**CPOA Fact Sheet**

# SB 178 (Leno)-Electronic Communications: Search Warrants

**Background:** CPOA worked with other associations to educate Senator Leno and other authors on the impacts of this bill, but with strong support from ACLU and other advocacy groups (and bipartisan support in the Legislature), this bill was signed by Governor Brown.

## Highlights

This bill creates the California Electronic Communications Privacy Act (CalECPA), which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.

- Prohibits law enforcement from:
    - Compelling the production of or access to electronic communication information from a service provider.
    - Compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
    - Accessing electronic device information by means of physical interaction or electronic communication with the device, although voluntary disclosure to a government entity is permitted.
- Permits a government entity to access electronic device information by means of physical interaction or electronic communication with the device only as follows
    - Pursuant to a warrant;
    - Pursuant to a wiretap order;
    - With the specific consent of the authorized possessor of the device;
    - With the specific consent of the owner of the device, only when the device has been reported as lost or stolen;
    - If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information;
    - If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device; and
    - If the device is seized from an inmate's possession or found in an area of a correctional facility where inmates have access and the device is not in the possession of an individual and the device is not known or believed to be the possession of an authorized visitor, except as otherwise provided by state or federal law.

- Requires any warrant for electronic information to comply with the following:
    - The warrant shall describe with particularity the information to be seized, including by specifying the time periods covered, and as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought;
    - The warrant shall require that any obtained information unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure unless a court issues an order that there is probable cause to believe that the information is relevant to an active investigation, or is otherwise required by state or federal law; and
    - The warrant or 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. Warrants directed to a service provider must be accompanied by an order to verify the authenticity of the electronic information produced, as specified.

- When issuing any warrant for electronic information, or upon the petition from the target or recipient of the warrant, a court may, at its discretion, do any or all of the following:
    - Appoint a special master, who is charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.
    - 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 termination of current or related investigations.

- Authorizes a service provider to voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

- Requires a government entity that receives electronic communication information voluntarily provided by a service provider to destroy that information within 90 days unless the entity has or obtains the specific consent of the sender or recipient, obtains a court order, or the information is retained for the investigation of child pornography and related crimes, as specified.

- Requires a government entity that obtains electronic information pursuant to an emergency to seek an authorizing warrant or order, or an approval motion, within three days after obtaining the electronic information, from the appropriate court, as specified.

- Declares that these provisions do not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do either of the following:
    - Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication;
    - Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic

communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity; or,

- Require a service provider to provide subscriber information.

- Requires a government entity that executes a warrant or obtains electronic information in an emergency pursuant to these provisions to serve or deliver a notice, as specified, to the identified targets stating that information about the target has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought, including a copy of the warrant, or a written statement setting forth facts giving rise to the emergency.

- Authorizes the government entity, when a search warrant is sought or electronic information obtained under emergency circumstances, to submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. Further requires the court to issue the order if the court determines that there is reason to believe that notification may have an adverse result, not to exceed 90 days, and the court may grant extensions of the delay of up to 90 days each, as specified.

- Requires, upon expiration of the period of delay of the notification, the government entity to serve or deliver to the identified targets of the warrant a document that includes the information required in 10 above, as well as a copy of all electronic information obtained or a summary of that information, and a statement of the grounds for the court's determination to grant a delay in notifying the target, as specified.

- Provides that if there is no identified target of a warrant or emergency request at the time of issuance, the government entity shall submit to the DOJ within three days of the execution of the warrant or issuance of the request all of the information required in 10 above. If an order delaying notice is obtained, the government entity shall submit to DOJ upon the expiration of the period of delay of the notification the information required in 12 above. DOJ shall publish those reports on its web site within 90 days of receipt, and may redact names or other personal identifying information from the reports.

- Declares that nothing in these provisions shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information, except as provided.

- Permits any person in a trial, hearing, or proceeding to move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter, as specified.

- Authorizes the Attorney General to commence a civil action to compel any government entity to comply with these provisions.

- Authorizes an individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with these provisions, or 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 this chapter, the California Constitution, or the United States Constitution.

- Declares that a California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to these provisions.

## Fiscal Impacts (as reported by CA Dept. of Finance)

Ongoing annual General Fund costs to [DOJ] of approximately $300,000 to research and provide notices to identified targets; unknown, though likely substantial, ongoing annual General Fund costs to [DOJ] for researching and completing reports for investigations with no identified targets, and posting local agency reports to its website.

Unknown ongoing annual costs for local law enforcement agencies for providing notices and producing investigation reports for [DOJ] publication. Though this bill is not keyed a local mandate, there could be substantial state mandated reimbursement of local costs.