VICTORVILLE DISTRICT

JUN 11 2018

BY 
WENDY ALVAREZ-MEDINA, DEPUTY

Subscribed and sworn to before me this 11 day of June, 2018

**STATE OF CALIFORNIA - COUNTY OF SAN
BERNARDINO**

SW NO. VVSW 18-1048

SEARCH WARRANT

**THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY PEACE OFFICER IN
THE COUNTY OF SAN BERNARDINO:**

THE UNITED STATES MARSHALS SERVICE and the SAN BERNARDINO COUNTY SHERIFF'S DEPARTMENT by Task Force Officer Scott Abernathy and, under authority of 28 U.S.C. Sec 564, and 566, and pursuant to special apprehension authority delegated to the United States Marshals Service by the Attorney General of the United States proof by affidavit and under penalty of perjury having been sworn to this day before me that there is probable cause for believing that the property and/or person described below may be found at the location(s) set forth below and is lawfully seizable pursuant to Penal Code Section 1524 and 1534 as indicated below by "x"(s) in that it:

- ☐ was stolen or embezzled
- ☐ was used as the means of committing a felony
- ☒ is possessed by a person with the intent to use it as means of committing a public offense or is possessed by another to whom he or she may have delivered it for the purpose of concealing it or preventing its discovery
- ☐ tends to show that a felony has been committed or that a particular person has committed a felony
- ☐ tends to show that sexual exploitation of a child, in violation of Penal Code Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring
- ☒ the location of a person for whose arrest there is probable cause for: [REDACTED] DOB: [REDACTED] for CA Penal Code 664/187; Attempted Murder
- ☒ is information to be received from the use of the Target Telephone(s), as tracking device(s) that constitutes evidence that tends to show that a felony has been or is being committed, tends to show that a particular person has committed or is committing a felony, or will assist in locating an individual who has committed or is committing a felony.

Additional Orders:

VVSW 18-1048

1. **Seal Unrelated Information:** As required by California Penal Code § 1546.1(d)(2), any information obtained through the execution of this warrant that is unrelated to the objective of the warrant shall be sealed by the affiant and shall not be subject to further review, use, or disclosure absent an order from the Court. Pursuant to CA Penal Code §§ 638.52 and 638.54, no content data is to be obtained and no SEALING of unrelated data is required.
2. **Production:** The listed service providers in Attachment A are commanded, within five (5) business days after receipt of this Search Warrant, to deliver by mail or otherwise, to the above-named law enforcement officer, together with the declaration as set forth below, a true, durable and legible copy of the requested records (See California Penal Code § 1524.2).
3. **Verification:** The custodian shall complete and sign the "Declaration of Custodian" which accompanies this Search Warrant. The "Declaration of Custodian" shall be returned with a copy of the requested records. (See California Penal Code §§ 1546.1(d)(3), 1524.2 (b)(4).)
4. **Disposition of Communications and/or Data:** Pursuant to California Penal Code §§ 1528(a) and 1536, all communications and/or data seized pursuant to this Search Warrant shall be retained in affiant's custody pending further Court order.
5. **Night Service Authorization:** This warrant may be served on provider at any hour of the day or night.
☒ Order granted
☐ Order not granted and/or not applicable
6. **Non-Disclosure Order:** Applicant's declaration has established grounds for a non-disclosure order pursuant to Penal Code § 1546.2 and 18 U.S.C. §§ 2705(b). The listed service providers in Attachment A are ordered not to notify the subscriber or any other person of the existence of this warrant pending further Court order.
☒ Order granted
☐ Order not granted and/or not applicable
7. **Delay of Notification:** This application requests that the notice required under Penal Code § 1546.2 be delayed for ninety (90) days as provided in subsection (b)(1). If investigators are able to obtain sufficient evidence to arrest all the suspects in this case prior to the end of the 90-day period, notice will be provided upon that arrest or within forty-eight (48) hours. Based upon the reading of the Search Warrant and Affidavit in support thereof, the notice required under § 1546.1 is hereby delayed for ninety (90) days, it appearing that there is reason to believe that the notification of the existence of the warrant to any person will result in one of the following:
☒ Endangering the life or physical safety of an individual
☒ Lead to flight from prosecution
☐ Lead to destruction of or tampering with evidence
☒ Lead to intimidation of potential witnesses
☒ Seriously jeopardize an investigation
☒ Unduly delay a trial or otherwise lead to an adverse result

8. **Extension of Time for Return:** The 10-day requirement for the Return to Search Warrant is extended in order to provide ample time for **the listed service providers in Attachment A** to provide the requested information. The Return to Search Warrant and Search Warrant are ordered to be filed with the Court within sixty (60) days of execution of the warrant.

☒ Order granted
☐ Order not granted and/or not applicable

9. **Sealing of Search Warrant, Attachment A, Affidavit, and Return:** Affiant has established good cause for a sealing order and as such, this Search Warrant, Attachment(s), the supporting Affidavit, and the Return are ordered sealed and shall not become a public record. This Search Warrant, Attachment(s) Affidavit, and Return shall be delivered into the custody of the Clerk of the Superior Court and remain sealed in the custody of the Clerk unless further ordered by the Court.

☒ Order granted
☐ Order not granted and/or not applicable

YOU ARE THEREFORE COMMANDED TO SEARCH: and obtain information to be received from the use of the **Subject Telephone(s)** in order to obtain real-time tracking information, including but not limited to satellite Global Positioning System (GPS), latitude and longitude coordinates and/or other Precise Location information relating to the following **Subject Telephone(s)**, and cell-site/tower data information for signals transmitted to and from the following **Subject Telephone(s)** by executing the warrant by serving the named third party possessor of the location data within 30 days after issuance.

Subject Telephone #1: A cellular telephone serviced by AT&T Wireless, assigned telephone number [REDACTED] believed to be prepaid cellular device (hereinafter referred to as the "**Subject Telephone(s)**" or "**Subject Telephone Number(s)**").

PROBABLE CAUSE having been shown by the applicant, TFO Michael Corral, certifying that the information likely to be obtained from the installation and use of the pen/trap device is relevant to an ongoing criminal investigation being conducted by the United States Marshals Service, in coordination with San Bernardino County Sheriff's Department, in connection with possible violations by [REDACTED] DOB [REDACTED] for violation of California Penal Code 664/187; Attempted Murder and pursuant to Title 18, United States Code, §§ 3122 and 3123 and California Penal Code §§ 638.50, 638.51, 638.52, 638.53 and 1546.1(b)(5); and further, the Government having offered specific and articulable facts showing that there are reasonable grounds, as well as probable cause, to believe that the records or information sought is relevant and material to said ongoing criminal investigation, pursuant to Title 18, United States Code, § 2703(c) and (d), and California Penal Code § 1546.1(b)(1).

And by Order, attached hereto as Attachment A, and further incorporated by reference.

AND TO SEIZE IT/THEM IF FOUND and bring it/them forthwith before me, or this Court, at the courthouse of this Court except that the 10-day requirement for the Return to Search Warrant is extended, as referenced above, and the Return is authorized within sixty (60) days of execution of the Warrant. Federal law enforcement agents employed by the United States Marshals Service are authorized to assist in the service of this Search Warrant/Order. This Search Warrant/Order and incorporated Affidavit was sworn to as true before me this 21st day of May 2018, at 1548 A.M. / P.M. Wherefore, I find probable cause for the issuance of this Search Warrant/Order and do issue it.

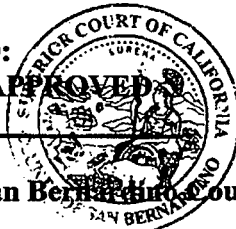
SEALING APPROVED:

NIGHT SEARCH APPROVED:

90 DAY DELAYED NOTICE APPROVED:

[Signature]
 [Signature of Magistrate]

Judge of the Superior Court, San Bernardino County



YES [] NO [X]
 YES [X] NO []
 YES [] NO [X]

FOR THE FOLLOWING PROPERTY/PERSONS: This Search Warrant is for the purpose of receiving information from the use of the **Subject Telephone(s)**, including but not limited to real-time monitoring of location data from satellite GPS, latitude and longitude coordinates, and/or other Precise Location information, and cellular site/tower data concerning the **Subject Telephone(s)**.

PROBABLE CAUSE HAVING BEEN SHOWN, THIS COURT HEREBY ORDERS:

Cellular telephone provider(s) known as: VERIZON WIRELESS, AT&T WIRELESS, AT&T, ALLEGIANCE TELECOM, SBC, VERIZON, VERIZON OF CALIFORNIA, AT&T BROADBAND, CRICKET, METRO PCS, LEAP WIRELESS, CINGULAR WIRELESS, CONEXONE WIRELESS, CONNECT COMMUNICATIONS CORP., CONNECT COMMUNICATIONS, COX COMMUNICATIONS, COX TELECOM, GST TELECOM XO, INTOUCH COMMUNICATIONS, MCI WORLDCOM, MEDIA ONE COMMUNICATIONS, NEXTEL COMMUNICATIONS, OPTEL, QUEST, QWEST WIRELESS, SPRINT LONG DISTANCE, SPRINT PCS, SPRINT SPECTRUM L.P., T-MOBILE COMMUNICATIONS, TELEPACIFIC COMMUNICATIONS, TIME WARNER TELECOM, M-POWER COMMUNICATIONS, U.S. SPRINT, QWEST, AND XO CALIFORNIA INC., upon the request of Inspectors of the United States Marshals Service, shall provide the following information and services without delay:

- (a) IT IS ORDERED, based on findings of probable cause and that the information sought is relevant to the ongoing criminal investigation pursuant to CA Penal Code §§ 638.52 et seq, 1546.1(b)(5) and Title 18, United States Code, §§ 3122(a)(2) and 3123(a)(2), that the U.S. Marshals Service is authorized to install and use a pen register, to register numbers dialed or otherwise transmitted from telephone number [REDACTED] (hereinafter referred to as the "**Subject Telephone Number(s)**"), to record the date and time of such dialings or transmissions, and to record the length of time the telephone receiver in question is "off the hook" for incoming or outgoing calls, LTE incoming and outgoing calls, for a period of thirty (30) days from the date of this Order. The installation and use of a trap and trace device, including the "caller identification feature," on the **Subject Telephone Number(s)**, to capture and record the incoming electronic or other impulses which identify the originating numbers of wire or electronic communications, and to record the date, time, and duration of calls created by such incoming impulses, is also authorized for a period of thirty (30) days from the date of this Order, and that tracing operations including the use of the "caller identification feature" be without geographical limits.
- (b) IT IS FURTHER ORDERED, pursuant to CA Penal Code §§ 638.52 et seq, 1546.1(b)(1) and (5) and Title 18, United States Code, §§ 2703(c) and (d), 3122 and 3123, and the Court's findings of probable cause and that the information sought is relevant and material to the ongoing criminal investigation, that Verizon, Verizon of California, Qwest, Media One Communications, M-Power Communications and Allegiance Telecom (hereinafter referred to as "the local carriers"); AT&T, US Sprint, MCI World Com (hereinafter referred to as "the long distance carriers"); Verizon Wireless, AT&T Wireless, Sprint Spectrum L.P., Sprint PCS, Cricket, T-Mobile Communications, and Metro PCS (hereinafter referred to as "the wireless carriers"); and any other local, long distance or wireless carrier shall provide subscriber information including, but not limited to: name and billing address, call activity, (which includes all inbound and outbound telephone calls) on all telephone numbers, call detail reports and non-content text messaging incoming or outgoing activity data, whether published or nonpublished (listed or unlisted), blocked or unblocked, LTE, to include cell site/sector beginning thirty (30) days prior from the date of this Order and continuing through thirty (30) days from the date of this Order, and that the local and long distance or wireless carrier(s) shall activate the dial digit extraction (AKA punch list) feature, along with 24 hour expedited service on all telephone numbers upon oral or written request made by Inspectors of the United States Marshals Service.

- (c) IT IS FURTHER ORDERED, that the “wireless carriers,” based upon the Court’s findings of specific and articulable facts supporting probable cause and that the information is relevant and material to an ongoing criminal investigation, shall provide, on an ongoing and/or real time basis, the location of cell-site/sector (physical address) at call origination (for outbound calls) to United States Marshals Service Headquarters CALEA network, call termination (for incoming calls) and during the progress of a call via United States Marshals Service Headquarters CALEA network, and direction and strength of signal, call progress locations (Automated Message Accounting (AMA) Data), dialed digit information and extended digit dialing (excluding content), and a listing of all control channels and their corresponding cell-sites for the **Subject Telephone Number(s)**, including local and “roam” mode cellular telephone calls, beginning from the date of the Court Order and continuing for thirty (30) days from the date of this Order.
- (d) IT IS FURTHER ORDERED, pursuant to California Penal Code §§ 629.50, 629.51, 629.52, 629.90, 629.91, 1546.1(b)(1) and (5) and 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d) and the Court’s findings of probable cause and that the requested information is relevant and material to the ongoing criminal investigation, that AT&T Wireless, shall supply for the Subject Telephone Number(s): the subscriber name and address, call detail records and incoming and outgoing communication session records relating to all voice, push-to-talk, non-content text messages, SMS, MMS, data sessions, packet data activity records, IP logs, destination port logs, origination port logs, socket address logs, etc. (including for phone applications purchased or downloaded), Per Call Measurement Data (PCMD), Trucall record data, LTE and any other stored records pertaining to packet data transmission, signaling, and delivery for the **Subject Telephone Number(s)** starting from March 30, 2018 to the present to include historical cell-site/sectors (physical address) and historical GPS Precision Location and/or latitude and longitude information upon oral or written request made by Inspectors of the United States Marshals Service.
- (e) IT IS FURTHER ORDERED, that this authorization for the installation and use of a pen register and trap and trace device, including the “caller identification feature,” and for the disclosure of cell-site location information, GPS, latitude and longitude information, and other Precise Location information, applies not only to the telephone number listed above for the **Subject Telephone(s)**, but also to any changed telephone number(s) subsequently assigned to the same instrument bearing the same Mobile Station ID (MSID), Mobile Equipment Identifier (MEID), Mobile Identification Number (MIN), International Mobile Subscriber Identity (IMSI), Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), Subscriber Identity Module (SIM) or Media Access Control addresses (MAC) and/or or any new MSID, MEID, MIN, IMSI, ESN, IMEI, SIM, or MAC, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the Subject Telephone(s) within the thirty (30) day period authorized by the Warrant/Order; and/or any new MSID, MEID, MIN, IMSI, ESN, IMEI, SIM, or MAC assigned to the Subject Telephone(s) or new/changed telephone number(s), whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the Subject Telephone(s) within the thirty (30) day period authorized by this Warrant/Order.
- (f) IT IS FURTHER ORDERED, in the event the Subject Telephone Number(s) was changed by the subscriber or customer during the thirty (30) days prior to the date of this Order, that the Service Provider shall provide the United States Marshals Service with the new unique telephone number, hardware or network identity number. The Court finds Applicant has offered specific and articulable facts showing there are reasonable grounds and probable cause to believe that the identification of any telephone number or unique device identifier which was assigned within the thirty (30) day period prior to the date of the Order is also relevant and material to the ongoing criminal investigation. Further, the Subject Telephone’s Service Provider, and all other telecommunications providers, persons or entities providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the Order, shall notify agents of the United

States Marshals Service, upon oral or written request, of any and all subscriber identity changes (including without limitation, additions, deletions, and transfers of telephone numbers, hardware, network identity or subscriber/customer/user identity) regarding the Subject Telephone(s) for a period of thirty (30) days from the date of this Order.

- (g) IT IS FURTHER ORDERED, that the **Subject Telephone Number(s)** remain active and in service and if the cellular telephone has been targeted for deactivation due to non-payment or breach of contract, that the Service Provider shall advise the United States Marshals Service and the United States Marshals Service will incur the future billing costs at the point of deactivation and compensate the wireless carrier for such additional billing costs beginning from the date of deactivation and continuing through the thirty (30) day time period authorized by this Order.
- (h) IT IS FURTHER ORDERED, based on probable cause having been shown, that "the wireless carrier" AT&T Wireless provide Inspectors of the United States Marshals Service, at their request, GPS latitude / longitude coordinates, and/or other Precision Location Information for the Subject Telephone Number(s) for thirty (30) days from the date of this Order.
- (i) IT IS FURTHER ORDERED, pursuant to CA Penal Code §§ 638.52 et seq, 1546.1(b)(1) and (5) and Title 18, United States Code, §§ 2703(c) and (d), 3122 and 3123 and the Court's finding of probable cause and a finding that the information sought is relevant and material to an ongoing criminal investigation, that the local, long distance and wireless carriers shall furnish Inspectors of the United States Marshals Service and the San Bernardino County Sheriff's Department forthwith, for thirty (30) days from the date of the Order: Direct connect, dispatch, or group call connections or attempts, non-content Short Message Service (SMS) data, all cell-site activations and sectors, together with a complete listing of cell site identification numbers, physical addresses, latitude and longitude records, sector identifiers, and true orientations of all cell-sites and sectors in the market where the **Subject Telephone(s)** may be located; together with a nationwide System Identity/Billing Identity (SID/BID) listing; and, upon request, an engineering map or maps identifying same (if the provider possesses such a map). Further, that the AT&T Wireless shall provide a list of control/radio channels and PN offsets (by sector) with their corresponding cell-sites in the market where the **Subject Telephone(s)** may be located. Further, that the PROVIDER shall provide all additional technical assistance necessary to accomplish the installation and use of the pen register-trap and trace device, including the "caller identification feature," unobtrusively and with minimum interference with the services that are accorded the persons whose dialings or transmissions are the subject of the pen register-trap and trace device.
- (j) IT IS FURTHER ORDERED, probable cause having been shown, pursuant to CA Penal Code §§ 629.66, that this entire Search Warrant be sealed until otherwise ordered by the Court, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any Service Provider or other person, and that the local, long distance and wireless carriers and their representatives, agents and employees shall not disclose in any manner, directly or indirectly, by any action or inaction, the existence of this Warrant/Order or the existence of the above-described investigation, to the listed subscriber for the **Subject Telephone Number(s)**, the occupant of said premises, the subscribers of the incoming calls to or outgoing calls from the **Subject Telephone Number(s)**, or to any other person, in full or redacted form, unless or until otherwise ordered by the Court.
- (k) IT IS FURTHER ORDERED, probable cause having been shown, pursuant to CA Penal Code §§ 1546.2, that notification be delayed for ninety (90) days based on the statement in the attached Affidavit and a finding of adverse results in that notification would seriously jeopardize the ongoing investigation and cause undue delay of trial, and further cause the fugitive of the investigation to flee from prosecution. Upon arrest of the fugitive, if located before the 90-day expiration period, the

VVSW 18-1048
affiant shall file a return to the warrant within sixty (60) days of the execution of the warrant and serve a copy of the warrant to the authorized handler of the device and the notice of the nature of the government's investigation.

- (1) IT IS FURTHER ORDERED, as part of the receipt of the requested data, that the U.S. Marshals Service is prohibited from seizing any tangible property, or any other prohibited wire or electronic information which would require an application under Penal Code §§ 629.50 et seq. The U.S. Marshals Service is not prohibited from doing so in relation to any other investigation or order authorized by law.

AND TO SEIZE IT/THEM IF FOUND and bring it/them forthwith before me, or this Court, at the courthouse of this Court except that the 10-day requirement for the Return to Search Warrant is extended, as referenced above, and the Return is authorized within sixty (60) days of execution of the Warrant/Order. Federal law enforcement agents employed by the United States Marshals Service are authorized to assist in the service of this Search Warrant/Order. This Search Warrant/Order and incorporated Affidavit was sworn to as true before me this 21st day of May 2018, at 1:54 A.M. / P.M. Wherefore, I find probable cause for the issuance of this Search Warrant/Order and do issue it.

Blam
[Signature of Magistrate]

Judge of the Superior Court, San Bernardino County



STATE OF CALIFORNIA - COUNTY OF SAN
BERNARDINO

SW NO. VVSW 18-1048

AFFIDAVIT

I, Michael Corral, being duly sworn, hereby depose and say that: I am a Deputy with the San Bernardino County Sheriff Department, State of California, and have been so employed since September 2010. As part of my regular assigned duties, I conduct investigations regarding the whereabouts of Federal and State Fugitives, most of which are violent offenders with extensive criminal histories. I am a duly commissioned federal law enforcement officer of the United States Marshals Service and San Bernardino County Sheriff, currently assigned to the Pacific Southwest Regional Fugitive Task Force – California. Deputy United States Marshals are empowered under Title 28, U.S.C. §§ 566 & 564 to carry firearms, execute state and federal warrants, make arrests for offenses against the United States of America and to perform other law enforcement duties as authorized by law.

In the experience of Deputy Michael Corral, fugitives, their family and close associates communicate with each other via cell phone or social media through multiple accounts and cellular devices. This method of communication is employed to assist the fugitive in avoiding being detected by law enforcement. As chronicled in past investigations, it is the experience of Deputy Michael Corral that these set of behaviors and actions provide the fugitive bearings to avert all contact with law enforcement. Based on my experience, Deputy Michael Corral has worked multiple cases in which fugitives will change their numbers or purchase new communication devices after being notified by family and friends that law enforcement is attempting to locate them, or shortly after committing a crime. Fugitives tend to discard, change their cellular number or purchase new cellular devices via prepaid phones after becoming a Fugitive from Justice. In the experience of Deputy Michael Corral, fugitives will instruct close family members and friends to do the same and / or on a frequent basis change devices to avoid detection. History has proven, after a fugitive establishes a new phone number and device, they will communicate with close family and friends via the new cell phone and sometimes instruct "top callers" to establish a new cell phone number and device for future communication. Additionally, the call historical detail records and subscriber information for the numbers the fugitive is in contact with have yielded information that is relevant and provides lead information for fugitive investigations. Lead information consists of names of family members, friends, associates, frequently visited locations and other individuals who can assist in the apprehension of the fugitive. As a result, the additional information sheds light on any individuals who may be harboring or aiding the wanted fugitive. In the experience of Deputy Michael Corral, fugitives will continue to keep in contact with close family and friends via cell phone. Furthermore, if the fugitive of justice or user of the **Subject Telephone** is informed that a warrant has been executed to allow for tracking of the **Subject Telephone(s)**, it would alert the user/subscriber and impede law enforcement's ongoing investigation. Consequently, this would prompt the person of interest to discard or "dump" the **Subject Telephone**. As a result of this notification, there will be a delay in the apprehension of the fugitive causing prolonged flight from prosecution, serious jeopardy to an investigation, or unjust delay of trial.

I receive, on an ongoing basis, training in various laws, regulations, and techniques related to my employment as a Deputy Sheriff. I have successfully completed the following training courses:

I, Deputy Michael Corral, am currently assigned to the Specialized Enforcement Division / SWAT. I currently hold an Advanced POST Certification. I am also SMASH certified, advanced Gang investigator and a major accident investigator. During the past 6 years, I have conducted numerous investigations of murders,

kidnappings, burglaries, assaults, grand theft, distribution, sales and use of controlled substances and other felony crimes. I have compiled information; collected evidence; and interviewed victims, witnesses, and informants to support the filing of criminal complaints. I have also been trained in the identification of potential Marijuana cultivation sites and assisted in the processing of Marijuana cultivation sites. I have been trained in the apprehension of fleeing felons, as well as organized and participated in the apprehension of numerous fugitives from justice. I am also cross sworn as a US Marshal and I have located and assisted others in locating several wanted subjects.

APPLICATION AND STATEMENT OF PROBABLE CAUSE

Your Affiant, in coordination with the United States Marshals Service, hereby applies for a Search Warrant/Order authorizing 1) the use of a "Pen Register" and "Trap-and-Trace" device for a period of thirty (30) days from the date of the Warrant/Order on AT&T Wireless telephone number(s) [REDACTED] subscribed to by an unknown subscriber (hereinafter the **Subject Telephone Number(s) or Subject Telephone(s)**); 2) the disclosure of subscriber and other historical and real-time information and records relating to the Subject Telephone Number(s), as further requested herein and in the attached proposed Warrant/Order; 3) the disclosure of subscriber names and addresses whether listed, unlisted or non-published, and the periods of telephone activation for numbers dialed or otherwise transmitted to and from the **Subject Telephone Number(s)**, along with 24 hour expedited service on all telephone numbers upon oral or written demand by investigators of the United States Marshals Service; 4) the disclosure, on an ongoing and real time basis and for a period of thirty (30) days from the date of the Warrant/Order, GPS, latitude/longitude coordinates, or other Precision Location, the location information for the **Subject Telephone Number(s)**, the location of cell-site/sector (physical address) at the call origination (for outbound calling), call termination (for incoming calls), and during the progress of a call; and the direction and strength of the signal, for the **Subject Telephone Number(s)**, which will help reveal the general geographical position and movement of the cellular phone handset subscribed to the **Subject Telephone Number(s)**, to aid in locating and apprehending [REDACTED] DOB [REDACTED] wanted for a violation of Calif. Penal Code Section 664/187; Attempted Murder. The information sought by the court Warrant/Order is relevant and material to the above listed investigation.

1. A "Pen Register" allows a telephone utility to capture the telephone numbers dialed out by the target telephone; a "Trap-and-Trace" device allows a telephone utility to capture the telephone numbers of telephones that call the **Subject Telephone Number(s)**.

2. PROBABLE CAUSE:

On Saturday, May 19, 2018, Deputies from the Barstow Sheriff station were dispatched to the area of Yermo Road and Interstate 15 Freeway in Yermo, California. Through investigation, it was learned that the Victim, [REDACTED], was staying with her boyfriend [REDACTED] (Date of birth [REDACTED]), at the El Rancho Motel in Yermo. [REDACTED] and [REDACTED] were involved in a verbal argument, when [REDACTED] called her family to pick her up from the location. [REDACTED] told [REDACTED] if she gets into a vehicle he will shoot her in the head.

[REDACTED] continued and got into the vehicle, which was occupied by two additional people. [REDACTED] left the motel. [REDACTED] got into his vehicle, a white 2008 Infiniti G35, bearing license plate [REDACTED] and gave chase to [REDACTED] vehicle. [REDACTED] aggressively pulled in front of [REDACTED] vehicle and forced her to pull the vehicle off the road way edge. [REDACTED] pointed a handgun at the vehicle and all the occupants inside the vehicle. [REDACTED] started shooting the vehicle multiple times. [REDACTED] vehicle was hit several times with bullets. [REDACTED] vehicle was able to drive away without further incident.

Deputies searched the area of the original incident and located approximately eight (8) fired casing of a .45 caliber round. [REDACTED] has not be located in the area. On May 20, 2018, [REDACTED] contacted [REDACTED] via telephone messages. [REDACTED] requested to meet with [REDACTED] in an attempt to apologize. [REDACTED] has been contacting [REDACTED] from the number of [REDACTED] each time he tries to meet up with her.

██████ is currently a wanted fugitive and is considered armed and dangerous. ██████ has a history of violence and multiple arrests. An arrest warrant was authored for the apprehension of ██████ with a bail of \$1,000,000.00.

3. Deputy Michael Corral further advises that the general geographic location of the **Subject Telephone Number(s)** derived from cell-site and GPS (Global Positioning System), latitude and longitude coordinates, and/or other Precision Location information associated with the **Subject Telephone Number(s)** can be used to verify the identification and location of the user of the **Subject Telephone Number(s)** thereby aiding in apprehension of the named fugitive.
4. Because there are reasonable grounds to believe that such information is relevant and material to the ongoing investigation, as well as probable cause to believe this information will aid in locating the fugitive for apprehension purposes, your affiant requests that the local, long distance and wireless carriers listed in the proposed Order, filed concurrently herewith, and continuing thirty (30) days from the date of this Order upon oral or written demand by agents of the United States Marshals Service, also be ordered to disclose, on an ongoing and/or real time basis, the location of cell-site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls) and during the progress of a call, GPS, latitude and longitude coordinates, and/or other Precision Location information, and the strength of signal, for the **Subject Telephone Number(s)**.
5. Because there are reasonable grounds to believe that such information is relevant and material to the ongoing investigation, Deputy Michael Corral request that the local, long distance and wireless carrier(s) listed in the proposed Order, filed concurrently herewith, be ordered to supply subscriber names and addresses, whether listed or unlisted, and periods of telephone activation for numbers dialed or otherwise transmitted from (as captured by the pen register) and dialed or otherwise transmitted to (as captured by the trap and trace device) the **Subject Telephone Number(s)**, beginning on March 30, 2018 and continuing through thirty (30) days from the execution of this Order, upon oral or written demand by agents of the United States Marshals Service.
6. It is further requested that that the authorization for the installation and use of a pen register and trap and trace device, including the "caller identification feature," and for the disclosure of cell-site location information, GPS, latitude and longitude information, and other Precise Location information apply not only to the telephone number listed above for the Subject Telephone Number(s), but also to any changed telephone number(s) subsequently assigned to the same instrument bearing the same Mobile Station ID (MSID), Mobile Equipment Identifier (MEID), Mobile Identification Number (MIN), International Mobile Subscriber Identity (IMSI), Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), Subscriber Identity Module (SIM) or Media Access Control addresses (MAC); and/or or any new MSID, MEID, MIN, IMSI, ESN, IMEI, SIM, or MAC, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the Subject Telephone(s) within the thirty (30) day period authorized by the Warrant/Order; and/or to any new MSID, MEID, MIN, IMSI, ESN, IMEI, SIM, or MAC assigned to the **Subject Telephone(s)** or new/changed telephone number(s), whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the Subject Telephone(s) within the thirty (30) day period authorized by this Warrant/Order.
7. Applicant further requests that in the event the Subject Telephone's unique telephone number, hardware or network identity number identified in the Warrant/Order as associated with the Subject Telephone(s) was changed by the subscriber or customer during the thirty (30) days prior to the date of the Warrant/Order, the Service Provider be directed to provide the United States Marshals Service with that new unique telephone number, hardware or network identity number. Fugitives and other criminals are known to change telephone numbers or device identifiers, sometimes on a frequent basis, in a deliberate and calculated effort to avoid detection by law enforcement and despite law enforcement's due diligence in attempting to identify the current telephone number or unique device identifier of the target device at the time legal process is sought. Law enforcement's ability to learn the "new" telephone number or unique device identifier is essential to its ability

to locate the fugitive. Law enforcement's knowledge of this "new" telephone number or unique device identifier would allow law enforcement to obtain additional legal processes to investigate the telephone number or unique device identifier further, in an effort to locate the fugitive's whereabouts and to apprehend him/her on the outstanding arrest warrants, further ensuring public safety. Accordingly, Applicant has offered specific and articulable facts showing there are reasonable grounds, and probable cause, to believe that the identification of any telephone number or unique device identifier which, within the thirty (30) day period prior to the Warrant/Order's issuance, replaced the telephone number or unique device identifier associated with the **Subject Telephone(s)** for which probable cause of its association with the fugitive has already been established herein and pursuant to the Affidavit, is also relevant and material to the ongoing criminal investigation.

8. It is further requested, that AT&T Wireless keep the **Subject Telephone Number(s)** active and in service, and that if the cellular telephone has been targeted for deactivation due to non-payment or breach of contract, the Service Provider shall advise the United States Marshals Service and that the United States Marshals Service will incur the future billing costs at the point of deactivation and compensate the wireless carrier for such additional billing costs beginning from the date of deactivation and continuing through the thirty (30) day period from the date of the Warrant/Order.

9. Based on the information provided in this application, Deputy Michael Corral believes that the disclosure of the requested Court Order may result in the flight from potential prosecution or the destruction of or tampering with evidence, or may otherwise seriously jeopardize the investigation. Therefore, pursuant to California Penal Code § 629.66, I further request that the Court seal this record and direct the local, long distance and wireless carriers listed in the proposed Order, filed concurrently herewith, and their representatives, agents and employees, not to disclose in any manner, to the listed subscriber for the **Subject Telephone Number(s)**, or to any other person, the existence of this Order, in full or redacted form, or of this investigation unless otherwise ordered by this Court.

10. Based on my training and experience, Deputy Michael Corral knows that fugitives often move around at all hours of the day and night in order to avoid law enforcement detection; because of this, the location where a fugitives might ultimately be found is often unpredictable. I am requesting that this Court authorize the monitoring of the requested GPS, latitude and longitude / or Precision Location tracking of the **Subject Telephone(s)** 24 hours per day, seven days a week, for a period of thirty (30) days from the date of the Order requested herein.

11. JUSTIFICATION FOR DELAY OF NOTIFICATION COURT ORDER PURSUANT TO A FINDING OF PROBABLE CAUSE UNDER CALIFORNIA PENAL CODE 1546.2;

I, Deputy Michael Corral, hereby applies to this Court, pursuant to § 1546.2(b)(2) of the Penal Code, for an order delaying for ninety (90) days the notification required by § 1546.2(a) of the Penal Code in connection with this Search Warrant requested on May 21, 2018 that was issued to obtain electronic information records pertaining to AT&T Wireless **Subject Telephone Number (s)** [REDACTED] which will help aid in the investigation on [REDACTED] DOB [REDACTED] whereabouts. It is FURTHER REQUESTED pursuant to CA Penal Code § 1546.2 (b)(3) that based on the supporting Affidavit, the Court delay the notification for a period of ninety (90) days justified by the following adverse results because it is believe that the notice will: 1. LEAD TO FURTHER FLIGHT FROM PROSECUTION and 2. OTHERWISE SERIOUSLY JEOPARDIZE AN INVESTIGATION OR UNDULY DELAY A TRIAL.

That is, in the experience and training of Deputy Michael Corral, once a fugitive from justice or user of the **Subject Telephone(s)** is informed that a warrant has been executed to allow for a tracking on the **Subject Telephone(s)**, it would alert the user/subscriber to law enforcement's ongoing investigation causing the fugitive

to undertake additional efforts, to including relating to his communications, to subvert law enforcement's efforts to locate him/her for apprehension purposes.

CONCLUSION

Based upon the above listed facts and circumstances, I believe there is evidence the fugitive is currently in possession of the aforementioned cellular device. I also believe that evidence of the fugitive's whereabouts will be located with the information requested in this affidavit, ultimately leading to an arrest. Therefore, I am respectfully requesting that a Search Warrant/Order be issued in this case.

Sworn to and subscribed before me on this 21st day of May, 2018 at 1548 AM / PM 8

Wherefore, he/she requests that this Search Warrant/Order be issued.

NIGHT SEARCH REQUESTED: YES ☐ NO ☐;

SEALING REQUESTED: YES ☐ NO ☐;

90 DAY DELAYED NOTICE: YES ☐ NO ☐;

[Handwritten Signature]

[Signature(s) of Affiant(s)]

[Handwritten Signature]

[Signature of Magistrate]

Judge of the Superior Court, San Bernardino County

