AB-358 Criminal procedure: privacy. (2025-2026)

Date Published: 06/25/2025 09:00 PM

AMENDED IN SENATE JUNE 25, 2025

AMENDED IN ASSEMBLY APRIL 10, 2025

AMENDED IN ASSEMBLY MARCH 18, 2025

CALIFORNIA LEGISLATURE— 2025–2026 REGULAR SESSION

ASSEMBLY BILL NO. 358

Introduced by Assembly Member Alvarez
(Coauthor: Assembly Member Macedo)

January 30, 2025

An act to amend ~~Section 1546.1~~ *Sections 1546.1 and 1546.4* of the Penal Code, relating to criminal procedure.

LEGISLATIVE COUNSEL'S DIGEST

AB 358, as amended, Alvarez. Criminal procedure: privacy.

Existing law, the Electronic Communications Privacy Act, prohibits a government entity from compelling the production of, or access to, electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions. Existing law authorizes a government entity to access electronic device information by means of physical interaction or electronic communication with the device in certain circumstances, including, pursuant to the specific consent of the authorized possessor of the device or if the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to a person requires access to the information. *Existing law requires a government entity that obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, within 3 court days after obtaining the electronic information, to file with the appropriate court an application for a warrant or order setting forth the facts giving rise to the emergency. Existing law requires the court to promptly rule on the application and to destroy all information obtained upon a finding that the facts did not give rise to an emergency or upon rejecting the application on any other ground.*

This bill would additionally authorize a government entity to access electronic device information with the specific consent of an individual who locates a tracking or surveillance device, as defined, and the device is reasonably believed to have been used to track or record the individual without their permission. *The bill would require a government entity that obtains information through this method, within 3 court days after obtaining the electronic information, to follow the above process for applying for a warrant or*

order from a court by setting forth the facts that describe the circumstances and would require the court to promptly rule on the application and order the immediate destruction of all information obtained upon a finding that the facts were not as described. Existing law authorizes an individual whose information is targeted by a warrant, order, or other legal process, or other specified recipients of a warrant, that is inconsistent with the act or the California or United States Constitution, 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 the act or the California or United States Constitution.

This bill would recast the provisions described above to authorize an individual whose information is sought or obtained by a government entity in a manner that is inconsistent with the act or the California or United States Constitution, or other specified recipients of a warrant, order, legal process, request, or demand seeking the individual's information, to petition a court to void or modify the warrant, order, other legal process, request, or demand to order the destruction of the information.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

---

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Section 1546.1 of the Penal Code is amended to read:

1546.1. (a) Except as provided in this section, a government entity shall not do any of the following:

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

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

(3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. 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.

(b) 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:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.

(4) Pursuant to a subpoena issued pursuant to existing state law, 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 by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(5) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.

(c) A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to a tracking device search warrant issued pursuant to paragraph (12) of subdivision (a) of Section 1524 and subdivision (b) of Section 1534.

(4) With the specific consent of the authorized possessor of the device.

(5) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.

(6) 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.

(7) If the government entity, in good faith, believes 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 the owner or authorized

possessor of the device.

(8) 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. This paragraph shall not be construed to supersede or override Section 4576.

(9) 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 postrelease community supervision under the supervision of county probation.

(10) 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.

(11) 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.

(12) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.

(13) (A) 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.

(B) For the purpose of subparagraph (A), a "tracking or surveillance device" means an electronic device the sole purpose of which is to record audio or visual information or to permit the tracking of a person.

(d) Any warrant for electronic information shall comply with the following:

(1) The warrant shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought, provided, however, that in the case of a warrant described in paragraph (1) of subdivision (c), the court may determine that it is not appropriate to specify time periods because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and 1054.7. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.

(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following:

(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.

(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

(g) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:

(1) The government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

(2) The government entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.

(3) The government entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(4) The service provider or subscriber is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.

(h) If a government entity 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, *or as described in paragraph (13) of subdivision (c),* the government entity shall, within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the ~~emergency,~~ *emergency or that describe the circumstances described in paragraph (13) of subdivision (c),* and, if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification shall be given pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency *or were not as described in paragraph (13) of subdivision (c),* or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.

(i) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:

(1) Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.

(2) Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.

(3) Require a service provider to provide subscriber information.

(j) This section does not limit the authority of the Public Utilities Commission or the State Energy Resources Conservation and Development Commission to obtain energy or water supply and consumption information pursuant to the powers granted to them under the Public Utilities Code or the Public Resources Code and other applicable state laws.

(k) This chapter shall not be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity's possession.

SEC. 2. *Section 1546.4 of the Penal Code is amended to read:*

1546.4. (a) 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 of this chapter. The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of Section 1538.5.

(b) The Attorney General may commence a civil action to compel any government entity to comply with the provisions of this chapter.

(c) An individual whose information is ~~targeted by a warrant, order, or other legal process~~ *sought or obtained by a government entity in a manner* that is inconsistent with this chapter, or the California Constitution or the United States Constitution, or a service provider or any other recipient of the warrant, order, ~~or~~ other legal ~~process~~ *process, request, or demand* may petition ~~the issuing~~ *a* court to void or modify the warrant, order, ~~or~~ *legal* process, *request, or demand* or to order the destruction of any information obtained in violation of this chapter, ~~or~~ the California Constitution, or the United States Constitution.

(d) A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization,

emergency certification, or wiretap order issued pursuant to this chapter.