Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 904 (Chau) – As Amended January 6, 2020

SUBJECT: Search warrants: tracking devices

SUMMARY: This bill would specify that a "tracking device" includes any software that permits the tracking of the movement of a person or object for purposes of existing law, which allows a search warrant to be issued when the information to be received from the use of a tracking device constitutes evidence that: (1) tends to show that either a felony, or certain misdemeanors, has been committed or is being committed; (2) tends to show that a particular person has committed or is committing a felony or certain misdemeanors; or, (3) will assist in locating an individual who has committed or is committing a felony or certain misdemeanors.

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 and the persons or things to be seized." (U.S. Const., 4th Amend.)

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

3) Provides that a tracking device search warrant issued pursuant to the above provision must identify the person or property to be tracked and must specify a reasonable length of time, not to exceed 30 days from the date the warrant is issued, that the device may be used. Authorizes courts to grant one or more extensions for good cause, as specified. The search warrant must 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, as specified, and requires the execution of the warrant to be completed no later than 10 days immediately after the date of issuance. As used in this section, "tracking device" means any electronic or mechanical device that permits the tracking of the movement of a person or object. (Pen. Code Sec. 1534(b).)

4) 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 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.)

5) Defines various terms for purposes of CalECPA, including the following:

- "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

- "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. "Electronic communication information" does not include subscriber information, as defined.

- "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

- "Electronic device" means a device that stores, generates, or transmits information in electronic form. An electronic device does not include the magnetic strip on a driver's license or an identification card issued by this state or a driver's license or equivalent identification card issued by another state.

- "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.

- "Electronic information" means electronic communication information or electronic device information. (Pen. Code Sec. 1546(c)-(h).)

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

COMMENTS:

1) **Purpose of this bill**: In addition to the existing prohibition on the use of tracking devices unless certain conditions are met, this bill seeks to ensure that government entities cannot use tracking *software* that permits the tracking of the movement of a person or object unless certain conditions are met. This bill is author-sponsored.

2) **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 closes this loophole by specifically prohibiting software-based tracking of individuals by law enforcement without a warrant. (Footnote citations omitted.)

3) **The Fourth Amendment and innovations in surveillance tools**: The Fourth Amendment states, "[t]he 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.) Stated another way, it prohibits Government from intruding on a person's right of privacy in their person, home, papers, and effects, unless the Government first obtains a warrant issued upon probable cause supported by sworn testimony and stating the place to be searched and the persons or things to be taken possession of. A warrant, thus, demonstrates that the search and seizure is "reasonable" as required by the Fourth Amendment's prohibition against "unreasonable searches and seizures."

While much of the early Fourth Amendment search doctrine focused on whether the Government "obtains information by physically intruding on a constitutionally protected area," more recent judicial precedent recognizes that "property rights are not the sole measure of Fourth Amendment protections." (*See Carpenter v. United States* (2018) 138 S.Ct. 2206, 2213, citing (*U.S. v. Jones* (2012) 565 U.S. 400 and *Soldal v. Cook County* (1992) 506 U.S. 56.) In the seminal case of *Katz v. United States* 389 U.S. 347, 351, the U.S.

Supreme Court established that "the Fourth Amendment protects people, not places." In doing so, the Court "expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Supreme Court] has held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." (*Carpenter,* 128 S.Ct. at 2213.)

As described most recently by the Supreme Court in the case of *Carpenter* (discussed further in Comment 4, below) Fourth Amendment jurisprudence reflects certain basic guideposts in the Court's analysis of what is an unreasonable search and seizure, as informed by a historical understanding of that concept when the Fourth Amendment was first adopted. First, the amendment seeks "to secure 'the privacies of life' against 'arbitrary power.'" Second, and related, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (*Id*. at 2214, internal citations omitted.) These guideposts apply when applying the Fourth Amendment to innovations in surveillance tools. "As technology has enhanced the Government's capacity to encroach on areas normally guarded from inquisitive eyes, [the] Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (*Id*., internal citations omitted.)

By way of examples, the Court has applied the Fourth Amendment as follows to various emerging technologies:

- In *Smith v. Maryland* (1979) 442 U.S. 735, the court ruled that the Government's use of a pen register (a device that records the outgoing phone numbers dialed on a landline phone) was not a search. Noting the pen register's limited capabilities, the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." As such, when Smith placed a call, he was said to have "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." (*Id*. at 742, 744).

- In *United States v. Knotts* (1983) 460 U.S. 276, 281, 282, the Court considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic as officers (with intermittent aerial assistance) followed the vehicle relying on the beeper's signal to keep the vehicle in view. There, the Court concluded that the "augment[ed]" visual surveillance did not constitute a search because a "person traveling in an automobile of public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."

- In *Kyllo v. United States* (2001) 533 U.S. 27, the Court determined that the Government could not capitalize on new sense-enhancing technology (thermal imaging) to explore what was happening within the home, absent a warrant.

- In *United States v. Jones* (2012) 565 U.S. 400, the Court was faced with a case wherein FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for almost 30 days. Based on the Government's

> physical trespass of the vehicle, five justices agreed that related privacy concerns would be raised by, for example, "surreptitiously activating a stolen vehicle detection system" in Jones's car to track him, or conducting GPS tracking of his cell phone. Since GPS monitoring of a vehicle tracks every movement that a person makes in the vehicle, the concurring Justices in *Jones* concluded that "'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large." (*Carpenter*, 138 S.Ct. at 2215, internal citations omitted.)

- In *Riley v. California* (2014) 573 U.S. 373, the Court recognized the immense storage capacity of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone.

Like the holdings in many of these cases, this bill recognizes that laws require periodic updating to ensure that rights are protected in as new technologies become available. The California Attorneys for Criminal Justice (CACJ), a statewide association of criminal defense attorneys in private practice and working in public defender offices, writes in support of this bill:

> AB 904 would clarify that the prohibition on accessing an electronic device without a search warrant includes any software that permits the tracking of a person or object. 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.

4) ***Carpenter v. United States***: Most recently, in 2017, the U.S. Supreme Court was faced with a question of how the Fourth Amendment applies "to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals" in the case of *Carpenter v. United States* (2018) 138 S. Ct. 2206. Using the guidelines of the cases described in Comment 3, above, the Court analogized that the "tracking partakes of many of the qualities of the GPS monitoring [the Court] considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." (*Id*. at 2216.)

   In *Carpenter*, the Court examined the issue under two lines of Fourth Amendment cases. First, it outlined a line of Fourth Amendment cases (including *Knotts* and *Jones*, discussed in Comment 3, above) that addressed a person's expectation of privacy in his or her physical location and movements. Second, it reviewed another line of decisions (including *Miller* and *Smith*) wherein the Court has drawn a line between what a person keeps to himself and what he shares with others, which has come to be known as the third party doctrine[1]. The

---

[1] A doctrine stating that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (*Smith v. Maryland* (1979) 442 U.S. 735, 743-744), "even if the information is revealed on the assumption that it will only be used for a limited purpose." (*United States v. Miller* (1976) 425 U.S. 435, 443). In those cases, the Government is typically free to obtain such information from the recipient without triggering the Fourth Amendment requirement for a warrant.

Carpenter Court ultimately held that the government's acquisition of Carpenter's cell-site records was a search for purposes of the Fourth Amendment and required a warrant.

5) **The California Electronic Communications Protection Act**: As noted by the author above, while instructive on how the Supreme Court may apply existing protections to emerging technologies in the near future, *Carpenter* had limited applicability in this state, as California has protected this information for a number of years. California also provides extensive protection to Californians by way of the California Electronic Communications Protection Act (CalECPA), but there does appear to be some question of whether the protection is comprehensive.

Enacted in 2015 by SB 178 (Leno, Ch. 651, Stats. 2015), CalECPA generally prohibits government entities from either: (1) compelling the production of or access to "electronic communication information" from a service provider; or, (2) compelling the production of or access to "electronic device information" from any person or entity other than the authorized possessor of the device. CalECPA authorizes such actions only in limited circumstances. Chief among these authorized circumstances is where the government entity properly obtains a warrant pursuant to existing state law generally governing the issuance of warrants and additional CalECPA warrant requirements. (*See* Pen. Code Sec. 1946.1(a)(1)-(2), (b) and (d).)

Further, CalECPA specifically prohibits government entities from accessing *electronic device information* by any means of physical interaction or *electronic communication* with the *electronic device*, outside of limited circumstances, which include where a warrant has been obtained consistent with those same laws. "Electronic device information" means any information stored on or generated through the operation of an *electronic device*. "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system. "Electronic device" includes any information stored on or generated through the operation of an electronic device.

Notably, this provision does not appear to limit the ability of government entities from accessing "electronic communication information" by means of physical interaction or electronic communication with the electronic device. "Electronic communication information" generally means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or *location of the sender or recipients at any point during the communication*, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address.

Stated another way, because CalECPA only: (1) limits the ability of a government entity from obtaining "electronic communication information" from a service provider; (2) limits the ability of a government entity to obtain "electronic device information" from any person or entity other than the authorized possessor of the device; and (3) only limits the ability of a government entity to access "electronic device information" by means of physical interaction or electronic communication with the electronic device, it appears possible for law

enforcement to obtain "electronic communication information" by means of physical interaction or electronic communication with an electronic device.

Additionally, CalECPA appears entirely silent on the issue of the ability of government to compel access to or surreptitiously access by physical interaction with *software* on a device. Because of this ambiguity, AB 904 seeks to ensure that the law is absolutely clear, by prohibiting the tracking of individuals through software without a warrant.

Two civil liberties groups, the American Civil Liberties Union of California (ACLU) and the Electronic Frontier Foundation, interpret the bill differently and are concerned that the bill would instead *authorize* software-based tracking by law enforcement. Writing in opposition, the ACLU argues:

> Allowing law enforcement use of tracking software that can be installed on a person's telephone or other electronic equipment without the person's knowledge poses a host of dangers to the privacy rights of Californians. Such software might also allow law enforcement access to more than just location information. For example, if spyware were installed on an individual's phone, that software could not only allow law enforcement to tack that person's location but also to access the phone's camera, listen in on conversations, see the person's activity on the phone, and collect other sensitive information.
>
> While we appreciate [the author's] intent to ensure that any law enforcement use of tracking software be carefully restricted under the law, in its current form, AB 904 unfortunately appears instead to authorize the use of software for tracking purposes when it is unclear whether law enforcement has the authority to install such software for that purpose under existing law. At a minimum, we believe that the bill should be amended to clarify that it does not authorize law enforcement installation or use of any software that was not previously authorized under law.

In response to these concerns, the author offers the following amendment which would clarify that the bill does not authorize the use of tracking software, but instead safeguards against it.

> Author's amendment:
>
> On Page 3, after line 18 insert ***"****(7) As used in this section, the reference to "software" is not intended to expand the authority of a government entity to use software for surveillance purposes under this chapter or any other law."* and renumber accordingly.

This amendment is consistent with the intent of the bill which seeks to strengthen and update California law by ensuring that: (1) government entities cannot obtain "electronic communication information" by way of physical interaction or electronic communication with an electronic device; and (2) government entities cannot obtain access to software on an individual's electronic device by either physical interaction or compelling a third party to provide that access, surreptitiously, unless the government entity follows California law governing wiretaps.

6) **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 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."

REGISTERED SUPPORT / OPPOSITION:

Support

California Attorneys for Criminal Justice

Opposition

American Civil Liberties Union of California
Electronic Frontier Foundation

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200