Date of Hearing: January 14, 2020
Counsel: Nikki Moore

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Reginald Byron Jones-Sawyer, Sr., Chair

AB 904 (Chau) – As Amended January 6, 2020

SUMMARY: Clarifies that if a law enforcement agency utilizes software to track a person's movements, whether in conjunction with a third party or by interacting with a person's electronic device, the provisions for obtaining a tracking device search warrant apply.

EXISTING LAW:

1) Provides that the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.; Cal. Const., art. I, § 13.)

2) Provides that a search warrant is an order in writing, in the name of the people, signed by a magistrate, directed to a peace officer, commanding him or her to search for a person or persons, a thing or things, or personal property, and, in the case of a thing or things or personal property, bring the same before the magistrate. (Pen. Code, § 1523.)

3) Provides that a search warrant may be issued upon any of the following grounds:

   a) When the property was stolen or embezzled;

   b) When the property or things were used as the means of committing a felony;

   c) When the property or things 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 he or she may have delivered them for the purpose of concealing them or preventing them from being discovered;

   d) When the property or things to be seized consist of any item or evidence that tends to show that a felony has been committed or that a particular person has committed a felony;

   e) When the property or things to be seized consist of evidence that tends to show sexual exploitation of a child or possession of child pornography;

   f) When there is a warrant to arrest a person;

   g) When a provider of electronic communication or remote computing service has records or evidence showing that property was stolen or embezzled constituting a misdemeanor,

or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor, or in the possession of another to whom he or she may have delivered them for the purpose of concealment;

h) When the things to be seized include evidence showing failure to secure workers compensation;

i) When the property includes a firearm or deadly weapon and specified circumstances related to domestic violence, examination of a person's mental condition; protective orders, as specified;

j) When the information to be received from the use of a tracking device tends to show a felony or misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code;

k) For purposes of obtaining a sample of the blood of a person in a driving under the influence matter when the person has refused to submit or complete, a blood test as required, as limited and specified;

l) The property or things to be seized are firearms or ammunition or both that are owned by, in the possession of, or in the custody or control of a person who is the subject of a gun violence restraining order, as specified;

m) When the property or things to be seized include a firearm that is owned by, or in the possession of, or in the custody or control of, a person who is subject to the prohibitions regarding firearms pursuant to Section 29800 or 29805, and the court has made a finding pursuant to subdivision (c) of Section 29810 that the person has failed to relinquish the firearm as required by law;

n) When the property or things to be seized are controlled substances or a device, contrivance, instrument, or paraphernalia used for unlawfully using or administering a controlled substance pursuant to the authority described in Section 11472 of the Health and Safety Code.

o) When there is evidence that tends to show a violation of the Harbors and Navigation Code;

p) When the property or things to be seized consists of evidence that tends to show a specified misdemeanor offense of invasion of privacy; and,

q) When there is a vehicle collision resulting in death or serious bodily injury to a person which tends to show the commission of a felony or misdemeanor offense. (Pen. Code § 1524, subd. (a)(1)- (19).)

4) Permits a tracking device search warrant to be issued when the information to be received from the use of a tracking device constitutes evidence that tends to show that either a felony, or a misdemeanor violation of the Fish and Game Code and the Public Resources Code, and the device will assist in locating an individual who has committed or is committing a felony, or a misdemeanor violation of the Fish and Game Code or Public Resources Code. (Pen.

Code, § 1534.)

5) Provides that a tracking device search warrant may be issued as specified, and that the warrant shall identify the person or property to be tracked, and shall specify a reasonable length of time, not to exceed 30 days from the date the warrant is issued, that the device may be used. Permits the court to, for good cause, grant one or more extensions for the time that the device may be used. (Pen. Code, § 1534, subd. (b).)

6) Requires that the search warrant command the officer to execute the warrant by installing a tracking device or serving a warrant on a third-party possessor of the tracking data, and requires the officer to perform any installation authorized by the warrant during the daytime unless the magistrate, for good cause, expressly authorizes installation at another time. Requires execution of the warrant be completed no later than 10 days immediately after the date of issuance. (Pen. Code, § 1534, subd. (b).)

7) Provides that an officer executing a tracking device search warrant shall not be required to knock and announce his or her presence before executing the warrant. (Pen. Code, § 1534, subd. (b)(2).)

8) Requires, no later than 10 calendar days after the use of the tracking device has ended, the officer executing the warrant to file a return to the warrant. (Pen. Code, § 1534, subd. (b)(3).)

9) Requires, no later than 10 calendar days after the use of the tracking device has ended, the officer who executed the tracking device warrant to notify the person who was tracked or whose property was tracked as specified, and permits delay as specified. (Pen. Code, § 1534, subd. (b)(4).)

10) Authorizes an officer installing a device authorized by a tracking device search warrant to install and use the device only within California. (Pen. Code, § 1534, subd. (b)(5).)

11) Defines "tracking device" to mean any electronic or mechanical device that permits the tracking of the movement of a person or object. (Pen. Code, § 1534, subd. (b)(6).)

12) Enacts the California Electronic Communications Privacy Act ("CalECPA"), which generally prohibits a government entity from compelling the production of or access to electronic communication information or electronic device information without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, except for emergency situations. (Pen. Code, §§ 1546-1546.4.)

13) Provides that a government entity may access electronic device information by means of a physical interaction or electronic communication device only: pursuant to a warrant; wiretap; with authorization of the possessor of the device; with consent of the owner of the device; in an emergency; if seized from an inmate. (Pen. Code, § 1546.1, subd. (b).)

14) Specifies the conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, tracking device search warrant, or

consent of the owner of the device. (Pen. Code, § 1546.1, subd. (c).)

15) Allows a service provider to voluntarily disclose electronic communication information or subscriber information, when the disclosure is not otherwise prohibited under state or federal law. (Pen. Code, § 1546.1, subd. (f).)

16) Provides that if a government entity receives electronic communication voluntarily it shall destroy that information within 90 days except under specified circumstances. (Pen. Code, § 1546.1, subd. (g).)

17) Provides for notice to the target of a warrant or an emergency obtaining electronic information to be provided either contemporaneously with the service of the warrant or within three days in an emergency situation. (Pen. Code, § 1546.2, subd. (a).)

18) Allows a person in a trial, hearing, or proceeding to move to suppress any electronic information obtained or retained in violation of the Fourth Amendment or the CalECPA. (Pen. Code, § 1546.4, subd. (a).)

19) Makes it a public offense to knowingly access and without permission take, copy, or make use of any data from a computer, computer system, or computer network, or take or copy any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. (Pen. Code, § 502, subd. (b)(2).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Author's Statement**: According to the author, "The rights of individuals against unlawful search and seizure are enshrined in both the Constitutions of the United States (through the Fourth Amendment) and the State of California. Having stood for over 200 years, this basic human right has consistently been reinterpreted to account for changes in government, technology, and society. Judicial understanding of this right has morphed from an explicit right of privacy within the home and personal documents, to an expansive protection against the collection of information by the government in a great many applications. Most recently, the United States Supreme Court recognized in *Carpenter v. United States* that the use of cell phone location information by law enforcement is an invasion of personal privacy, which requires the granting of a search warrant.

   "This decision certainly represents a landmark case in the jurisprudence of the Supreme Court, but had limited applicability to the residents of California because this specific requirement has been applied to law enforcement agencies in California since 2012. With the rest of the country following suit, it is important that California continues to look ahead at the changing landscape of technology and maintains the lead in protecting our residents against unlawful search and seizure.

   "Penal Code Section 1534 currently requires search warrants prior to an officer 'installing a tracking device or serving a warrant on a third-party possessor of the tracking data.' It is, however, no longer necessary for an officer to make physical contact with a device, person, or vehicle to 'install' a 'device' in order to track an individual. On the contrary, a government

official need only have wireless access to download tracking software that will provide investigators with far more information than just a person's or a vehicle's location.

"AB 904 would make clear that a tracking device includes any software that permits the tracking of the movement of a person or object for purposes of the statute."

2) **Constitutional Protections Against Unreasonable Searches and Seizures**: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." (U.S. Const., 4th Amend.)

The Fourth Amendment was borne from the concern that government officials would arbitrarily and unreasonably rummage through the homes and belongings of its citizens; it acts as a shield to protect the privacy and security of individuals against the arbitrary invasion of governmental officials. When society deems a place or thing to be covered by a reasonable expectation of privacy, a warrant supported by probable cause is required to search or inspect that place or thing. No single rubric definitively resolves which expectations of privacy are entitled to protection under the Fourth Amendment, but a fundamental purpose in imposing limitations on government intrusions has long been to prevent too pervasive a state of police surveillance.

The government's ability to obtain a warrant to search a place or thing is generally limited to offenses that warrant such invasion in the first place. California law specifies the types of crimes that permit intrusion into a person's places or things including: when property is stolen or embezzled, among other specified offenses; when there is probable cause that a felony was committed and for a limited list of specified misdemeanors; and when there is a warrant to arrest a person. In the last five years, the Legislature has expanded the crimes that will allow the issuance of a warrant, and continues to suggest additions to the list.

Fourth Amendment jurisprudence has developed to permit a government entity to access information held by a third party, in some cases with a warrant and in some, without. The third-party doctrine is grounded in the idea that an individual has a reduced expectation of privacy when knowingly sharing information with another. For example, the United States Supreme Court held that a person does not have a reasonable expectation of privacy in bank records, which may be subpoenaed by law enforcement with reasonable suspicion that those records will reveal that a crime has been committed.[1] More recently, however, the court has said that for law enforcement to obtain location information from a third party through use of a cellphone likely requires a warrant, except in exigent circumstances.

As technology advances, the courts and lawmakers should be careful not to "embarrass the future" by making decisions that are in discord with the "progress of science."[2] This sentiment is at the core of the holdings in three recent United States Supreme Court cases,

---

[1] *United States v. Miller*, 425 U.S. 435 (1976).
[2] *Carpenter v. United States*, 585 U.S. _ (2018) (citing *Northwest Airlines, Inc. v. Minnesota*, 322 U. S. 292, 300 (1944), and *Olmstead v. U.S.*, 277 U. S. 438, 473-474 (1928)).

Jones,[3] *Riley*[4] and *Carpenter*[5] which establish warrant requirements for use of and access to electronic communications and devices to surveil a person.

In tandem with the evolving Supreme Court case law, California passed the CalECPA with SB 178 (Leno) Chapter 651 in 2015. SB 178 established in statute that law enforcement officials are required to obtain a warrant before "searching" a third party's electronic records for law enforcement purposes, either by actually searching a person's cellphone or electronic device, or by requesting that information from a third party which holds it.

Any California court issuing a warrant must decide whether to grant that warrant on a case by case basis. Under CalECPA, a law enforcement agency must have probable cause to search electronic records held by a third party, including tech companies that host untold terabytes of data about their users and subscribers. The law limits the reach of any warrant to information described with particularity, under specific time periods, identifying the "target individuals or accounts, the applications or services covered, and the types of information sought." The law also specifies that any information unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure without a court order.

CalECPA states that any warrant applied for shall comply with California and federal law, and that the normal procedures for a warrant apply including a typical warrant for records or things, or an arrest; a wiretap order; a tracking device search warrant; and a pen register or trace device; among others. When CalECPA was initially passed, it did not include reference to a tracking devices or pen registers. In 2016, the Legislature passed AB 1924 (Low) to authorize the use of a tracking device and pen register pursuant to CalECPA with a warrant.

3) **Existing Law Requires a Warrant to Track a Person's Movements**: In 2012, the United States Supreme Court held in *United States v. Jones* that the use of a self-contained GPS tracking device ("slap-on") on a motor vehicle to monitor the vehicle's movements constituted a "search." Thus a warrant is required to utilize such technology. That year, California passed AB 2055 (Fuentes) Chapter 818 to codify and expand the case, and require a warrant when a government entity utilizes such tracking device. Now, Pen. Code, §1534 sets forth specific procedures for obtaining a tracking device search warrant. Tracking devices may only be used to investigate felony violations, or misdemeanor violations of the Public Resources Code and the Fish and Game Code. A tracking device warrant is not authorized for other misdemeanor conduct for which a warrant for historical information is permitted, like to investigate a misdemeanor offense involving a motor vehicle.[6]

After CalECPA was passed by the Legislature in 2015, there was concern that the law nullified existing provisions of law permitting the use of pen registers and tracking devices. The next year, the Legislature passed AB 1924 (Low) Chapter 511 to incorporate existing

---

[3] *United States v. Jones*, 564 U.S. 400 (2012) (Holding that the attachment of a global-positioning-system tracking device to an individual's vehicle, and monitoring of the vehicle's movements on public streets, constituted a search or seizure within the meaning of the Fourth Amendment.)
[4] *Riley v. California*. 573 U.S. 373 (2014) (Holding that police may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.)
[5] *Carpenter v. United States*, 585 U.S. _ (2018) (Holding that the government's acquisition from wireless carriers of defendant's historical cell-site location information was a search under the Fourth Amendment.)
[6] Pen. Code, § 1524, subd. (a)(19).

laws permitting the use of pen registers and tracking devices into CalECPA. The result of amending CalECPA to include the tracking device search warrant procedures was to establish that any time a law enforcement agent seeks to obtain a person's real-time location data, that a warrant complying with Pen. Code, §1534 is required, whether the tracking occurs by utilizing a "slap-on" device or by compelling production of that information from a service provider through CalECPA, or by physically interacting with an electronic device, or by electronically communicating with an electronic device.

CalECPA sets forth rules when a government agency seeks to access a person's information from a third party, like Google, or when an official seeks to seize a person's cellphone and search it. The plain language of CalECPA encompasses activity that may arguably constitute certain types of hacking activity of an electronic device by specifying that the law's dictates apply when government engages in "physical interaction or electronic communication with the device." Pen. Code, § 1546.1, subd. (c).

Cellphones, vehicle computer systems, and other electronic devices are susceptible to being hacked, and also to receiving malware, a virus, or software which exploit a vulnerability in a device's operating system and provide the entity exploiting the vulnerability the ability to access, among other things, a person's location data.

This bill clarifies that the procedures for employing a tracking device, including heightened and specified warrant requirements, must be complied with if a law enforcement agency uses software by means of physical interaction or electronic communication with an electronic device, to track a person's movements.

4) **Concerns that this Bill Authorizes Law Enforcement to Hack a Person's Cellphone or Device**: Whether government officials are permitted to "exploit vulnerabilities in software and hardware products to gain remote access to computers"[7] or other electronic devices to "remotely search, monitor user activity on, or even interfere with the operation of those machines" is not squarely addressed by California law.

Pen. Code, § 502 prohibits hacking activity generally, including the right to be free "from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer system." There is no exception for law enforcement officials. In contrast, Pen. Code, § 632 which prohibits recording a private communication without all parties consent to record has a specified exemption for law enforcement to record for investigatory purposes. Thus, Pen. Code, § 502 does not appear to authorize law enforcement hacking activity.

Turning to the plain language of CalECPA, the law recognizes that a government entity may have the ability to access a person's electronic information "by means of physical interaction or electronic communication with" an electronic device, and also may compel a service provider to provide records, electronic information, and subscriber information, including things like emails, text messages, and historical location data.

---

[7] Riana Pfefferkorn, *Security Risks of Government Hacking* (Sept. 2018) Stanford Law School: The Center for Internet and Society, available at: https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf [last accessed Jan. 8, 2020].

The legislative history of SB 178 (Leno) does not state that a possible intent of CalECPA is to authorize the hacking of an electronic device. (See bill analyses for SB 178 from the Assembly and Senate Public Safety Committees and the Assembly Privacy and Consumer Protection Committee.) However the plain language of the statute states that a physical interaction or communication with an electronic device is permitted with a warrant. Arguably, this may encompass activity that is similar to hacking or the sending of malware or a virus to an electronic device.[8] CalECPA recognizes that the proper type of warrant is required to access information. For example, if a police department is coordinating with AT&T to track the real-time movements of a person through their cellphone with a search warrant, the specified tracking device search warrant procedures would apply in addition to any other provisions of CalECPA.

Whether a judge would authorize activity that constitutes the hacking of a person's cellphone or otherwise engage in conduct that violates Pen. Code, § 502, for which law enforcement officials have no exception, is another question. And if a judge did so authorize such activity, would reviewing courts deem that to be a reasonable search under Fourth Amendment scrutiny?

5) **Argument in Support**: According to the *California Attorneys for Criminal Justice*, "This bill closes a loophole in the law that could allow for the software-based tracking of individuals by law enforcement without a warrant. Search warrants protect the public from unreasonable searches and seizures, a constitutional right that CACJ supports and believes should be expanded in the face of new technology."

6) **Argument in Opposition**: According to the *Electronic Frontier Foundation*, "A.B. 904 would amend the California Electronic Communications Privacy Act ('CalECPA'), a watershed statute that established bright-line rules for California government entities seeking to obtain, retain, and use digital information. CalECPA was drafted with the specific intention of reinforcing the privacy rights set forth at Article 1, Section 1, of the California Constitution—a response to the 'modern threat to personal privacy' posed by increased surveillance and then-emerging data collection technology. *White v. Davis*, 13 Cal.3d 757, 774 (1975).

"We are extremely concerned that A.B. 904 would create and authorize, for any California government entity, an entirely new 'procedure for accessing or installing software into an electronic device.' CalECPA already allows access to information stored on a device. A.B. 904's new procedure would seem to expressly authorize the government to 'access' applications like cameras, microphones, or electronic mail on a person's smartphone, tablet, or computer. At the very least, this could allow the government to use a person's device as a hidden camera or microphone, or as a launching pad to covertly access email or other documents or communications that are not stored on the device.

---

[8]The only reported hacking activities have been accomplished by federal authorities in a highly controversial public case where a private company was hired to hack an iPhone of a California resident. See Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, Washington Post (April 12, 2016), available at: https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html [last accessed Jan. 8, 2020].

"Even worse, the bill expressly authorizes 'installing software,' which appears to authorize government 'hacking' into people's devices in order to install malware. This would constitute a broad new surveillance authority that presents serious risks to computer security. At this point, it is an all-too-familiar story when even elite intelligence and law enforcement agencies are unable to maintain control of their hacking tools and they are exploited by outside actors."

7) **Prior Legislation**:

a) SB 178 (Leno), Chapter 651, Statutes of 2015, prohibits a government entity from compelling the production of, or access to, electronic-communication information or electronic-device information without a search warrant or wiretap order, except under specified emergency situations.

b) AB 929 (Chau), Chapter 204, Statutes of 2015, authorizes state and local law enforcement to use pen register and trap and trace devices under state law, and permits the issuance of emergency pen registers and trap and trace devices.

c) AB 1924 (Low), Chapter 511, Statutes of 2016, requires an order or extension order authorizing or approving the installation and use of a pen register or a trap and trace device direct that the order be sealed until the order, including any extensions, expires, and would require that the order or extension direct that the person owning or leasing the line to which the pen register or trap and trace device is attached not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber or to any other person.

d) AB 1638 (Olbernolte), Chapter 196, Statutes of 2019, expands authorization for the issuance of a search warrant to obtain information from a motor vehicle's software that tends to show the commission of a felony or misdemeanor offense involving a motor vehicle, resulting in death or serious bodily injury.

REGISTERED SUPPORT / OPPOSITION:

Support

California Attorneys for Criminal Justice

Oppose

American Civil Liberties Union of California
Electronic Frontier Foundation

Analysis Prepared by: Nikki Moore / PUB. S. / (916) 319-3744