Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1638 (Obernolte) – As Amended April 11, 2019

SUBJECT: Search warrants: vehicle recording devices

SUMMARY: This bill would authorize the issuance of a search warrant on the grounds that the property or things to be seized are data, from a recording device installed by the manufacturer of a motor vehicle, that constitutes evidence that tends to show the commission of a public offense involving a motor vehicle resulting in death or "serious bodily injury" as defined under the Penal Code. This bill would prohibit the data accessed by a warrant from exceeding the scope of the data that is directly related to the public offense for which the warrant is issued. This bill would define "recording device" to have the same meaning as provided to that term under the Vehicle Code, as specified, and would limit the scope of data accessible by a warrant issued pursuant to this bill to the information described in the Vehicle Code. This bill would make other non-substantive changes.

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, 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 an the persons or things to be seized." (U.S. Const., Fourth Amend; *see also* Cal. Const. art. 1, Sec. 13.)

2) Governs search warrants, including the grounds upon which a search warrant may be issued. (Pen. Code Sec. 1523 et seq.)

3) Defines a "search warrant" as a written order 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 Sec. 1523.)

4) Authorizes a search warrant to be issued upon any of the following grounds, among others:

   - 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.

   - 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.

   - 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.

- When the information to be received from the use of a tracking device, as defined, constitutes evidence that tends to show: (a) either a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code has been committed or is being committed; (b) that a particular person has committed or is committing a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code, or will assist in locating an individual who has committed or is committing a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code.

- When the property or things to be seized consists of evidence that tends to show that specified violations of privacy (by way of looking through a hole or opening by means of instrumentalities such as periscopes, telescopes, binoculars, and more; or by way of using a concealed camcorder, motion picture camera, or photographic camera of any type to secretly tape, film, photograph or record by electronic means another identifiable person, as specified) under the Penal Code, has occurred or is occurring. (Pen. Code Sec. 1524.)

5) Provides that a search warrant cannot be issued but upon probable cause, supported by affidavit, naming or describing the person to be searched or searched for, and particularly describing the property, thing, or things and the place to be searched. (Pen. Code Sec. 1525.)

6) 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 from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. CalECPA also generally specifies the only 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, consent of the owner of the device, or emergency situations, as specified. (Pen. Code Sec. 1546 et seq.)

7) Defines "serious bodily injury" to mean a serious impairment of physical condition, including, but not limited to, the following: loss of consciousness; concussion; bone fracture; protracted loss or impairment of function of any bodily member or organ; a wound requiring extensive suturing; and serious disfigurement. (Pen. Code Sec. 243(f)(4).)

8) Requires owner's manuals to disclose to the owner when a car is installed with event data recorders (EDRs) or sensing and diagnostic modules and defines "recording device" for these purposes to mean a device that is installed by the manufacturer of the vehicle and does one or more of the following, for the purpose of retrieving data after an accident:

- records how fast and in which direction the motor vehicle is traveling;

- records a history of where the motor vehicle travels;

- records steering performance;

- records brake performance, including, but not limited to, whether brakes were applied before an accident; and,

- records the driver's seatbelt status; and/or,

- has the ability to transmit information concerning an accident in which the motor vehicle has been involved to a central communications system when an accident occurs. (Veh. Code Sec. 9951(b).)

9) Specifies that such data from a recording device, identified above, can only be accessed under certain circumstances, including where the registered owner of the motor vehicle consents to the retrieval of the information, or in response to an order of a court having jurisdiction to issue the order. (Veh. Code Sec. 9951(c).)

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: This bill seeks provide law enforcement the ability to obtain a warrant to access certain vehicle data after automobile accidents resulting in serious bodily injury or death. This is an author-sponsored bill.

2) **Author's statement**: According to the author, "Event Data Recorders (EDR) have become increasingly prevalent in motor vehicles in recent years. However, EDR data cannot be legally obtained by law enforcement without a court order or the consent of the vehicle's registered owner ([Vehicle Code Sec.] 9951). Unfortunately, there are many solo vehicle accidents where the driver is deceased or has been critically injured and, therefore, is unable to give consent. In those cases, there is no statutory "court order" available to law enforcement, making it impossible for the officer to use the EDR data to help with the accident investigation. The statute authorizing courts to issue search warrants (Penal Code 1524) applies to EDR data only for felonies. While [Vehicle Code Sec.] 9951 also allows EDR data to be downloaded with consent of the vehicle's registered owner, it is not always possible in fatality accidents. Specifically, this bill has been narrowly drafted to give law enforcement the statutory authority to obtain a search warrant in order to get information from the vehicle's EDR that is related to the commission of a public offense involving a motor vehicle accident that results in a person's death or serious bodily injury."

3) **Authorizing warrants to be issued for EDR data**: Generally speaking, the Fourth Amendment to the United States Constitution (and art. I, Sec. 13 of the California Constitution) generally provides the right of people to be secure from unreasonable searches and seizures of their person or property, and a requirement that search warrants be specific and based on probable cause (with some exceptions). A search occurs when the government impinges on an individual's "reasonable expectation of privacy." The rule is enforced in part by excluding evidence from trial that was obtained in violation of these requirements.

   In 2015, out of concern that the law had not been adequately updated to protect all forms of electronic communications and their metadata, AB 178 (Leno, Ch. Stats. 2015) was adopted to codify and strengthen privacy protections under the California Constitution in a number of ways. For example, it required a demonstration of probable cause to obtain electronic

communications information from a third party service provider, responding to a high percentage of legally inadequate requests from law enforcement. It also applied the probable cause requirement to past electronic communications, regardless of their age, which was an improvement over federal law. SB 178 also guaranteed that geolocation information is protected by the same standard, which codifies protections established in case law, and also protects some forms of "metadata." The author's end goal with SB 178, according to the Assembly Floor analysis, was to create a "clear, uniform warrant rule for California law enforcement access to electronic information."

As noted in this Committee's analysis of SB 178 at the time that bill was heard, generally CalECPA's requirement for a search warrant or probable cause order for electronic communications information is protective of personal privacy and in keeping with the California Constitution's explicit protection of an individual's right of privacy, but does provide for the traditional exceptions in limited circumstances (*i.e.*, volunteered information, lost devices, emergency situations, and so forth). Moreover, CalECPA's requirements explicitly limit the searches to necessary information, ensure judicial oversight of information obtained without a warrant or order, and mandate deletion of unneeded information. Specifically, and of relevance to this bill, it 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.

This bill seeks to allow law enforcement to obtain a warrant on the grounds that data from a recording device installed by a vehicle manufacturer constitutes evidence that tends to show the commission of a public offense involving a motor vehicle that resulted in death or serious bodily injury. The bill defines "recording device" to have the same meaning as under a specific provision of the Vehicle Code (Veh. Code Sec. 9951) which generally requires owner's manuals to disclose to the owner when a car is installed with event data recorders (EDRs) or sensing and diagnostic modules. Under that Vehicle Code definition, "recording device" means a device installed by a vehicle manufacturer that records or has the ability to transmit certain data for purposes of retrieving data after an accident. This includes recording information regarding, for example: (1) how fast and in which direction the motor vehicle is traveling; (2) a history of where the motor vehicle travels; (3) records steering performance; and (4) brake performance, including, but not limited to, whether brakes were applied before an accident, and the driver's seatbelt status.

As amended in the Assembly Public Safety Committee, the bill limits the information made accessible from an EDR under a warrant to the information listed in that Vehicle Code definition. The recent amendments to the bill also limit the scope of information that may be obtained from the EDR to "data that is directly related to the public offense for which the warrant is issued." According to the Assembly Public Safety Committee analysis, in practice, this means that EDR information related to a deadly accident may be released to the extent that the data sought is relevant to the accident, but a warrant would not be issued for wide-ranging access to the driver's data for long periods of time, for example, over the week prior to the accident.

4) **CalECPA addresses need for a warrant to obtain electronic communications information and electronic device information**: Of particular relevance to this bill, CalECPA not only protects against the unreasonable search and seizure of "electronic communications information," but also "electronic device information." Electronic device

information means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device. Relatedly, electronic device generally means a device that stores, generates, or transmits information in electronic form.

As discussed in Comment 3, above, to protect the privacy interests that is held in electronic information, CalECPA expressly excludes government entities from compelling the production of or access to electronic communication information from a service provider, absent. The exceptions to this are where the government entity obtains: (1) a warrant that has been issued pursuant to the Penal Code as specified, subject to additional heightened requirements for warrants pursuant to CalECPA; (2) a wiretap order; (4) an order for electronic reader records; (4) a subpoena (provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense); or, (5) an order for a pen register or trap and trace device, or both. Similarly, CalECPA also prohibits government entities from compelling the production of or accessing electronic device information from any person or entity other than the authorized possessor of that device in the absence of a warrant or such orders enumerated above.

Accordingly, to the extent that this bill seeks to authorize law enforcement to access a car's black box data, it appears somewhat redundant of CalECPA, which requires that law enforcement either obtain a warrant in criminal investigations or prosecutions or subpoena in non-criminal investigations or prosecutions in order to compel or otherwise access the data off an electronic device from any person or entity (such as the manufacturer) other than the vehicle owner. Indeed, even if this bill expressly authorizes a warrant specifically be issued for this type of data, it does not relieve law enforcement of their obligation to meet the CalECPA standards for a warrant. Specifically, under CalECPA, a warrant for electronic information must comply with the following requirement:

- The warrant must describe with particularity the information to be seized by specifying, as appropriate, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought, except as specified.

- The warrant must require that any information sought through the execution of the warrant that is unrelated to the objective of the warrant are sealed and not subject to further review, use, or disclosure except pursuant to a court order requiring probable cause or to comply with discover, as specified.

- The warrant must comply with all other provisions of California or federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. (*See* Pen. Code Sec. 1546.1(d).)

Thus, the key difference between existing law and this bill appears to relate to the cases in which a warrant could be authorized under this bill as opposed to CalECPA. This bill would now allow for warrants to be issued in cases where law enforcement seeks information off of a car's black box, not just in cases of felonies, but misdemeanors and other public offenses.

Currently, CalECPA recognizes the ability of law enforcement to seek a warrant for electronic device information pursuant to the Penal Code chapter governing the issuance of warrants ("search warrants chapter"), subject to the CalECPA warrant requirements above.

The search warrants chapter, in turn, only expressly authorizes the issuance of a warrant in connection with misdemeanor violations in two areas. First, it permits a 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 under the Fish and Game Code or Public Resources Code, has been committed or is being committed; tends to show that a particular person has committed or is committing a felony or such misdemeanor violations; or will assist in locating an individual who has committed or is committing a felony or such misdemeanor violations. (Pen. Code Sec. 1524(a)(12).) Second, it permits a warrant to be issued when a provider of electronic communication service or remote computing service has records or evidence, as specified, 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 public offense. (Pen. Code Sec. 1524(a)(7).) Similarly, the search warrants chapter authorizes warrants to be issued in two instances involving "public offenses"- one of which refers specifically to "misdemeanor public offense," and the other which references "public offense" more generally. In that case, a warrant can be issued on the grounds that 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. (Pen. Code Sec. 1524(a)(3).)

Arguably, given the sensitivity of and significant privacy implications involved with electronic information, a question arises as to whether law enforcement should be able to obtain that information in cases that do not involve a felony, particularly when given that subpoenas may be granted in non-criminal cases involving accidents. (*See* Comment 5 for more.)

5) **Unclear that a public offense is sufficient to warrant such an invasion of privacy involving electronic information**: Despite recent amendments in the prior policy committee to narrow the bill, it remains unclear as to what constitutes a "public offense" sufficient for a warrant under this bill, other than it must involve death or serious bodily injury. Presumably, it includes misdemeanors and not just felonies, but it could also include infractions that involved death or serious bodily injury. This has potentially critical privacy implications for individuals to whom this car black box data pertains.

In its opposition to the introduced version of this bill, the American Civil Liberties Union (ACLU) highlighted this issue, raising concerns about the privacy concerns implicated when electronic information is sought by government entities. As stated in by ACLU:

> In accordance with fundamental constitutional principles, California's search warrant statute operates to curb governmental overreach, and to protect the privacy and personal security of those within our state. In order to balance these privacy concerns with the legitimate public safety concerns, our existing law is designed to permit the issuance of a search warrant only under narrow circumstances, for the most serious offenses, and only when governmental needs have been determined to outweigh those of private individuals.
>
> Privacy concerns are heightened when it is electronic information that is sought. Because the electronic information routinely collected by our phones, devices and cars is so extensive and contains such a wealth of highly private information, California's Electronic Communications Privacy Act puts in place additional protections when the

government seeks access to this type of information. The kinds of information available from a motor vehicle recording device provide a good example of why additional protection is needed for electronic information: the data may include records of where the vehicle has been and the speeds at which it has been driven as well as steering and braking information and other information.

AB 1638 would contravene the carefully crafted balance of our search warrant statute by allowing the issuance of a warrant for the extensive data available from a motor vehicle recording device when the crime under investigation is a misdemeanor. The bill would allow the privacy rights of the individual to be violated when the governmental interest, in investigating a less-serious offense, does not warrant that violation.

The author responds that this bill "is very narrowly crafted to only allow law enforcement to access this information from the vehicle's EDR that is related to the commission of a public offense involving a motor vehicle accident that results in a person's death or serious bodily injury. In these circumstances the law enforcement officer would need a judge to issue a search warrant and then the officer would only be able to access information that is related to the accident in order to aid with the accident investigation. No personal information from the driver would be able to be obtained under this bill."

6) **Related legislation**: AB 904 (Chau) would prohibit a court from granting a search warrant to conduct real-time surveillance of a person through an electronic device possessed by that person, except in extraordinary circumstances. AB 904 is currently in the Assembly Public Safety Committee.

7) **Prior legislation**: AB 1924 (Low, Ch. 511, Stats. 2016) provided an exemption from CalECPA for pen registers and trap and trace devices to permit authorization for the devices to be used for 60 days.

SB 178 (Leno, Ch. 651, Stats. 2015) enacted CalECPA, which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.

AB 929 (Chau, Ch. 204, Stats. 2015) authorized state and local law enforcement to use pen register and trap and trace devices under state law, and permitted the issuance of emergency pen registers and trap and trace devices. The authorization for the use of a trap and trace device or a pen register was for 60 days from the date of issuance, with extensions of up to 60 days. However, the governor signed AB 929 prior to signing the ECPA and as a result the authorization was chaptered out by the ECPA's 10-day authorizations.

SB 467 (Leno, 2013) would have required a search warrant when a governmental agency is seeking the contents of a wire or electronic communication that is stored, held or maintained by a provider. SB 467 was vetoed by Governor Brown, who wrote: "The bill, however, imposes new notice requirements that go beyond those required by federal law and could impede ongoing criminal investigations. I do not think that is wise."

SB 1434 (Leno, 2012) would have required a government entity to get a search warrant in order to obtain the location information of an electronic device. SB 1434 was vetoed by Governor Brown, who wrote: "It may be that legislative action is needed to keep the law

current in our rapidly evolving electronic age. But I am not convinced that this bill strikes the right balance between the operational needs of law enforcement and individual expectations of privacy."

SB 914 (Leno, 2011) would have required a search warrant to search the contents of a portable electronic device that is found during a search incident to an arrest. SB 914 was vetoed by Governor Brown, who wrote: "This measure would overturn a California Supreme Court decision that held that police officers can lawfully search the cell phones of people who they arrest. The courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections."

8) **Double-referral**: This bill was double-referred to the Assembly Public Safety Committee where it was heard on April 9, 2019, and passed on a 5-0 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

California District Attorneys Association

Opposition

American Civil Liberties Union

Analysis Prepared by: Ronak Daylami / P. & C.P. / (916) 319-2200