(0178

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

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" is any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, location, or time of the sender or recipients at any point during the communication, 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" is 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) "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.

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

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 Specific consent may be withdrawn at any time.

(k) "Subscriber information" means the name, street address, phone number, email address, or similar contact information provided by the subscriber to the provider of an electronic communication service for the purpose of establishing a communication

channel between that subscriber and that provider, 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 device, except with the specific consent of the authorized possessor of the device.

(b) A government entity may compel the production of or access to electronic communication information or electronic device information, or access electronic device information by means of physical interaction or electronic communication with the device, subject to subdivision (c) 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) Any warrant or wiretap order for electronic communication information or electronic device information shall comply with the following:

(1) The 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 order shall identify the effective date upon which the warrant 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 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.

(d) When issuing any warrant or wiretap order for electronic communication information or electronic device information, 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.

(e) 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 law.

(f) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (e), 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.

(g) If a government entity requests that a service provider disclose information pursuant to an emergency under either Section 2702(b)(8) or 2702(c)(4) of Title 18 U.S.C., the entity shall, within three days after seeking disclosure, file with the appropriate court a motion seeking approval of the requested 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 received in response to the request upon a finding that the facts did not give rise to an emergency under either Section 2702(b)(8) or 2702(c)(4) of Title 18 U.S.C.

1546.2. (a) Except as otherwise provided in this section, any government entity that executes a warrant or wiretap order or issues an emergency request 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 at the time of its issuance, the government entity shall take reasonable steps to provide the notice, within three days of the execution of the warrant, to all individuals about whom information was disclosed.

(c) (1) When a wiretap order or search warrant is sought under Section 1546.1, the government entity may include in the application a request supported by a sworn affidavit for an order delaying notification and prohibiting the party on whom the warrant or order is served from notifying the subject of the warrant or order. The court shall grant the request if the court determines that there is reason to believe that notification of the existence of the warrant may have an adverse result, but only for the period of time that the court finds there is reason to believe that the warrant 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 warrant 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 warrant, each individual whose electronic communication information was acquired, a document that includes the information described in subdivision (a), a copy of all information disclosed 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.

(4) 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 communication information or electronic device 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) If a warrant or wiretap order does not comply with this chapter, a service provider, any other recipient of the warrant or wiretap order, or any individual whose information is targeted by the warrant or wiretap order, may petition the issuing court to void or modify the warrant or wiretap order or to order the destruction of any information obtained in violation of this chapter.

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

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

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

(1) Electronic communication content.

(2) Location information.

(3) Electronic device information.

(4) Other electronic communication information.

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

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

(A) Wiretap orders obtained pursuant to this chapter.

(B) Search warrants obtained pursuant to this chapter.

(C) Emergency requests pursuant to subdivision (g) of Section 1546.1.

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

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

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

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

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

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

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

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

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

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

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

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

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