AMENDED IN ASSEMBLY JUNE 24, 2015

AMENDED IN SENATE JUNE 2, 2015

AMENDED IN SENATE APRIL 22, 2015

AMENDED IN SENATE MARCH 16, 2015

SENATE BILL No. 178

Introduced by Senators Leno and Anderson
(Principal coauthor: Assembly Member Gatto)
(Coauthors: Senators Cannella, Gaines, Hertzberg, Hill, McGuire, Nielsen, and Roth)
(Coauthors: Assembly Members Chiu, Dahle, Gordon, Maienschein, Obernolte, Quirk, Ting, and Weber)

February 9, 2015

An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 178, as amended, Leno. Privacy: electronic communications: search warrant.

(1) Existing law provides that a search warrant may only be issued 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. Existing law also states the grounds upon which a search warrant may be issued, including, among other grounds, when the property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony, or when there is a warrant to arrest a person.

This bill would prohibit a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant or wiretap order, except for emergency situations, as defined. The bill would define a number of terms for those purposes, including, among others, "electronic communication information" and "electronic device information," which the bill defines collectively as "electronic information." The bill would require a search warrant for electronic information to encompass no more information than is necessary to achieve the objective of the search and would impose other conditions on the use of the search warrant or wiretap order and the information obtained, including retention and disclosure. The bill would, subject to exceptions, require a government entity that executes a search warrant or wiretap order pursuant to these provisions to contemporaneously provide notice, as specified, to the identified target, that informs the recipient that information about the recipient has been compelled or requested, and that states the nature of the government investigation under which the information is sought. The bill would authorize a delay of 90 days, subject to renewal, for providing the notice under specified conditions that constitute an emergency. The bill would require the notice to include a copy of the warrant or order or statement describing the emergency under which the notice was delayed. The bill would provide that electronic information obtained in violation of these provisions would be inadmissible in a criminal, civil, or administrative proceeding. The bill would provide that 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, wiretap order, or other order issued pursuant to these provisions.

(2) The California Constitution provides for the Right to Truth in Evidence, which requires a ⅔ vote of the Legislature to exclude any relevant evidence from any criminal proceeding, as specified.

Because this bill would exclude evidence obtained or retained in violation of its provisions in a criminal proceeding, it requires a ⅔ vote of the Legislature.

Vote: ⅔. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Chapter 3.6 (commencing with Section 1546) is added to Title 12 of Part 2 of the Penal Code, to read:

Chapter 3.6. Electronic Communications Privacy Act

1546. For purposes of this chapter, the following definitions apply:

(a) An "adverse result" means any of the following:

(1) Danger to the life or physical safety of an individual.

(2) Flight from prosecution.

(3) Imminent destruction of or tampering with evidence.

(4) Intimidation of potential witnesses.

(5) Serious jeopardy to an investigation or undue delay of a trial.

(b) "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.

(c) "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.

(d) "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 in this chapter.

(e) "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.

(f) "Electronic device" means a device that stores, generates, or transmits information in electronic form.

(g) "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.

(h) "Electronic information" means electronic communication information or electronic device information.

(i) "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(j) "Service provider" means a person or entity offering an electronic communication service.

(k) "Specific consent" means consent ~~delivered~~ *provided* directly to the government entity seeking ~~information.~~ *information, including, but not limited to, when the government entity is the addressee or intended recipient of an electronic communication.*

(*l*) "Subscriber information" means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

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 except the authorized possessor of the device.

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

(b) A government entity may compel the production of or access to electronic information subject to subdivision (d) and only pursuant to a wiretap order pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1, or pursuant to a search warrant pursuant to Chapter 3 (commencing with Section 1523), provided that the warrant shall not compel the production of or authorize access to the contents of any electronic communication initiated after the issuance of the warrant.

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

(1) In accordance with a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1 or in accordance with a search warrant issued pursuant to Chapter 3 (commencing with Section 1523), provided that a warrant shall not authorize accessing the contents of any electronic communication initiated after the issuance of the warrant.

(2) With the specific consent of the authorized possessor of the ~~device, including when a government entity is the intended recipient of an electronic communication initiated by the authorized possessor of the device.~~ *device.*

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

(4) 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.

(5) 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.

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

(1) The warrant or order shall be limited to only that information necessary to achieve the objective of the warrant or wiretap order, including by specifying the target individuals or accounts, the applications or services, the types of information, and the time periods covered, as appropriate.

(2) The warrant or order shall identify the effective date upon which the warrant or order is to be executed, not to exceed 10 days from the date the warrant is signed, or explicitly state whether the warrant or wiretap order encompasses any information created after its issuance.

(3) The warrant or order 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 or wiretap orders.

(e) When issuing any warrant or wiretap order for electronic information, or upon the petition from the target or recipient of the warrant or wiretap order, a court may, at its discretion, do any or all 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 that determination is made.

(f) A service provider may disclose, but shall not be required to 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 delete that information within 90 days unless the entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed or 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.

(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, the entity shall, within three days after obtaining the electronic information, file with the appropriate court a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency. The court shall promptly rule on the motion and shall order the immediate destruction of all information obtained, upon a finding that the facts did not give rise to an emergency.

(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 either 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.

1546.2. (a) Except as otherwise provided in this section, any government entity that executes a warrant or wiretap order or obtains electronic information in an emergency pursuant to Section 1546.1 shall contemporaneously serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant, order, or emergency request, a notice that informs the recipient that information about the recipient has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or order, or a written statement setting forth facts giving rise to the emergency.

(b) If there is no identified target of a warrant, wiretap order, or emergency request or access at the time of its issuance, the government entity shall submit to the Department of Justice within 72 hours a report that states with reasonable specificity the nature of the government investigation under which the information was sought and includes a copy of the warrant, or order, or a written statement setting forth facts giving rise to the emergency. The Department of Justice shall publish each report received pursuant to this subdivision on its Internet Web site within 90 days of receiving the report.

(c) (1) When a wiretap order or search warrant is sought under Section 1546.1, the government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).

(3) Upon expiration of the period of delay of the notification, the government entity shall serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, each individual whose electronic information was acquired, a document that includes the information described in subdivision (a), a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.

(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

1546.4. (a) Except as proof of a violation of this chapter, no evidence obtained or retained in violation of this chapter shall be admissible in a criminal, civil, or administrative proceeding, or used in an affidavit in an effort to obtain a search warrant or court order.

(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, wiretap order, or other legal process 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, wiretap order, or other legal process may petition the issuing court to void or modify the warrant, wiretap order, or process, or to order the destruction of any information obtained in violation of this chapter, 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

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

O