Study G-300 February 10, 2015

Second Supplement to Memorandum 2015-3

State and Local Agency Access to Customer Information from Communication Service Providers: General Statutory Objectives

On February 9, 2015, Senators Leno and Anderson introduced Senate Bill 178. That bill would enact the California Electronic Communications Privacy Act ("Cal-ECPA"). Cal-ECPA would require a warrant or wiretap order whenever state or local agencies access any type of electronic communication information (including content, metadata, and location tracking information). A copy of the bill is attached.

The content of SB 178 would substantially overlap with the matters that the Commission is currently studying. The bill's effect would largely be in accord with the main conclusions drawn by the staff, as to the existing requirements of constitutional and statutory law.[1]

This overlap puts the Commission in a somewhat difficult position, for two reasons:

(1) The Commission is prohibited from taking any position on pending legislation on topics that it has been authorized to study.[2] If the Commission continues to work on the matters that overlap with SB 178, it will need to be very careful to remain strictly neutral as to the merits of that bill.

(2) The Commission was about to begin the process of drafting proposed legislation. To the extent that the proposed legislation covers the same ground as SB 178, it could be a waste of the Commission's resources. If SB 178 is enacted, much of the drafting work would become redundant.

The staff sees three ways that the Commission could address the situation.

1. See Memorandum 2015-3.

2. Gov't Code § 8288 ("No employee of the commission and no member appointed by the Governor shall, with respect to any proposed legislation concerning matters assigned to the commission for study pursuant to Section 8293, advocate the passage or defeat of the legislation by the Legislature or the approval or veto of the legislation by the Governor or appear before any committee of the Legislature as to such matters unless requested to do so by the committee or its chairperson. In no event shall an employee or member of the commission appointed by the Governor advocate the passage or defeat of any legislation or the approval or veto of any legislation by the Governor, in his or her official capacity as an employee or member.").

Proceed as Planned

The Commission could simply continue its work on the electronic surveillance study while taking pains to make clear that its work product should not be construed as a judgment on the merits of SB 178.

The Commission has taken this approach in the past, when active studies overlapped with pending legislation. It can be done, but it is somewhat risky. First, it could waste resources by duplicating the efforts of the Legislature. Second, supporters or opponents of SB 178 could use the Commission's preliminary materials in the legislative process, creating a misimpression that the Commission has taken a final position on the issues.

Proceed with a General Report, but Suspend Work on Legislative Drafting

The Commission has largely completed its review of the background law and may be in a position to draw some general conclusions on the level of legal process that is currently required by constitutional and statutory law. It could (1) prepare a tentative report on its findings, (2) circulate that tentative report for comment, and then (3) finalize the report *without* drafting statutory language to implement its general conclusions.

This would allow the Commission to make productive use of the work that it has done to date, without creating a risk that further work would be rendered redundant by action on SB 178. If SB 178 is enacted, the Commission could then assess whether it would be appropriate to do any further work on this study. If SB 178 is not enacted, the Commission could proceed to draft statutory language implementing its general conclusions.

This approach should minimize the possibility that the Commission's position would be misconstrued. The finalization of a formal report would ensure that the Commission is saying exactly what it means to say and is doing so using its conventional method — a recommendation that has been formally approved for submission to the Legislature and Governor.

Suspend Work on Electronic Surveillance Entirely

If the Commission is concerned about any possible duplication of legislative effort or misunderstanding of the Commission's position of neutrality, it could suspend all work on the study of electronic surveillance. This would be the surest way to avoid the problems described above, but it would come at a cost. The Legislature and Governor would be denied the benefit of the Commission's

work in this study, at a time when it might have considerable value. Because the Legislature specifically directed the Commission to undertake this study, that drawback warrants careful consideration.

Effect of Work Suspension

If the Commission were to suspend part or all of its work on electronic surveillance issues, it would still have productive work to do on matters assigned by SCR 54 (Padilla) (2013). In addition to assigning the Commission work relating to electronic surveillance, that resolution also required the Commission to examine the law on government interruption of communication services. The Commission was planning to turn to that topic once work on surveillance had been completed. It could do so sooner, if need be.

Next Step

Because a decision on the issues discussed above will immediately affect the Commission's work, including its consideration of Memorandum 2015-3 and its First Supplement, the staff recommends that this issue be resolved before turning to the issues presented in those memoranda.

How would the Commission like to proceed?

Respectfully submitted,

Brian Hebert
Executive Director

SENATE BILL No. 178

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:

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.

O