SENATE COMMITTEE ON PUBLIC SAFETY

Senator Jesse Arreguín, Chair
2025 - 2026 Regular

Bill No:	AB 358	**Hearing Date:**	June 24, 2025
Author:	Alvarez		
Version:	April 10, 2025		
Urgency:	No	**Fiscal:**	Yes
Consultant:	SU		

Subject: ***Criminal procedure: privacy***

HISTORY

Source: San Diego County District Attorney

Prior Legislation: AB 928 (Grayson), failed passage Assembly Public Safety, 2020
AB 1638 (Olbernolte), Ch. 196, Stats. of 2019
AB 165 (Cooper), not heard in Assembly Privacy, 2017
AB 1924 (Low), Ch. 511, Stats. of 2016
SB 178 (Leno), Ch. 651, Stats. of 2015

Support: California District Attorneys Association; California State Sheriffs' Association; San Diego County District Attorney's Office; Survivor Leader Network of California

Opposition: Culver City Democratic Club; Electronic Frontier Foundation

Assembly Floor Vote: 63 - 1

PURPOSE

The purpose of this bill is to create an exemption from the warrant requirement imposed by the California Electronic Communications Privacy Act (CalECPA), which would authorize law enforcement to access specified electronic device information without a warrant if an individual locates a device within their residence, automobile, or personal property and gives consent.

Existing law 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.)

Existing law provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these the fundamental right to privacy. (Cal. Const. art. I, § 1.)

Existing law 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.)

Existing law 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.)

Existing law enacts 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. (Pen. Code, §§ 1546-1546.4.)

Existing law states that a government entity may not do any of the following, except as authorized by statute:

- Compel the production of or access to electronic communication information from a service provider.
- Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
- Access electronic device information by means of physical interaction or electronic communication with the electronic device, however this 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, subd. (a)(1)-(3).)

Existing law allows a government entity to 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:

- Pursuant to a warrant;
- Pursuant to a wiretap order;
- Pursuant to an order for electronic reader records;
- Pursuant to a subpoena issued pursuant to existing state law, as specified; and,
- Pursuant to an order for a pen register or trap and trace device, or both. (Pen. Code, § 1546.1, subd. (b).)

Existing law allows a government entity to access electronic device information by means of physical interaction or electronic communication with the device only as follows:

- Pursuant to a warrant;
- Pursuant to a wiretap order;
- Pursuant to a tracking device search warrant;
- With the specific consent of the authorized possessor of the device;
- With the specific consent of the owner of the device, only when the device has been reported as lost or stolen;
- If the government entity believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information;

- If the government entity believes, in good faith, the device to be lost, stolen, or abandoned, provided that the government entity shall only access electronic device information in order to attempt to identify, verify, or contact its owner or authorized possessor;
- If the device is seized from an incarcerated person's possession, as specified;
- If the device is seized from an authorized possessor who is on parole under post-release community supervision;
- If the device is seized from an authorized possessor who is subject to an electronic device search condition of probation, mandatory supervision, or pretrial release;
- 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; and,
- Pursuant to an order for a pen register or trap and trace device, or both. (Pen. Code, § 1546.1, subd. (c).)

Existing law 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).)

Existing law allows an individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with CalECPA, or the California or U.S. Constitution, or a service provider or any other recipient of the warrant, order, or other legal process to petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of CalECPA, or the California or U.S. Constitution. (Pen. Code, § 1546.4, subd. (c).)

This bill creates an exception to CalECPA's warrant requirement which allows a government entity to access electronic device information with the specific consent of 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.

This bill defines a "tracking or surveillance device" as "an electronic device the sole purpose of which is to record audio or visual information or to permit the tracking of a person."

COMMENTS

1. Need for This Bill

According to the author:

> The ease of access to spy cameras and geo-trackers, some costing as little as $19.99, has led to a concerning rise in unauthorized surveillance and tracking of movements. This has enabled individuals with malicious intent to discreetly install cameras in others' homes. Under current state law, law enforcement must obtain a judicial warrant to search any electronic device, even when that device was secretly placed in someone's home or personal space without their knowledge or consent. A warrant can take anywhere from an hour, or up to 30 days according to the San Diego District Attorney's office. However, any delay in accessing these spy devices

allows perpetrators to hide their tracks and continue violating the privacy of their victims.

AB 358 empowers victims of stalking and abuse by ensuring law enforcement can access critical digital evidence—like surveillance footage or GPS data—without unnecessary delays. Specifically, the bill provides a narrow victim-centered exemption to CA Electronic Communication Privacy Law (CalECPA) by allowing individuals who locate spy cameras and geo-trackers in their own homes and vehicles to consent to those devices being searched by law enforcement.

AB 358 aligns with the U.S. Supreme Court's decision in California v. Greenwood to ensure it does not violate any Fourth Amendment protections. The amended bill only applies to spy cameras and movement trackers, while excluding cell phones, tablets, laptops, and cloud data that may contain personal information.

2. The Fourth Amendment and California Electronic Communications Privacy Act (CalECPA):

Both the United States and the California Constitutions guarantee the right of all persons to be secure from unreasonable searches and seizures. (U.S. Const., Amend. IV; Cal. Const., art. 1, sec. 13.) This protection applies to all unreasonable government intrusions into legitimate expectations of privacy. (*United States v. Chadwick* (1977) 433 U.S. 1, 7, overruled on other grounds by *California v. Acevedo* (1991) 500 U.S. 565.) In general, a search is not valid unless it is conducted pursuant to a warrant. A search warrant may not be issued without probable cause. "Reasonable and probable cause exists if a man of ordinary care and prudence would be led to conscientiously entertain an honest and strong suspicion that the accused is guilty." (*People v. Alvarado* (1967) 250 Cal.App.2d 584, 591, citations and quotations omitted.) The mere reasonableness of a search, assessed in light of the surrounding circumstances, is not a substitute for the warrant required by the Constitution. (*Arkansas v. Sanders* (1979) 442 U.S. 753, 758, overruled on other grounds by *California v. Acevedo*, supra.) There are exceptions to the warrant requirement, but the burden of establishing an exception is on the party seeking one. (*Arkansas v. Sanders*, 442 U.S. at 760.)

Application of the Fourth Amendment to searches or seizures of electronic information by law enforcement was directly addressed by the U.S. Supreme Court in several cases which largely formed the basis for the CalECPA. In *United States v. Jones* (2012) 565 U.S. 400, law enforcement agents planted a GPS tracking device on a vehicle without a warrant. The court ruled that this was an unreasonable search, due to the amount of information a tracking device discloses and based on the length of time the person was tracked. (*Id*. at p. 404.) California reacted to the *Jones* case by establishing a warrant protocol for the use of a tracking device in Penal Code section 1534.

Two years later, the Supreme Court decided *Riley v. California* (2014) 573 U.S. 373, the Unites States Supreme Court unanimously held that police must generally obtain a warrant before searching digital information on arrestee's cell phone. (*Id*. at p. 386.) In so doing, the Court recognized that the search of digital data has serious implications for an individual's privacy. The court observed that cell phones are both qualitatively and quantitatively different than other objects which might be found on an arrestee's person. (*Id*. at p. 393.) "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as telephones. They could just as easily be called cameras, video

players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." (*Ibid*.) The Court also recognized that "cloud computing" poses additional complications when considering privacy concerns because the data viewed may not in fact be stored on the device itself. (*Id*. at p. 397.) The Court concluded, "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." (*Id*. at p. 403, quotation omitted.)

In so doing, the Court noted:

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.
>
> Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. (*Riley, supra,* at p. 401.)

In response to *Riley v. California*, *supra*, 573 U.S. 373, the Legislature passed SB 178 (Leno), Chapter 651, Statutes of 2015, which established CalECPA. SB 178 codified the requirement that law enforcement officials obtain a warrant before "searching" a third party's electronic records for law enforcement purposes. In doing so, California made it clear that a warrant is required when there is an intrusion into a person's electronic records and devices even if a third party has access to them.

CalECPA has various exceptions including in cases involving the consent of the device's owner. (Pen. Code, § 1546.1, subd. (c)(5).) Another exemption allows a government entity to access electronic information without a warrant with the specific consent of the authorized possessor of the device. (Pen. Code, § 1546.1, subd. (c)(4).) "Authorized possessor" is defined as 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, subd. (b).)

This bill would create a related exception to CalECPA and permit law enforcement to seize and search a device when an individual finds a tracking or surveillance device in their home, vehicle, or personal property and gives consent because it is reasonably believed that the device has been used for the purpose of tracking or recording that person without their permission. This exception would apply only to an electronic devices which has the *sole* purpose of recording audio or visual information or to permit tracking of a person. In other words, this exception would apply to a camera or an AirTag or other GPS tracking device, but not to a cell phone.

Significantly, one of the United States Supreme Court cases which formed the basis for CalECPA involved the use of a GPS tracking device. (See *U.S. v. Jones*, *supra*, 565 U.S. 400.) Moreover, AB 539 (Acosta), Chapter 342, Statutes of 2017, addressed law enforcement ability to investigate disorderly conduct in which the individual uses any instrumentality to view and invade a person's privacy and secretly videotape, film, photograph, or record by electronic

means them in violation of Penal Code section 647, subdivisions (j)(1)-(3). Since January 1, 2018, Penal Code section 1524, subdivision (a) explicitly allows law enforcement to obtain a warrant when the property or things to be seized consist of evidence that tends to show that a violation of the crime of disorderly conduct related to invasion of privacy has occurred or is occurring.

Proponents of this bill argue that by requiring them to obtain a warrant to get subscriber or personally identifying information, investigations are delayed and the IP address may change by the time local law enforcement obtains the warrant. Presumably, some of those same concerns have been present since law enforcement has had the ability to obtain a warrant for these types of offenses, and yet individuals have been held accountable. For example, police might choose to leave a tracking device or camera in place while a warrant is sought and the case investigated so as not to tip off the owner of the device. As the Supreme Court noted in *Riley*, *supra*, 573 U.S. 373:

> The warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency." [Citation] Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient. [Citations]

(*Id*. at p. 401, citations omitted.)

If however, in balancing privacy interests, police efficiency, and victim safety, this Committee feels that another exception to CalECPA is warranted, should the bill be amended to require law enforcement to obtain a warrant after the fact, as is the case with the emergency exception to CalECPA? Penal Code Section 1546.1, subdivision (h) requires a law enforcement officer who obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person that requires access to the electronic information without delay, to file an application for a warrant within three court days after obtaining the electronic information. Should this same requirement be applied under these circumstances?

Relatedly, should there be a remedy for individuals other than a criminal defendant who are impacted? While a defendant might be able to file a motion to suppress, the same is not true if there are not criminal charges filed. For example, what if a person accidentally drops an AirTag in an Uber but the driver mistakenly believes that they are being tracked? Penal Code section 1546.4, subdivision (c) allows an individual whose information is targeted by a warrant that is inconsistent with CalECPA, or the Constitution to petition the issuing court to void or modify the warrant or to order the destruction of any information obtained in violation of CalECPA or the Constitution. Should this same remedy be allowed for persons impacted by exception this bill seeks to create?

3. Consent Searches in Joint Owner or Occupant Situations

The Fourth Amendment's prohibition against warrantless searches does not apply when voluntary consent to the search has been given by someone authorized to do so. (*Illinois v. Rodriguez* (1990) 497 U.S. 177, 181; *People v. Rivera* (2007) 41 Cal.4th 304, 311.) And as noted above, CalECPA contains an exception for when the owner of the electronic device consents to the search.

The problem is that in the scenario addressed by this bill, the owner of the device is not giving consent; rather it is the person who found the device on their property. This raises the question of whether there is valid consent when there are joint owners or occupants in the property where the tracking or recording device is found?

Courts have held that a person with common authority over a premise or property may validly consent to its search. (See *U.S. v. Matlock* (1974) 415 U.S. 164, 170 [consent to search rented room by person who told police she and defendant were co-occupants]; *People v. Witkins* (1993) 14 Cal.App.4th 761, 765 [consent by co-tenant]; *Fraiser v. Cupp* (1969) 394 U.S. 731, 740 [joint user of duffle bag].) Consent has also been found to be valid in cases of apparent authority, such as when a wife has left the residence and was staying at a domestic violence shelter. (See *People v. Bishop* (1996) 44 Cal.App.4t 220, 236-239.) However, when "a physically present inhabitan[t]" refuses to consent, that refusal "is dispositive as to him, regardless of the consent of a fellow occupant." (*Georgia v. Randolph* (2006) 547 U.S. 103, 122-123.)

Recently, in *People v. Clymer* (2024) 107 Cal.App.5th 131, the Court of Appeal, relying on the "authorized possessor" exception, held that search of the decedent's electronic devices without a warrant did not violate CalECPA because the decedent's parents were "authorized possessors" of his electronic devices, and consented to the search. In that case, the decedent's parents repeatedly urged police to search their son's iPhone and iPad so the officer could "find out what happened to their son," and they provided the passcode to the devices. (*Id*. at p. 135.)

Nevertheless, a proprietary interest in a property does not automatically imply actual or apparent authority to consent to a search, such as in the case of a landlord. (See *Chapman v. U.S*. (1961) 365 U.S. 610, 612.)

4. Argument in Support

According to the San Diego County District Attorney, the sponsor of this bill:

> The CalECPA created a new framework for warrants in the digital space. AB 358 aims to empower victims, preserve evidence, and save resources by creating a narrow exception to this newly created statutory framework. This exception will align CalECPA with general Fourth Amendment jurisprudence.
>
> In its current form, CalECPA can lead to results that shock the conscience:
>
> - A Peeping Tom leaves a spy camera in a women's bunkroom at a fire station. Their employer has no right to consent to the search of the device.
>
> - A guest in a family home leaves spy cameras in the children's bathroom. The parents have no right to consent to the search of these devices.
>
> The collection of this evidence can be highly time sensitive. First and foremost, there are our victims and their families. Victims have a right to have crimes involving them investigated judiciously and prudently.
>
> 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 do not expect privacy, at the expense of victims who do expect 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.

Granting authorization to the victims in these very narrow circumstances — specifically, when a tracking device is found and being used to commit the crime, and the victim has a reasonable expectation of privacy at the location 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.

5. Argument in Opposition

According to the Electronic Frontier Foundation:

EFF co-sponsored CalECPA, which requires state law enforcement to get a warrant before they can access electronic information about who we are, where we go, who we know, and what we do. The law was supported by many civil liberties groups and technology companies as a common-sense extension of the U.S. Supreme Court's unanimous decision in *Riley v. California*. Recognizing that the information held on smart phones can reveal comprehensive records of a person's familial, political, professional, religious, and sexual associations, the Court in *Riley* held that before police can access information held on a smart phone, they must get a search warrant. Among other provisions, CalECPA reflects *Riley* and generally requires police to get a warrant before accessing electronic device information via physical or electronic interaction with the device.

We appreciate the work and continued conversations with the author's office about how to address the bill's problems.

As written, however, the bill 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.)

Thus, 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 the need for this new exception remains unclear.

Creating a new provision for warrantless searches threatens the proper balance between privacy and public safety that the Legislature carefully crafted in passing CalECPA. 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. 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 another court order. 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.

To address our concerns around the new proposed exemption to CalECPA, we suggest two amendments that would remove our opposition to this bill. Our first amendment adds a revision to Penal Code Section 1546.1(h) to require law enforcement get a warrant within 72 hours after doing the warrantless search that A.B. 358 would create. This ensures A.B. 358 will reflect current practice for warrants…

Our second suggested change goes hand-in-hand with the first. This amendment would add a revision to Penal Code Section 1546.4(c) to give a remedy to people whose rights were violated because law enforcement failed to comply with AB 358…

The warrant requirement in the first half of our amendments allows a court to order that law enforcement delete the information they obtained from the device, which could include revealing photos, audio, or locations that are not relevant to any criminal investigation. The second half of our amendment ensures that those subject to wrongful or overbroad searches have a way to seek redress, which is especially important when the police conduct searches without a warrant.

-- END –