

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, Quirk, ~~Steinorth~~, 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.

Existing

(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,~~” “~~service provider,~~” *information*” and “~~electronic device information,~~” *information,*” which the bill defines collectively as “*electronic information.*” The bill would require a search warrant for ~~electronic communication~~ 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 communication~~ 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 or warrant,~~ wiretap order, *or other order* issued pursuant to these provisions. The bill would also require a government entity that obtains ~~electronic communication~~ information pursuant to these provisions to make an annual report to the Attorney General, and would require the Department of Justice to annually publish a summary of the report on its Internet Web site. By requiring local law enforcement entities to make those annual reports, this bill would impose a state-mandated local program.

(2) The California Constitution provides for the Right to Truth in Evidence, which requires a $\frac{2}{3}$ 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 $\frac{2}{3}$ vote of the Legislature.

The

(3) *The California Constitution* requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that, if the Commission on State Mandates determines that the bill contains costs mandated by the state, reimbursement for those costs shall be made pursuant to these statutory provisions.

Vote: ~~majority~~^{2/3}. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

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

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

3
4 CHAPTER 3.6. ELECTRONIC COMMUNICATIONS PRIVACY ACT
5

6 1546. For purposes of this chapter, the following definitions
7 apply:

8 (a) An “adverse result” means any of the following:

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

10 (2) Flight from prosecution.

11 (3) Imminent destruction of or tampering with evidence.

12 (4) Intimidation of potential witnesses.

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

15 (b) “Authorized possessor” means the possessor of an electronic
16 device when that person is the owner of the device or has been
17 authorized to possess the device by the owner of the device.

18 (c) “Electronic communication” means the transfer of signs,
19 signals, writings, images, sounds, data, or intelligence of any nature
20 in whole or in part by a wire, radio, electromagnetic, photoelectric,
21 or photo-optical system.

22 (d) “Electronic communication information”—~~is~~ *means* any
23 information about an electronic communication or the use of an
24 electronic communication service, including, but not limited to,
25 the contents, sender, recipients, format, or location of the sender
26 or recipients at any point during the communication, the time or
27 date the communication was created, sent, or received, or any
28 information pertaining to any individual or device participating in

1 the communication, including, but not limited to, an IP address.
2 Electronic communication information does not include subscriber
3 information as defined in this chapter.

4 (e) “Electronic communication service” ~~is~~ *means* a service that
5 provides to its subscribers or users the ability to send or receive
6 electronic communications, including any service that acts as an
7 intermediary in the transmission of electronic communications, or
8 stores electronic communication information.

9 (f) “Electronic device” means a device that stores, generates,
10 or transmits information in electronic form.

11 (g) “Electronic device information” means any information
12 stored on or generated through the operation of an electronic
13 device, including the current and prior locations of the device.

14 (h) *“Electronic information” means electronic communication*
15 *information or electronic device information.*

16 ~~(h)~~

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

20 ~~(i)~~

21 (j) “Service provider” means a person or entity offering an
22 electronic communication service.

23 ~~(j)~~

24 (k) “Specific consent” is consent delivered directly to the
25 government entity seeking information.

26 ~~(k)~~

27 (l) “Subscriber information” means the name, street address,
28 telephone number, email address, or similar contact information
29 provided by the subscriber to the provider to establish or maintain
30 an account or communication channel, a subscriber or account
31 number or identifier, the length of service, and the types of services
32 used by a user of or subscriber to a service provider.

33 1546.1. (a) Except as provided in this section, a government
34 entity shall not do any of the following:

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

37 (2) Compel the production of or access to electronic device
38 information from any person or entity except the authorized
39 possessor of the device.

1 (3) Access electronic device information by means of physical
2 interaction or electronic communication with the device, ~~except~~
3 ~~with the specific consent of the authorized possessor of the device.~~

4 (b) A government entity may compel the production of or access
5 to ~~electronic communication information or electronic device~~
6 ~~information, or access electronic device information by means of~~
7 ~~physical interaction or electronic communication with the device,~~
8 *information* subject to subdivision ~~(e)~~ (d) and only pursuant to a
9 wiretap order pursuant to Chapter 1.4 (commencing with Section
10 629.50) of Title 15 of Part 1, or pursuant to a search warrant
11 pursuant to Chapter 3 (commencing with Section 1523), provided
12 that the warrant shall not compel the production of or authorize
13 access to the contents of any electronic communication initiated
14 after the issuance of the warrant.

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

18 (1) In accordance with a wiretap order issued pursuant to
19 Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part
20 1 or in accordance with a search warrant issued pursuant to Chapter
21 3 (commencing with Section 1523), provided that a warrant shall
22 not authorize accessing the contents of any electronic
23 communication initiated after the issuance of the warrant.

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

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

30 (4) If the government entity, in good faith, believes that an
31 emergency involving ~~imminent~~ danger of death or serious physical
32 injury to any person requires access to the electronic device
33 information.

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

38 (d) Any warrant or wiretap order for ~~electronic communication~~
39 ~~information or electronic device~~ information shall comply with
40 the following:

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

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

11 (3) The warrant or order shall comply with all other provisions
12 of California and federal law, including any provisions prohibiting,
13 limiting, or imposing additional requirements on the use of search
14 warrants or wiretap orders.

15 (e) When issuing any warrant or wiretap order for electronic
16 ~~communication information or electronic device~~ information, *or*
17 *upon the petition from the target or recipient of the warrant or*
18 *wiretap order*, a court may, at its discretion, do any or all of the
19 following:

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

24 (2) Require that any information obtained through the execution
25 of the warrant or order that is unrelated to the objective of the
26 warrant be destroyed as soon as feasible after that determination
27 is made.

28 (f) A service provider may disclose, but shall not be required
29 to disclose, electronic communication information or subscriber
30 information when that disclosure is not otherwise prohibited by
31 *state or federal law*.

32 (g) If a government entity receives electronic communication
33 information voluntarily provided pursuant to subdivision (f), it
34 shall delete that information within 90 days unless the entity has
35 or obtains the specific consent of the sender or recipient of the
36 electronic communications about which information was disclosed
37 or obtains a court order authorizing the retention of the information.
38 A court shall issue a retention order upon a finding that the
39 conditions justifying the initial voluntary disclosure persist, in
40 which case the court shall authorize the retention of the information

1 only for so long as those conditions persist, or there is probable
2 cause to believe that the information constitutes evidence that a
3 crime has been committed.

4 (h) If a government entity ~~requests that a service provider~~
5 ~~disclose information, or if the government entity obtains~~
6 ~~information,~~ *obtains electronic information* pursuant to an
7 emergency involving danger of death or serious physical injury to
8 a person, that requires access to the electronic information without
9 delay, the entity shall, within three days after ~~seeking disclosure,~~
10 *obtaining the electronic information*, file with the appropriate court
11 a motion seeking approval of the ~~requested~~ emergency disclosures
12 that shall set forth the facts giving rise to the emergency. The court
13 shall promptly rule on the motion and shall order the immediate
14 destruction of all information ~~received in response to the request~~
15 *obtained*, upon a finding that the facts did not give rise to an
16 emergency.

17 (i) This section does not limit the authority of a ~~governmental~~
18 *government* entity to use an administrative, grand jury, trial, or
19 civil discovery subpoena to do either of the following:

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

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

29 1546.2. (a) Except as otherwise provided in this section, any
30 government entity that executes a warrant or wiretap order or ~~issues~~
31 *obtains electronic information in* an emergency ~~request~~ pursuant
32 to Section 1546.1 shall contemporaneously serve upon, or deliver
33 by registered or first-class mail, electronic mail, or other means
34 reasonably calculated to be effective, the identified targets of the
35 warrant, order, or emergency request, a notice that informs the
36 recipient that information about the recipient has been compelled
37 or requested, and states with reasonable specificity the nature of
38 the government investigation under which the information is
39 sought. The notice shall include a copy of the warrant or order, or
40 a written statement setting forth facts giving rise to the emergency.

1 (b) If there is no identified target of a warrant, wiretap order,
2 or emergency request *or access* at the time of its issuance, the
3 government entity shall take reasonable steps to provide the notice,
4 within three days of the execution of the warrant, *wiretap order*,
5 *or emergency request or access*, to all individuals about whom
6 information was disclosed or obtained.

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

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

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

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

36 1546.4. (a) Except as proof of a violation of this chapter, no
37 evidence obtained or retained in violation of this chapter shall be
38 admissible in a criminal, civil, or administrative proceeding, or
39 used in an affidavit in an effort to obtain a search warrant or court
40 order.

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

4 (c) ~~If a warrant or wiretap order does not comply~~ *An individual*
5 *whose information is targeted by a warrant, wiretap order, or*
6 *other legal process that is inconsistent with this chapter, or the*
7 *California or United States Constitution, or a service provider,*
8 *provider or any other recipient of the warrant or wiretap order, or*
9 ~~any individual whose information is targeted by the warrant or~~
10 ~~wiretap order, warrant, wiretap order, or other legal process~~ may
11 petition the issuing court to void or modify the ~~warrant or wiretap~~
12 ~~order~~ *warrant, wiretap order, or process, or to order the destruction*
13 *of any information obtained in violation of this chapter, the*
14 *California Constitution, or the United States Constitution.*

15 (d) A California or foreign corporation, and its officers,
16 employees, and agents, are not subject to any cause of action for
17 providing records, information, facilities, or assistance in
18 accordance with the terms of a ~~warrant~~ *warrant, court order,*
19 *statutory authorization, emergency certification, or wiretap order*
20 issued pursuant to this chapter.

21 1546.6. A government entity that obtains electronic
22 ~~communication~~ information pursuant to this chapter shall make
23 an annual report to the Attorney General. The report shall be made
24 on or before February 1, 2017, and each February 1 thereafter. To
25 the extent it can be reasonably determined, the report shall include
26 all of the following:

27 (a) The number of requests or demands for electronic
28 ~~communication~~ information.

29 (b) The number of requests or demands made, and the number
30 of records received for each of the following types of records:

- 31 (1) Electronic communication content.
- 32 (2) Location information.
- 33 ~~(3) Electronic device information.~~
- 34 ~~(4)~~
- 35 (3) Other electronic ~~communication~~ information.

36 (c) For each of the types of records listed in subdivision (b), all
37 of the following:

38 (1) The number of requests or demands that were each of the
39 following:

- 40 (A) Wiretap orders obtained pursuant to this chapter.

1 (B) Search warrants obtained pursuant to this chapter.
 2 (C) Emergency requests pursuant to subdivision (h) of Section
 3 1546.1.

4 (2) The total number of users whose information was requested
 5 or demanded.

6 (3) The total number of requests or demands that did not specify
 7 a target individual.

8 (4) The number of requests or demands complied with in full,
 9 partially complied with, or refused.

10 (5) The number of times the notice to the affected party was
 11 delayed and the average length of the delay.

12 (6) The number of times records were shared with other
 13 government entities or any department or agency of the federal
 14 government, and the agencies with which the records were shared.

15 (7) For contents of electronic communications, the total number
 16 of communications contents received.

17 (8) For location information, the average period for which
 18 location information was obtained or received and the total number
 19 of location records received.

20 (9) For other electronic communication information, the types
 21 of records requested and the total number of records of each type
 22 received.

23 1546.8. (a) On or before April 1, 2017, and each April 1
 24 thereafter, the Department of Justice shall publish on its Internet
 25 Web site both of the following:

26 (1) The individual reports from each government entity that
 27 requests or compels the production of contents or records pertaining
 28 to an electronic communication or location information.

29 (2) A summary aggregating each of the items in subdivisions
 30 (a) to (c), inclusive of Section 1546.6.

31 (b) Nothing in this chapter shall prohibit or restrict a service
 32 provider from producing an annual report summarizing the
 33 demands or requests it receives under this chapter.

34 SEC. 2. If the Commission on State Mandates determines that
 35 this act contains costs mandated by the state, reimbursement to
 36 local agencies and school districts for those costs shall be made
 37 pursuant to Part 7 (commencing with Section 17500) of Division
 38 4 of Title 2 of the Government Code.

O