

AMENDED IN SENATE AUGUST 19, 2016

AMENDED IN SENATE AUGUST 1, 2016

AMENDED IN ASSEMBLY MAY 23, 2016

AMENDED IN ASSEMBLY APRIL 5, 2016

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 1924

**Introduced by Assembly Member Low
(Principal coauthor: Assembly Member Bigelow)**

February 11, 2016

An act to amend Sections 638.52 and 1546.1 of, and to add Sections 638.54 and 638.55 to, the Penal Code, relating to privacy, and declaring the urgency thereof, to take effect immediately.

LEGISLATIVE COUNSEL'S DIGEST

AB 1924, as amended, Low. ~~Pen registers: trap and trace devices: orders.~~ *Privacy: electronic communications.*

(1) Existing law generally makes it a crime to install or use a pen register or trap and trace device without court approval. Existing law allows a peace officer to make an application to a magistrate for an order authorizing or approving the installation and use of a pen register or trap and trace device and requires a provider of wire or electronic communication service, landlord, custodian, or other person, upon presentation of an order, to provide the peace officer with all information, facilities, and technical assistance necessary to accomplish the installation, as specified, if the assistance is directed by the order. Under existing law, an order or extension order authorizing or approving the installation and use of a pen register or a trap and trace device is

required to direct that the order be sealed until otherwise ordered by the magistrate who issued the order, or a judge of the superior court, and that the person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber or to any other person, except as specified.

This bill would instead require an order or extension order authorizing or approving the installation and use of a pen register or a trap and trace device direct that the order be sealed until the order, including any extensions, expires, and would require that the order or extension direct that the person owning or leasing the line to which the pen register or trap and trace device is attached not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber or to any other person. The bill would require a government entity that obtains information pursuant to an order for a pen register or trap and trace device to notify the identified targets of the order within 30 days after the termination of the period of the order that information about the recipient has been compelled or requested. The bill would allow a court to order a delay of this notification if it finds that there is reason to believe notification may have an adverse result, as defined, and to grant extensions of the delay, as provided. The bill would require the requesting peace officer's law enforcement agency to compensate a provider of a wire or electronic communication service, landlord, custodian, or other person who provides facilities or technical assistance pursuant to these provisions for the reasonable expenses incurred in providing the facilities and assistance.

(2) Existing law authorizes a government entity to compel the production of, or access to, electronic communication from a service provider or access to electronic device information only pursuant to a warrant, wiretap order, order for electronic reader records, or subpoena.

This bill would additionally authorize a government entity to compel production of the above communications and information pursuant to an order for a pen register or trap and trace device.

(3) Existing law authorizes a government entity to access electronic device information by means of physical interaction or electronic communication with the device only in specified circumstances, including, among others, pursuant to a warrant or wiretap order, or with the specific consent of the authorized possessor of the device.

This bill would additionally authorize a government entity to access electronic device information by means of physical interaction or electronic communication with the device pursuant to an order for a pen register or trap and trace device.

(4) The California Constitution provides for the Right to Truth in Evidence, which requires a $\frac{2}{3}$ vote of the Legislature to enact a statute that would exclude any relevant evidence from any criminal proceeding, as specified.

This bill would authorize any person in a trial, hearing, or proceeding to move to suppress wire or electronic information obtained or retained in violation of the 4th Amendment to the United States Constitution or of the pen register and trap and trace device provisions described above, as specified, and would authorize the Attorney General to commence a civil action to compel any government entity to comply with those provisions. The bill would also authorize an individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with those provisions, the California Constitution, or the United States 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 those provisions, the California Constitution, or the United States Constitution. Because this bill would authorize the exclusion of relevant evidence obtained or retained in violation of those pen register and trap and trace device provisions in a criminal proceeding, it requires a $\frac{2}{3}$ vote of the Legislature.

(5) *This bill would provide that the prohibition against a government entity 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 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.*

(6) *The bill would incorporate changes to Section 1546.1 of the Penal Code proposed by both this bill and SB 1121, which would become operative only if both bills are enacted and become effective on or before January 1, 2017, and this bill is enacted after SB 1121.*

(5)

(7) This bill would declare that it is to take effect immediately as an urgency statute.

Vote: 2/3. Appropriation: no. Fiscal committee: yes.

State-mandated local program: no.

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

1 SECTION 1. Section 638.52 of the Penal Code is amended to
2 read:

3 638.52. (a) A peace officer may make an application to a
4 magistrate for an order or an extension of an order authorizing or
5 approving the installation and use of a pen register or a trap and
6 trace device. The application shall be in writing under oath or
7 equivalent affirmation, and shall include the identity of the peace
8 officer making the application and the identity of the law
9 enforcement agency conducting the investigation. The applicant
10 shall certify that the information likely to be obtained is relevant
11 to an ongoing criminal investigation and shall include a statement
12 of the offense to which the information likely to be obtained by
13 the pen register or trap and trace device relates.

14 (b) The magistrate shall enter an ex parte order authorizing the
15 installation and use of a pen register or a trap and trace device if
16 he or she finds that the information likely to be obtained by the
17 installation and use of a pen register or a trap and trace device is
18 relevant to an ongoing investigation and that there is probable
19 cause to believe that the pen register or trap and trace device will
20 lead to any of the following:

- 21 (1) Recovery of stolen or embezzled property.
- 22 (2) Property or things used as the means of committing a felony.
- 23 (3) Property or things in the possession of a person with the
24 intent to use them as a means of committing a public offense, or
25 in the possession of another to whom he or she may have delivered
26 them for the purpose of concealing them or preventing them from
27 being discovered.
- 28 (4) Evidence that tends to show a felony has been committed,
29 or tends to show that a particular person has committed or is
30 committing a felony.
- 31 (5) Evidence that tends to show that sexual exploitation of a
32 child, in violation of Section 311.3, or possession of matter

1 depicting sexual conduct of a person under 18 years of age, in
2 violation of Section 311.11, has occurred or is occurring.

3 (6) The location of a person who is unlawfully restrained or
4 reasonably believed to be a witness in a criminal investigation or
5 for whose arrest there is probable cause.

6 (7) Evidence that tends to show a violation of Section 3700.5
7 of the Labor Code, or tends to show that a particular person has
8 violated Section 3700.5 of the Labor Code.

9 (8) Evidence that does any of the following:

10 (A) Tends to show that a felony, a misdemeanor violation of
11 the Fish and Game Code, or a misdemeanor violation of the Public
12 Resources Code, has been committed or is being committed.

13 (B) Tends to show that a particular person has committed or is
14 committing a felony, a misdemeanor violation of the Fish and
15 Game Code, or a misdemeanor violation of the Public Resources
16 Code.

17 (C) Will assist in locating an individual who has committed or
18 is committing a felony, a misdemeanor violation of the Fish and
19 Game Code, or a misdemeanor violation of the Public Resources
20 Code.

21 (c) Information acquired solely pursuant to the authority for a
22 pen register or a trap and trace device shall not include any
23 information that may disclose the physical location of the
24 subscriber, except to the extent that the location may be determined
25 from the telephone number. Upon the request of the person seeking
26 the pen register or trap and trace device, the magistrate may seal
27 portions of the application pursuant to *People v. Hobbs* (1994) 7
28 Cal.4th 948, and Sections 1040, 1041, and 1042 of the Evidence
29 Code.

30 (d) An order issued pursuant to subdivision (b) shall specify all
31 of the following:

32 (1) The identity, if known, of the person to whom is leased or
33 in whose name is listed the telephone line to which the pen register
34 or trap and trace device is to be attached.

35 (2) The identity, if known, of the person who is the subject of
36 the criminal investigation.

37 (3) The number and, if known, physical location of the telephone
38 line to which the pen register or trap and trace device is to be
39 attached and, in the case of a trap and trace device, the geographic
40 limits of the trap and trace order.

1 (4) A statement of the offense to which the information likely
2 to be obtained by the pen register or trap and trace device relates.

3 (5) The order shall direct, if the applicant has requested, the
4 furnishing of information, facilities, and technical assistance
5 necessary to accomplish the installation of the pen register or trap
6 and trace device.

7 (e) An order issued under this section shall authorize the
8 installation and use of a pen register or a trap and trace device for
9 a period not to exceed 60 days.

10 (f) Extensions of the original order may be granted upon a new
11 application for an order under subdivisions (a) and (b) if the officer
12 shows that there is a continued probable cause that the information
13 or items sought under this subdivision are likely to be obtained
14 under the extension. The period of an extension shall not exceed
15 60 days.

16 (g) An order or extension order authorizing or approving the
17 installation and use of a pen register or a trap and trace device shall
18 direct that the order be sealed until the order, including any
19 extensions, expires, and that the person owning or leasing the line
20 to which the pen register or trap and trace device is attached not
21 disclose the existence of the pen register or trap and trace device
22 or the existence of the investigation to the listed subscriber or to
23 any other person.

24 (h) Upon the presentation of an order, entered under subdivisions
25 (b) or (f), by a peace officer authorized to install and use a pen
26 register, a provider of wire or electronic communication service,
27 landlord, custodian, or other person shall immediately provide the
28 peace officer all information, facilities, and technical assistance
29 necessary to accomplish the installation of the pen register
30 unobtrusively and with a minimum of interference with the services
31 provided to the party with respect to whom the installation and
32 use is to take place, if the assistance is directed by the order.

33 (i) Upon the request of a peace officer authorized to receive the
34 results of a trap and trace device, a provider of a wire or electronic
35 communication service, landlord, custodian, or other person shall
36 immediately install the device on the appropriate line and provide
37 the peace officer all information, facilities, and technical assistance,
38 including installation and operation of the device unobtrusively
39 and with a minimum of interference with the services provided to

1 the party with respect to whom the installation and use is to take
2 place, if the installation and assistance is directed by the order.

3 (j) A provider of a wire or electronic communication service,
4 landlord, custodian, or other person who provides facilities or
5 technical assistance pursuant to this section shall be reasonably
6 compensated by the requesting peace officer's law enforcement
7 agency for the reasonable expenses incurred in providing the
8 facilities and assistance.

9 (k) Unless otherwise ordered by the magistrate, the results of
10 the pen register or trap and trace device shall be provided to the
11 peace officer at reasonable intervals during regular business hours
12 for the duration of the order.

13 (l) The magistrate, before issuing the order pursuant to
14 subdivision (b), may examine on oath the person seeking the pen
15 register or the trap and trace device, and any witnesses the person
16 may produce, and shall take his or her affidavit or their affidavits
17 in writing, and cause the affidavit or affidavits to be subscribed
18 by the parties making them.

19 SEC. 2. Section 638.54 is added to the Penal Code, to read:

20 638.54. (a) Except as otherwise provided in this section, a
21 government entity that obtains information pursuant to Section
22 638.52, or obtains information pursuant to oral authorization
23 pursuant to Section 638.53, shall serve upon, or deliver to by
24 registered or first-class mail, electronic mail, or other means
25 reasonably calculated to be effective, the identified targets of the
26 order a notice that informs the recipient that information about the
27 recipient has been compelled or requested and states with
28 reasonable specificity the nature of the government investigation
29 under which the information is sought. The notice shall include a
30 copy of the order or a written statement setting forth facts giving
31 rise to the emergency. The notice shall be provided no later than
32 30 days after the termination of the period of the order, any
33 extensions, or an emergency request.

34 (b) (1) Prior to the expiration of the 30-day period specified in
35 subdivision (a), the government entity may submit a request,
36 supported by a sworn affidavit, for an order delaying unsealing of
37 the order and notification and prohibiting the person owning or
38 leasing the line to which the pen register or trap and trace device
39 is attached from disclosing the existence of the pen register or trap
40 and trace device or the existence of the investigation to the listed

1 subscriber or any other person. The court shall issue the order if
2 the court determines that there is reason to believe that notification
3 may have an adverse result, but only for the period of time that
4 the court finds there is reason to believe that the notification may
5 have that adverse result, and not to exceed 90 days.

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

8 (3) Upon expiration of the period of delay of the notification,
9 the government entity shall serve upon, or deliver to by registered
10 or first-class mail, electronic mail, or other means reasonably
11 calculated to be effective as specified by the court issuing the order
12 authorizing delayed notification, the identified targets of the order
13 or emergency authorization a document that includes the
14 information described in subdivision (a) and a copy of all electronic
15 information obtained or a summary of that information, including,
16 at a minimum, the number and types of records disclosed, the date
17 and time when the earliest and latest records were created, and a
18 statement of the grounds for the court's determination to grant a
19 delay in notifying the individual. The notice shall be provided no
20 later than three days after the expiration of the period of delay of
21 the notification.

22 (c) If there is no identified target of an order or emergency
23 request at the time of its issuance, the government entity shall
24 submit to the Department of Justice, no later than three days after
25 the termination of the period of the order, any extensions, or an
26 emergency request, all of the information required in subdivision
27 (a). If an order delaying notice is obtained pursuant to subdivision
28 (b), the government entity shall submit to the department, no later
29 than three days after the expiration of the period of delay of the
30 notification, all of the information required in paragraph (3) of
31 subdivision (b). The department shall publish all those reports on
32 its Internet Web site within 90 days of receipt. The department
33 may redact names or other personal identifying information from
34 the reports.

35 (d) For the purposes of this section, "adverse result" has the
36 meaning set forth in subdivision (a) of Section 1546.

37 SEC. 3. Section 638.55 is added to the Penal Code, immediately
38 following Section 638.54, to read:

39 638.55. (a) Any person in a trial, hearing, or proceeding may
40 move to suppress wire or electronic information obtained or

1 retained in violation of the Fourth Amendment to the United States
2 Constitution or of this chapter. The motion shall be made,
3 determined, and be subject to review in accordance with the
4 procedures set forth in subdivisions (b) to (q), inclusive, of Section
5 1538.5.

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

9 (c) An individual whose information is targeted by a warrant,
10 order, or other legal process that is not in compliance with this
11 chapter, the California Constitution, or the United States
12 Constitution, or a service provider or any other recipient of the
13 warrant, order, or other legal process may petition the issuing court
14 to void or modify the warrant, order, or process, or to order the
15 destruction of any information obtained in violation of this chapter,
16 the California Constitution, or the United States Constitution.

17 SEC. 4. Section 1546.1 of the Penal Code is amended to read:

18 1546.1. (a) Except as provided in this section, a government
19 entity shall not do any of the following:

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

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

25 (3) Access electronic device information by means of physical
26 interaction or electronic communication with the electronic device.
27 This section does not prohibit the intended recipient of an electronic
28 communication from voluntarily disclosing electronic
29 communication information concerning that communication to a
30 government entity.

31 (b) A government entity may compel the production of or access
32 to electronic communication information from a service provider,
33 or compel the production of or access to electronic device
34 information from any person or entity other than the authorized
35 possessor of the device only under the following circumstances:

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

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

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

3 (4) Pursuant to a subpoena issued pursuant to existing state law,
4 provided that the information is not sought for the purpose of
5 investigating or prosecuting a criminal offense, and compelling
6 the production of or access to the information via the subpoena is
7 not otherwise prohibited by state or federal law. Nothing in this
8 paragraph shall be construed to expand any authority under state
9 law to compel the production of or access to electronic information.

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

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

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

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

20 (3) With the specific consent of the authorized possessor of the
21 device.

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

24 (5) If the government entity, in good faith, believes that an
25 emergency involving danger of death or serious physical injury to
26 any person requires access to the electronic device information.

27 (6) If the government entity, in good faith, believes the device
28 to be lost, stolen, or abandoned, provided that the entity shall only
29 access electronic device information in order to attempt to identify,
30 verify, or contact the owner or authorized possessor of the device.

31 (7) Except where prohibited by state or federal law, if the device
32 is seized from an inmate's possession or found in an area of a
33 correctional facility under the jurisdiction of the Department of
34 Corrections and Rehabilitation where inmates have access and the
35 device is not in the possession of an individual and the device is
36 not known or believed to be the possession of an authorized visitor.
37 ~~Nothing in this paragraph shall~~ *This paragraph shall not be*
38 construed to supersede or override Section 4576.

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

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

6 (1) The warrant shall describe with particularity the information
7 to be seized by specifying the time periods covered and, as
8 appropriate and reasonable, the target individuals or accounts, the
9 applications or services covered, and the types of information
10 sought.

11 (2) The warrant shall require that any information obtained
12 through the execution of the warrant that is unrelated to the
13 objective of the warrant shall be sealed and not subject to further
14 review, use, or disclosure without a court order. A court shall issue
15 such an order upon a finding that there is probable cause to believe
16 that the information is relevant to an active investigation, or review,
17 use, or disclosure is required by state or federal law.

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

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

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

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

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

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

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

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

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

22 (h) If a government entity obtains electronic information
23 pursuant to an emergency involving danger of death or serious
24 physical injury to a person, that requires access to the electronic
25 information without delay, the entity shall, within three days after
26 obtaining the electronic information, file with the appropriate court
27 an application for a warrant or order authorizing obtaining the
28 electronic information or a motion seeking approval of the
29 emergency disclosures that shall set forth the facts giving rise to
30 the emergency, and if applicable, a request supported by a sworn
31 affidavit for an order delaying notification under paragraph (1) of
32 subdivision (b) of Section 1546.2. The court shall promptly rule
33 on the application or motion and shall order the immediate
34 destruction of all information obtained, and immediate notification
35 pursuant to subdivision (a) of Section 1546.2 if such notice has
36 not already been given, upon a finding that the facts did not give
37 rise to an emergency or upon rejecting the warrant or order
38 application on any other ground.

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

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

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

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

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

20 *SEC. 4.5. Section 1546.1 of the Penal Code is amended to
21 read:*

22 1546.1. (a) Except as provided in this section, a government
23 entity shall not do any of the following:

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

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

29 (3) Access electronic device information by means of physical
30 interaction or electronic communication with the electronic device.
31 This section does not prohibit the intended recipient of an electronic
32 communication from voluntarily disclosing electronic
33 communication information concerning that communication to a
34 government entity.

35 (b) A government entity may compel the production of or access
36 to electronic communication information from a service provider,
37 or compel the production of or access to electronic device
38 information from any person or entity other than the authorized
39 possessor of the device only under the following circumstances:

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

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

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

7 (4) Pursuant to a subpoena issued pursuant to existing state law,
8 provided that the information is not sought for the purpose of
9 investigating or prosecuting a criminal offense, and compelling
10 the production of or access to the information via the subpoena is
11 not otherwise prohibited by state or federal law. Nothing in this
12 paragraph shall be construed to expand any authority under state
13 law to compel the production of or access to electronic information.

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

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

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

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

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

27 ~~(3)~~

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

30 ~~(4)~~

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

33 ~~(5)~~

34 (6) If the government entity, in good faith, believes that an
35 emergency involving danger of death or serious physical injury to
36 any person requires access to the electronic device information.

37 ~~(6)~~

38 (7) If the government entity, in good faith, believes the device
39 to be lost, stolen, or abandoned, provided that the *government*
40 entity shall only access electronic device information in order to

1 attempt to identify, verify, or contact the owner or authorized
2 possessor of the device.

3 (7)

4 (8) Except where prohibited by state or federal law, if the device
5 is seized from an inmate's possession or found in an area of a
6 correctional facility ~~under the jurisdiction of the Department of~~
7 ~~Corrections and Rehabilitation~~ *or a secure area of a local detention*
8 *facility* where inmates have ~~access and~~ *access*, the device is not in
9 the possession of an ~~individual~~ *individual*, and the device is not
10 known or believed to be the possession of an authorized visitor.
11 ~~Nothing in this~~ *This* paragraph shall *not* be construed to supersede
12 or override Section 4576.

13 (9) *Except where prohibited by state or federal law, if the device*
14 *is seized from an authorized possessor of the device who is serving*
15 *a term of parole under the supervision of the Department of*
16 *Corrections and Rehabilitation or a term of postrelease community*
17 *supervision under the supervision of county probation.*

18 (10) *Except where prohibited by state or federal law, if the*
19 *device is seized from an authorized possessor of the device who*
20 *is subject to an electronic device search as a clear and*
21 *unambiguous condition of probation, mandatory supervision, or*
22 *pretrial release.*

23 (11) *If the government entity accesses information concerning*
24 *the location or the telephone number of the electronic device in*
25 *order to respond to an emergency 911 call from that device.*

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

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

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

1 (2) The warrant shall require that any information obtained
2 through the execution of the warrant that is unrelated to the
3 objective of the warrant shall be sealed and ~~not shall not be~~ subject
4 to further review, use, or disclosure ~~without a court order.~~ *except*
5 *pursuant to a court order or to comply with discovery as required*
6 *by Sections 1054.1 and 1054.7.* A court shall issue such an order
7 upon a finding that there is probable cause to believe that the
8 information is relevant to an active investigation, or review, use,
9 or disclosure is required by state or federal law.

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

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

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

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

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

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

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

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

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

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

21 (h) If a government entity obtains electronic information
22 pursuant to an emergency involving danger of death or serious
23 physical injury to a person, that requires access to the electronic
24 information without delay, the *government* entity shall, within
25 three *court* days after obtaining the electronic information, file
26 with the appropriate court an application for a warrant or order
27 authorizing obtaining the electronic information or a motion
28 seeking approval of the emergency disclosures that shall set forth
29 the facts giving rise to the emergency, and if applicable, a request
30 supported by a sworn affidavit for an order delaying notification
31 under paragraph (1) of subdivision (b) of Section 1546.2. The court
32 shall promptly rule on the application or motion and shall order
33 the immediate destruction of all information obtained, and
34 immediate notification pursuant to subdivision (a) of Section
35 1546.2 if ~~such~~ *that* notice has not already been given, upon a
36 finding that the facts did not give rise to an emergency or upon
37 rejecting the warrant or order application on any other ground.
38 *This subdivision does not apply if the government entity obtains*
39 *information concerning the location or the telephone number of*

1 *the electronic device in order to respond to an emergency 911 call*
2 *from that device.*

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

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

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

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

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

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

26 *SEC. 5. Section 4.5 of this bill incorporates amendments to*
27 *Section 1546.1 of the Penal Code proposed by both this bill and*
28 *Senate Bill 1121. It shall only become operative if (1) both bills*
29 *are enacted and become effective on or before January 1, 2017,*
30 *but this bill becomes operative first, (2) each bill amends Section*
31 *1546.1 of the Penal Code, and (3) this bill is enacted after Senate*
32 *Bill 1121, in which case Section 1546.1 of the Penal Code, as*
33 *amended by Section 4 of this bill, shall remain operative only until*
34 *the operative date of Senate Bill 1121, at which time Section 4.5*
35 *of this bill shall become operative.*

36 ~~SEC. 5.~~

37 *SEC. 6. This act is an urgency statute necessary for the*
38 *immediate preservation of the public peace, health, or safety within*
39 *the meaning of Article IV of the Constitution and shall go into*
40 *immediate effect. The facts constituting the necessity are:*

1 In order for government entities to more effectively utilize pen
2 registers and trap and trace devices when engaging in vital law
3 enforcement activities, it is necessary for this bill to take immediate
4 effect.

O