Date of Hearing: April 22, 2025

Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 358 (Alvarez) – As Amended April 10, 2025

SUBJECT: Criminal procedure: privacy

SYNOPSIS

In the early 2010s, two landmark Supreme Court cases helped define the scope of Fourth Amendment protections in the digital age. In United States v. Jones (2010), the Court ruled that the government must obtain a warrant to track an individual using GPS. In Riley v. California (2014), the Court held that law enforcement must obtain a warrant to access digital information on a cell phone belonging to an arrested person. In both cases, the Court emphasized the importance of protecting individual privacy under the Fourth Amendment in the context of modern technology.

To codify these principles, the California Legislature enacted the California Electronic Communications Privacy Act (CalECPA) (SB 127 (Leno; Stats. 2015, Chap. 651). CalECPA prohibits the government from accessing electronic communication records from individuals, service providers, or through physical or digital access to a device, without a warrant. It includes exceptions in cases of imminent danger or with the consent of the device's owner.

This new bill, sponsored by the San Diego County District Attorney's Office, would add an exception to CalECPA. It would allow law enforcement to conduct a warrantless search of a surveillance or tracking device found on someone's property if the person who discovered it reasonably believes it was used to monitor them without consent. The bill narrowly defines such devices to include hidden cameras, geotags, and audio recorders—excluding commonly used devices like phones and laptops. It was introduced in response to growing concerns about the misuse of surveillance technology to stalk or harass individuals.

The bill is supported by the California District Attorneys Association, California State Sheriffs' Association, Crime Victims Alliance, and other law enforcement organizations. It is opposed by the Electronic Frontier Foundation, the San Francisco Public Defender's Office, Universidad Popular, and other civil rights advocacy groups.

This bill passed the Assembly Public Safety Committee on a 6-0-3 vote.

THIS BILL:

1) Allows a government entity to access electronic device information by means of physical interaction or electronic communication with the device with the specific consent from an individual who locates a tracking or surveillance device within their residence, automobile, or personal property, and the device is reasonably believed to have been used for the purpose of recording or tracking the individual without their permission.

2) Defines a "tracking or surveillance device" to mean an electronic device the sole purpose of which is to record audio or visual information or to permit the tracking of a person.

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., Amend. IV.)

2) Provides that all people have an inalienable right to privacy. (Cal. Const., art. I, § 1.)

3) Provides that the right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized. (Cal. Const., art. I, § 13.)

4) 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.)

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, § 1525.)

6) States, except as authorized by statute, a government entity may not do any of the following:

    a) Compel the production of or access to electronic communication information from a service provider.

    b) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.

    c) Access electronic device information by means of physical interaction or electronic communication with the electronic device, however this section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity. (Pen. Code, § 1546.1(a)(1-3).)

7) Authorizes a government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

    a) Pursuant to a warrant;

    b) Pursuant to a wiretap order;

c) Pursuant to an order for electronic reader records;

d) Pursuant to a subpoena, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited; or

e) Pursuant to an order for a pen register or trap and trace device, as specified. (Pen. Code, § 1546.1(b)(1-5).)

8) Allows a government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

a) Pursuant to a warrant, as specified.

b) Pursuant to a wiretap order.

c) Pursuant to a tracking device search warrant.

d) With the specific consent of the authorized possessor of the device.

e) With the specific intent of the owner of the device, only when the device has been reported lost or stolen.

f) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

g) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

h) Except where prohibited by state or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility or a secure area of a local detention facility where inmates have access, the device is not in the possession of an individual, and the device is not known or believed to be the possession of an authorized visitor.

i) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is serving a term of parole under the supervision of the Department of Corrections and Rehabilitation or a term of post-release community supervision under the supervision of county probation.

j) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release.

k) If the government entity accesses information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device. (Pen. Code, § 1546.1(c)(1-11).)

9) States any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or existing statute. (Pen. Code, § 1546.4(a).)

COMMENTS:

1) **Author's statement**. According to the author:

The California Electronic Communication Privacy Act requires, with limited exceptions, a warrant in order to access electronic devices and/or communication. Exceptions are limited by Penal Code section 1546.1(c)(3)—(c)(11) and includes specific consent from the 'authorized possessor' (Pen. Code §(c)(3)). An 'authorized possessor' 'means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.' (Pen. Code § 1546(b).) In limited circumstances, a device and/or electronic communication information can be accessed if it's reasonably believed that the device has been abandoned, lost, or stolen, or if there is a belief that accessing the device will prevent death or serious bodily injury.

Current law pertaining to law enforcement's ability to access devices and/or electronic information without a warrant is unnecessarily narrow, frustrating the ability for law enforcement to protect the rights of victims. AB 358 seeks to rectify this by adding two additional exemptions to the need to acquire a warrant to access an electronic device. The first being when the device is believed in good faith to belong to a deceased individual, the second, when the device is found by a victim and was being used to record and/or track the victim without their consent.

Every Californian deserves justice, dignity, and protection under the law. AB 358 addresses this by amending the California Electronic Privacy Communication's Act in two ways. First, AB 358 allows that families who have lost loved ones to tragedy to be contacted and get the answers they deserve. Second, the bill protects survivors of domestic violence and stalking from being re-victimized through abusive use of technology tools.

One example is the fentanyl crisis that has devastated communities across our state, leaving parents, siblings, and children searching for closure after an unimaginable loss. Right now, outdated and uncertain legal barriers prevent law enforcement from accessing a deceased victim's device in a timely manner, delaying critical investigations that could save lives and prevent further harm. These delays mean that families are left without answers, and dangerous drugs continue circulating in our communities. AB 358 ensures that when tragedy strikes, we act with urgency and compassion by giving law enforcement and public administrators' access to electronic devices to contact next of kin or to investigate a death.

Similarly, no one should have to live in fear of being watched, tracked, or controlled by an abuser. Technology has given bad actors new ways to invade people's most private spaces, yet our laws have not kept up. Even when survivors discover hidden tracking or

recording devices, law enforcement cannot access them without a warrant. This delay gives perpetrators the opportunity to remotely erase evidence, making it nearly impossible to hold them accountable. AB 358 gives victims the ability to seek immediate protection by allowing law enforcement to investigate these devices when found in a private space.

AB 358 is not about weakening privacy protections—it is about balancing them with the real and urgent needs of victims. It is about giving families peace, keeping our communities safe, and ensuring that survivors are not left defenseless against technological exploitation.

2) ***Court Rulings and Cal ECPA.*** Before the 2010s, there was significant uncertainty surrounding the privacy rights and legal standards for accessing electronic devices. During this time, cell phones rapidly evolved from basic communication tools into powerful pocket-sized computers containing vast amounts of personal information. As a result, law enforcement increasingly sought access to these devices, raising important questions about what level of authorization was required to protect individuals' privacy. This legal ambiguity culminated in two landmark Supreme Court decisions and ultimately led to the passage of the California Electronic Communications Privacy Act (CalECPA).

The first case was *United States v. Jones* (132 S.Ct. 945 (2012)), the Court ruled that the physical attachment of a global positioning system (GPS) device to a car in order to monitor its movements over the course of a month as part of a drug trafficking investigation required a search warrant under the Fourth Amendment, although the reasoning differed between the Justices. This left open the question of whether government's collection of geolocation data requires a warrant when there is no physical invasion, such as getting GPS information from a mobile phone company. The Court even highlighted this uncertainty, writing, "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." Instead, Justice Alito appears to invite action by Congress and the states, saying "a legislative body is well suited to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."

The second case, *Riley v. United States* (134 S.Ct. 2473 (2014), was a landmark case that held that the Fourth Amendment requires a warrant prior to searching digital information on a cellphone seized during an arrest. The Court found that searching an individual's purse for evidence or a weapon during an arrest is qualitatively different than searching someone's cellphone in part because there is less danger of potential harm to an officer or of evidence being destroyed, but there is also a far greater danger to an individual's privacy because of the vast quantities and distinct types of personal information that can be stored on a phone. In one widely quoted passage, the Court wrote that treating the search of a purse like the search of a cellphone "would be like saying a ride on horseback is materially indistinguishable from a flight to the moon."

To codify the *Riley* ruling, CalECPA (SB 178, Leno; Stats 2015 Chap. 651) was passed which ultimately prohibits the government from compelling the release of electronic communication records from individuals, from a service provider, or through physical or digital manipulation of an electronic communication device. Electronic communication records can only be accessed via a warrant unless they meet any of the following criteria:

1. There is the consent of the owner or an authorized possessor.

2. A governmental entity has a good faith basis to believe that an emergency involving danger of death or serious physical injury requires access to the device's information.

3. The device is lost, stolen, or abandoned and a government entity must access the device for purposes of identifying the owner of the device.

4. A device is seized from a person incarcerated in a prison or jail.

5. It is necessary to locate the phone or user to respond to a 911 call.

6. When a person is on probation or parole and there are lawful search terms related to their electronic communication devices.

In all other circumstances, a government entity (i.e., a law enforcement agency), must obtain a search warrant.

3) **What this bill would do and policy considerations.** This bill would create a new exception to the warrant requirement under CalECPA, allowing for warrantless searches of tracking or surveillance devices discovered in an individual's residence, automobile, or personal property—if the individual has reason to believe the device was used to record or track them without their consent. The bill defines a "tracking or surveillance device" to include only those that can be used for surreptitiously monitoring, such as hidden cameras, geotags, and audio recorders, explicitly excluding devices like phones and laptops. Additionally, the bill requires that the individual who finds the device must consent to the warrantless search.

Supporters of the bill express concern that if such a device is discovered, its contents could be remotely wiped before law enforcement has time to obtain a warrant. This risk could become troubling in cases involving repeat stalking, where identifying the perpetrator is crucial. Opponents, however, argue that law enforcement already has effective strategies to prevent remote data deletion, such as removing the device's battery or placing it in a Faraday cage to block communications and prevent wiping.

Ultimately, the debate centers on whether a tracking or surveillance device found on private property and used without permission, should be afforded privacy protections, and whether that violation of the expectation of privacy in such spaces merits warrantless access.

The American Civil Liberties Union California Action, in opposition, argues:

> [N]othing in CalECPA prevents police from searching alleged stalking devices in an efficient and timely manner. As stated above, CalECPA simply requires that law enforcement get a warrant before searching any device – a process that can take as little as 15 minutes. Moreover, CalECPA currently allows *warrantless* searches of devices where the police agency believes an emergency involving danger of death or serious physical injury to *any person* requires accessing the device, so long as the agency files an appropriate warrant application within three days of the search. Therefore, AB 358's broad warrantless search scheme is unneeded because CalECPA already allows police to search electronic devices quickly, including without a warrant during an emergency.

The California Districts Attorney Association argues in support that:

> AB 358 permits victims of stalking and surreptitious recording to allow police to investigate any electronic devices used to record or track those victims. This exception allows law enforcement to expeditiously investigate crimes of stalking or surveillance without being restricted by CalECPA's broad expansion of privacy protections. CalECPA has expanded the privacy rights of defendants such that they now eclipse the privacy rights of their victims in these circumstances. Such a reversal of privacy rights benefitting defendants at the expense of their victims cannot stand and the legal framework should be returned to the constitutional principles underpinning those rights.

This legal framework, as highlighted in the analysis of the bill by the Assembly Public Safety Committee, may find some standing in *California v. Greenwood* (1988) 486 U.S. 35, where the U.S. Supreme Court held that the Fourth Amendment does not extend to garbage left for collection outside the home. One could argue that placing a tracking or surveillance device on someone else's property constitutes abandonment, akin to discarding trash, and therefore forfeits any reasonable expectation of privacy in the device. However, current case law has yet to directly address the use of such tracking and surveillance technologies in the context of warrantless searches, and it remains uncertain whether this violation of privacy would constitute a waiving of the Fourth Amendment protection. As the Assembly Public Safety Committee concludes, "it is not clear why the police cannot take the device found, get a warrant, and identify the person who left the device."

ARGUMENTS IN SUPPORT: The Office of the District Attorney of San Diego, the sponsor of the bill, write in support:

> The collection of this evidence can be extremely time-sensitive. First and foremost, there are our victims and their families. Victims have a right to have crimes involving them judiciously and prudently investigated.
>
> There are also technological reasons why the collection of data from a device is time-sensitive. Most notably, there are technological limitations on data extraction from devices. If a device restarts or powers down for any reason, the state it enters (known as "BFU") makes it much harder, or even impossible, to extract data from it. Some modern devices have, by design, self-imposed timers that force a restart after as little as 72 hours, putting the device in BFU mode automatically at the expiration of the timer. Whether due to the battery dying or a restart caused by the device itself, once the power down occurs, the chance of collecting usable evidence to solve a crime drastically diminishes.
>
> […]
>
> Finally, as to the surveillance and tracking component of AB 358, this narrow exception is focused on righting a wrong that CalECPA may have unintentionally created. In traditional Fourth Amendment jurisprudence, the focus was always on one's "reasonable expectation of privacy." CalECPA, in some circumstances, has empowered individuals committing crimes who have no expectation of privacy, at the expense of victims who do have an expectation of privacy. As mentioned above, cases that we have seen in San Diego include: (1) a person putting spy cameras in vents in a victim's home to spy on her in her bedroom and bathroom;

(2) a person putting spy cameras in bathrooms of local stores; and (3) a person putting spy cameras in a dorm within a public employer.

Giving authorization to the victims in these very narrow circumstances — a tracking device is found and being used to commit the crime, and the victim has a reasonable expectation of privacy where the device is located — empowers the victim, speeds up investigations, and brings CalECPA closer in line with Fourth Amendment jurisprudence.

AB 358 modernizes California's criminal procedure by protecting victims targeted by stalkers and domestic abusers who exploit increasingly available tracking tools. These concealable surveillance devices, like Bluetooth-enabled trackers and hidden cameras, can be placed in a victim's vehicle, home, or personal belongings, invade their privacy, and even threaten their lives. AB 358 sends a strong message that California will not tolerate the misuse of surveillance technology to harass and endanger others. We must act now to protect the rights and safety of individuals, including survivors of domestic abuse before further harm is done.

ARGUMENTS IN OPPOSITION: In opposition to the bill, Electronic Frontier Foundation argues:

As amended, the current bill still introduces a dangerous and unnecessary loophole into this important law. CalECPA currently allows warrantless searches of devices when a law enforcement agency believes an emergency involving danger of death or serious physical injury to any person requires accessing the device. To do so, an agency must file an appropriate warrant application within three days of the search. (If no emergency exists, then the police can simply get a warrant to search the device.)

Therefore, CalECPA already allows law enforcement officers to quickly search electronic devices without a warrant in appropriate situations. For this reason, we share the opinion of the Assembly Public Safety analysis that it remains unclear it is necessary to create this additional exception.

Creating a new provision for warrantless searches threatens the proper balance between privacy and public safety that the Legislature carefully crafted in passing CalECPA. A warrantless search, without a proper exception, violates Californians' constitutional rights. CalECPA includes strong protections that prohibit the government from overreaching. Search warrants must be narrowly particularized to ensure that they properly describe the information sought and seized.8 And any information obtained that is unrelated to the subject matter of the warrant must be "sealed and shall not be subject to further review, use, or disclosure" without an another court order.9 These additional protections protect Californians' constitutional rights and ensure that material unrelated to the search—which might be associated with people with no connection at all to a criminal investigation—are not rummaged through by law enforcement.

REGISTERED SUPPORT / OPPOSITION:

Support

San Diego County District Attorney's Office (Sponsor)
California District Attorneys Association

California Narcotic Officers' Association
California State Sheriffs' Association
Crime Victims Alliance
San Diego County Probation Officers Association

Opposition

ACLU California Action
All of Us or None (HQ)
All of Us or None Los Angeles
Californians United for A Responsible Budget
Electronic Frontier Foundation
Legal Services for Prisoners With Children
San Francisco Public Defender
Silicon Valley De-bug
Sister Warriors Freedom Coalition
Universidad Popular

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200