

Introduced by Senators Leno and Anderson

**(Coauthors: Senators Cannella, Gaines, Hertzberg, McGuire,
Nielsen, and Roth)**

(Coauthors: Assembly Members Chiu, Dahle, Gordon, Maienschein,
Quirk, Steinorth, and Ting)

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 introduced, Leno. Privacy: electronic communications: search warrant.

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," and "electronic device 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 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.

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. 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:

1 CHAPTER 3.6. ELECTRONIC COMMUNICATIONS PRIVACY ACT

2
3 1546. For purposes of this chapter, the following definitions
4 apply:

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

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

7 (2) Flight from prosecution.

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

9 (4) Intimidation of potential witnesses.

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

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

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

19 (d) “Electronic communication information” is any information
20 about an electronic communication or the use of an electronic
21 communication service, including, but not limited to, the contents,
22 sender, recipients, format, location, or time of the sender or
23 recipients at any point during the communication, or any
24 information pertaining to any individual or device participating in
25 the communication, including, but not limited to, an IP address.
26 Electronic communication information does not include subscriber
27 information as defined in this chapter.

28 (e) “Electronic communication service” is a service that provides
29 to its subscribers or users the ability to send or receive electronic
30 communications, including any service that acts as an intermediary
31 in the transmission of electronic communications, or stores
32 electronic communication information.

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

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

38 (h) “Government entity” means a department or agency of the
39 state or a political subdivision thereof, or an individual acting for
40 or on behalf of the state or a political subdivision thereof.

1 (i) “Service provider” means a person or entity offering an
2 electronic communication service.

3 (j) “Specific consent” is consent delivered directly to the
4 government entity seeking information that is given in response
5 to a specific request and is valid only for a specified period of time.
6 Specific consent may be withdrawn at any time.

7 (k) “Subscriber information” means the name, street address,
8 phone number, email address, or similar contact information
9 provided by the subscriber to the provider of an electronic
10 communication service for the purpose of establishing a
11 communication channel between that subscriber and that provider,
12 a subscriber or account number or identifier, the length of service,
13 and the types of services used by a user of or subscriber to a service
14 provider.

15 1546.1. (a) Except as provided in this section, a government
16 entity shall not do any of the following:

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

19 (2) Compel the production of or access to electronic device
20 information from any person or entity except the authorized
21 possessor of the device.

22 (3) Access electronic device information by means of physical
23 interaction or electronic communication with the device, except
24 with the specific consent of the authorized possessor of the device.

25 (b) A government entity may compel the production of or access
26 to electronic communication information or electronic device
27 information, or access electronic device information by means of
28 physical interaction or electronic communication with the device,
29 subject to subdivision (c) and only pursuant to a wiretap order
30 pursuant to Chapter 1.4 (commencing with Section 629.50) of
31 Title 15 of Part 1, or pursuant to a search warrant pursuant to
32 Chapter 3 (commencing with Section 1523), provided that the
33 warrant shall not compel the production of or authorize access to
34 the contents of any electronic communication initiated after the
35 issuance of the warrant.

36 (c) Any warrant or wiretap order for electronic communication
37 information or electronic device information shall comply with
38 the following:

39 (1) The order shall be limited to only that information necessary
40 to achieve the objective of the warrant or wiretap order, including

1 by specifying the target individuals or accounts, the applications
2 or services, the types of information, and the time periods covered,
3 as appropriate.

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

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

12 (d) When issuing any warrant or wiretap order for electronic
13 communication information or electronic device information, a
14 court may, at its discretion, do any or all of the following:

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

19 (2) Require that any information obtained through the execution
20 of the warrant or order that is unrelated to the objective of the
21 warrant be destroyed as soon as feasible after that determination
22 is made.

23 (e) A service provider may disclose, but shall not be required
24 to disclose, electronic communication information or subscriber
25 information when that disclosure is not otherwise prohibited by
26 law.

27 (f) If a government entity receives electronic communication
28 information voluntarily provided pursuant to subdivision (e), it
29 shall delete that information within 90 days unless the entity has
30 or obtains the specific consent of the sender or recipient of the
31 electronic communications about which information was disclosed
32 or obtains a court order authorizing the retention of the information.
33 A court shall issue a retention order upon a finding that the
34 conditions justifying the initial voluntary disclosure persist, in
35 which case the court shall authorize the retention of the information
36 only for so long as those conditions persist, or there is probable
37 cause to believe that the information constitutes evidence that a
38 crime has been committed.

39 (g) If a government entity requests that a service provider
40 disclose information pursuant to an emergency under either Section

1 2702(b)(8) or 2702(c)(4) of Title 18 U.S.C., the entity shall, within
2 three days after seeking disclosure, file with the appropriate court
3 a motion seeking approval of the requested emergency disclosures
4 that shall set forth the facts giving rise to the emergency. The court
5 shall promptly rule on the motion and shall order the immediate
6 destruction of all information received in response to the request
7 upon a finding that the facts did not give rise to an emergency
8 under either Section 2702(b)(8) or 2702(c)(4) of Title 18 U.S.C.

9 1546.2. (a) Except as otherwise provided in this section, any
10 government entity that executes a warrant or wiretap order or issues
11 an emergency request pursuant to Section 1546.1 shall
12 contemporaneously serve upon, or deliver by registered or
13 first-class mail, electronic mail, or other means reasonably
14 calculated to be effective, the identified targets of the warrant,
15 order, or emergency request, a notice that informs the recipient
16 that information about the recipient has been compelled or
17 requested, and states with reasonable specificity the nature of the
18 government investigation under which the information is sought.
19 The notice shall include a copy of the warrant or order, or a written
20 statement setting forth facts giving rise to the emergency.

21 (b) If there is no identified target of a warrant, wiretap order,
22 or emergency request at the time of its issuance, the government
23 entity shall take reasonable steps to provide the notice, within three
24 days of the execution of the warrant, to all individuals about whom
25 information was disclosed.

26 (c) (1) When a wiretap order or search warrant is sought under
27 Section 1546.1, the government entity may include in the
28 application a request supported by a sworn affidavit for an order
29 delaying notification and prohibiting the party on whom the warrant
30 or order is served from notifying the subject of the warrant or
31 order. The court shall grant the request if the court determines that
32 there is reason to believe that notification of the existence of the
33 warrant may have an adverse result, but only for the period of time
34 that the court finds there is reason to believe that the warrant
35 notification may have that adverse result, and not to exceed 90
36 days.

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

39 (3) Upon expiration of the period of delay of the warrant
40 notification, the government entity shall serve upon, or deliver by

1 registered or first-class mail, electronic mail, or other means
2 reasonably calculated to be effective as specified by the court
3 issuing the warrant, each individual whose electronic
4 communication information was acquired, a document that includes
5 the information described in subdivision (a), a copy of all
6 information disclosed or a summary of that information, including,
7 at a minimum, the number and types of records disclosed, the date
8 and time when the earliest and latest records were created, and a
9 statement of the grounds for the court's determination to grant a
10 delay in notifying the individual.

11 (4) Except as otherwise provided in this section, nothing in this
12 chapter shall prohibit or limit a service provider or any other party
13 from disclosing information about any request or demand for
14 electronic communication information or electronic device
15 information.

16 1546.4. (a) Except as proof of a violation of this chapter, no
17 evidence obtained or retained in violation of this chapter shall be
18 admissible in a criminal, civil or administrative proceeding, or
19 used in an affidavit in an effort to obtain a search warrant or court
20 order.

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

24 (c) If a warrant or wiretap order does not comply with this
25 chapter, a service provider, any other recipient of the warrant or
26 wiretap order, or any individual whose information is targeted by
27 the warrant or wiretap order, may petition the issuing court to void
28 or modify the warrant or wiretap order or to order the destruction
29 of any information obtained in violation of this chapter.

30 1546.6. A government entity that obtains electronic
31 communication information pursuant to this chapter shall make
32 an annual report to the Attorney General. The report shall be made
33 on or before February 1, 2017, and each February 1 thereafter. To
34 the extent it can be reasonably determined, the report shall include
35 all of the following:

36 (a) The number of requests or demands for electronic
37 communication information.

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

40 (1) Electronic communication content.

- 1 (2) Location information.
2 (3) Electronic device information.
3 (4) Other electronic communication information.
4 (c) For each of the types of records listed in subdivision (b), all
5 of the following:
6 (1) The number of requests or demands that were each of the
7 following:
8 (A) Wiretap orders obtained pursuant to this chapter.
9 (B) Search warrants obtained pursuant to this chapter.
10 (C) Emergency requests pursuant to subdivision (g) of Section
11 1546.1.
12 (2) The total number of users whose information was requested
13 or demanded.
14 (3) The total number of requests or demands that did not specify
15 a target individual.
16 (4) The number of requests or demands complied with in full,
17 partially complied with, or refused.
18 (5) The number of times the notice to the affected party was
19 delayed and the average length of the delay.
20 (6) The number of times records were shared with other
21 government entities or any department or agency of the federal
22 government, and the agencies with which the records were shared.
23 (7) For contents of electronic communications, the total number
24 of communications contents received.
25 (8) For location information, the average period for which
26 location information was obtained or received and the total number
27 of location records received.
28 (9) For other electronic communication information, the types
29 of records requested and the total number of records of each type
30 received.
31 1546.8. (a) On or before April 1, 2017, and each April 1
32 thereafter, the Department of Justice shall publish on its Internet
33 Web site both of the following:
34 (1) The individual reports from each government entity that
35 requests or compels the production of contents or records pertaining
36 to an electronic communication or location information.
37 (2) A summary aggregating each of the items in subdivisions
38 (a) to (c), inclusive of Section 1546.6.

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

4 SEC. 2. If the Commission on State Mandates determines that
5 this act contains costs mandated by the state, reimbursement to
6 local agencies and school districts for those costs shall be made
7 pursuant to Part 7 (commencing with Section 17500) of Division
8 4 of Title 2 of the Government Code.

O