SENATE COMMITTEE ON PUBLIC SAFETY

Senator Aisha Wahab, Chair
2023 - 2024 Regular

Bill No:	AB 522	**Hearing Date:**	July 11, 2023
Author:	Kalra		
Version:	February 7, 2023		
Urgency:	No	**Fiscal:**	Yes
Consultant:	SC		

Subject: ***State departments: investigations and hearings: administrative subpoenas***

HISTORY

Source: California Law Review Commission

Prior Legislation: SB 178 (Leno), Ch. 651, Stats. 2015
SCR 54 (Padilla) Ch. 115, Stats. 2013

Support: Unknown

Opposition: None known

Assembly Floor Vote: 80 - 0

PURPOSE

The purpose of this bill is to establish procedures that the state must follow to administratively subpoena a person's electronic communication information.

Existing law the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of, or access to, electronic communication information without a warrant, wiretap order, an order for electronic reader records, a subpoena, or an order for a pen register or trap and trace device. CalECPA also provides the target whose information is sought the ability to void or modify the warrant or order. (Pen. Code §§ 1546-1546.5.)

Existing law defines a "search warrant" as a written order in the name of the people, signed by a magistrate and directed to a peace officer, commanding them to search for a person or persons, a thing or things, or personal property, and in the case of a thing or things or personal property, bring the same before the magistrate. (Pen. Code, § 1523.)

Existing law provides the specific grounds upon which a search warrant may be issued, including 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. (Pen. Code, § 1524.)

Existing law provides that a search warrant cannot be issued but 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. (Pen. Code, § 1525.)

Existing law requires a magistrate to issue a search warrant if they are satisfied of the existence of the grounds of the application, or that there is probable cause to believe their existence. (Pen. Code, § 1528, subd. (a).)

Existing law requires a provider of electronic communication services or remote computing services to disclose to a governmental prosecuting or investigating agency the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of that service, and the types of services the subscriber or customer utilized, when the governmental entity is granted a search warrant. (Pen. Code, § 1524.3, subd. (a).)

Existing law states that a governmental entity receiving subscriber records or information is not required to provide notice of the warrant to a subscriber or customer. (Pen. Code, § 1524.3, subd. (b).)

Existing law authorizes a court issuing a search warrant, on a motion made promptly by the service provider, to quash or modify the warrant if the information or records requested are unusually voluminous in nature, or if compliance with the warrant otherwise would cause an undue burden on the provider. (Pen. Code, § 1524.3, subd. (c).)

Existing law requires a provider of wire or electronic communication services or a remote computing service, upon the request of a peace officer, to take all necessary steps to preserve records and other evidence in its possession pending the issuance of a search warrant or a request in writing and an affidavit declaring an intent to file a warrant to the provider. Records shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the peace officer. (Pen. Code, § 1524.3, subd. (d).)

Existing law specifies that no cause of action shall be brought against any provider, its officers, employees, or agents for providing information, facilities, or assistance in good faith compliance with a search warrant. (Pen. Code, § 1524.3, subd. (e).)

Existing law provides for a process for a search warrant for records that are in the actual or constructive possession of a foreign corporation that provides electronic communication services or remote computing services to the general public, where the records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent or from those customers, or the content of those communications. (Pen. Code, § 1524.2.)

Existing law provides that it is the state's policy to divide the work of executing and administering its laws into departments. (Gov. Code § 11150.)

Existing law empowers state department heads to issue subpoenas for the attendance of witnesses and the production of papers, books, accounts, documents, any writing (as that term is defined under the Evidence Code), tangible things, and testimony pertinent or material to any inquiry, investigation, hearing, proceeding, or action conducted in any part of the state. (Gov. Code § 11181, subd. (e).)

Existing law requires, pursuant to the California Right to Financial Privacy Act, that when a financial institution is served with an administrative subpoena requesting the customer's records,

the customer be given adequate notice and an opportunity to bring a motion to quash the subpoena. (Gov. Code § 7474.)

Existing law requires a consumer, as defined, whose personal records are being subpoenaed from a third party to be given notice and an opportunity to object to the production of their records. (Code Civ. Proc. § 1985.3, subd. (b).)

Existing law authorizes designated persons who are commanded by a subpoena to produce books, documents, or other items to bring a motion in court to quash or modify the subpoena. (Code Civ. Proc. § 1987.1.)

This bill establishes procedures that the state must follow to administratively subpoena a person's electronic communication information.

This bill defines "customer" to mean "a person or entity that receives an electronic communication service from a service provider."

This bill conforms its definitions for "electronic communication service," "electronic communication information" and "service provider" with existing definitions in CalECPA.

This bill provides that an administrative subpoena may be used to obtain a customer's electronic communication information from a service provider only if all of the following conditions are satisfied:

- The department has properly served the customer with notice of the administrative subpoena, following specified procedures;
- A copy of the administrative subpoena is attached to the notice;
- The administrative subpoena includes the name of the department that issued it and the statutory purpose for which the electronic communication information is to be obtained; and,
- The notice includes a statement in substantially the following form: "The attached subpoena was served on a communication service provider to obtain your electronic communication information. The service provider has made a copy of the information specified in the subpoena. Unless you (1) move to quash or modify the subpoena within 10 days of service of this notice, and (2) notify the service provider that you have done so, the service provider will disclose the information pursuant to the subpoena."
- The department has served a proof of service on the service provider stating its compliance with the above requirements.

This bill states that unless the customer has notified the service provider that a motion to quash or modify the subpoena has been filed, the service provider shall produce the electronic communication information specified in the subpoena no sooner than 10 days after the department served the proof of service as required.

This bill specifies that if a customer files a motion to quash or modify an administrative subpoena for electronic communication information, the proceeding shall be afforded priority on

the court calendar, and the matter shall be heard within 10 days from the filing of the motion to quash or modify.

This bill states that this section does not require a service provider to inquire whether, or to determine that, the department has complied with the requirements of this bill if the documents served on the service provider facially show compliance.

This bill states that a service provider is not precluded from notifying a customer of the receipt of an administrative subpoena.

This bill requires a service provider shall maintain, for a period of five years, a record of any disclosure of its customers' electronic communication information and shall include a copy of the administrative subpoena.

This bill states that upon customer request and the payment of the reasonable cost of reproduction and delivery, a service provider shall provide to the customer any part of the record maintained that relates to the customer.

This bill provides that if an administrative subpoena is served on a service provider, the service provider shall promptly make a copy of any electronic communication information that is within the scope of the subpoena and within the possession of the service provider at the time that the subpoena was served and preserve the copy only until it is disclosed pursuant to the subpoena or the subpoena is quashed or modified.

COMMENTS

1. Need for This Bill

According to the author of this bill:

> As a member of the California Law Revision Commission, consumer protection has continued to be a priority for me to protect vulnerable people. AB 522 would provide greater protection to consumers when the government subpoenas their electronic records via a communications company. Although consumers are in their right to exercise the Fourth Amendment, administrative subpoenas do not grant the consumer adequate time to seek judicial review of the reasonableness of the search before any records are produced. By extending these protections already applied to financial institutions, AB 522 will further protect consumers' constitutional rights before the state intrudes on their privacy.

2. The California Electronic Communications Privacy Act (CalECPA)

In 2015, the Legislature enacted CalECPA (SB 178 (Leno), Chapter 651 , Statutes of 2015), a comprehensive digital privacy law which took effect on January 1, 2016 (§ 1546 et seq.).

> [CalECPA] requires all California state and local law enforcement agencies to obtain a search warrant or wiretap order before they can access any electronic communication information. The law defines 'electronic communication information' in the broadest terms possible so that it includes emails, digital documents, text messages, location information, and any digital information

> stored in the cloud. The law protects all aspects of electronic communication information, not just its contents, but also metadata information relating to the sender, recipient, format, time, date, and location of the communications, including IP addresses.
>
> CalECPA also limits the ability of California law enforcement to obtain information directly from a smartphone or similar device, or to track them. Law enforcement must either obtain a warrant or get the consent of the person possessing the electronic device.

(Daniels, *California Updates Privacy Rights with the Electronic Communications Privacy Act* (Nov. 17, 2015) JDSupra.

The act defines "electronic device information" as any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device. "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. "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.

This bill cross references CalECPA's definitions for "electronic communication service," "electronic communication information" and "service provider" in its provisions.

3. California Law Review Commission Report

Ten years ago, the Legislature enacted Senate Concurrent Resolution 54 (Padilla, Chap. 115, Stats. 2013) (SCR 54), which directed the Commission to recommend to the Legislature how best to "revise statutes governing access by state and local government agencies to customer information from communications service providers" so that these statutes met specified requirements, including safeguarding customers' constitutional rights, accommodating mobile and Internet-based technologies, and enabling state and local government agencies to protect public safety.

Two years later, many of SCR 54's requirements were met when the Legislature enacted SB 178 (Leno, Chap. 651, Stats. 2015), CalECPA, which established a legal framework governing how state and local law enforcement agencies could lawfully obtain nearly every form of electronic communications and related data, whether stored in a physical device belonging to a person or in equipment owned or operated by a service provider. Information covered by CalECPA ranges from records of whom a person has spoken to on the phone; to the content of text messages, emails, and voicemails; to metadata such as a person's location when answering their phone. At its core, CalECPA requires law enforcement agencies to have a search warrant in order to obtain such information. CalECPA also requires that the target of the warrant be given adequate notice (in emergency circumstances, notice can be provided after the fact) and authorizes that person to petition to void or modify the warrant, as well as to move to suppress evidence obtained in violation of the law's requirements.

The California Law Revision Commission issued a report last year making recommendations to address the one issue that was not resolved by CalECPA, specifically the need for notice to a customer when an administrative subpoena is served on a communication service provider to obtain the customer's information. (*State and Local Agency Access to Electronic Communications: Notice of Administrative Subpoena* (Mar. 2022) CLRC, http://www.clrc.ca.gov/pub/Printed-Reports/Pub244-G300.pdf [as of June 29, 2023]. This bill adopts the California Law Revision Commission's recommendations to provide adequate notice and an opportunity to challenge the subpoena in court before the customer's records are produced.

4. Constitutional Requirements for a Valid Administrative Subpoena

The United States Supreme Court has recognized the lawfulness of administrative subpoenas. (*See v. Seattle* (1967) 387 U.S. 541, 544-545.) But people and entities whose records are sought via an administrative subpoena are nevertheless protected by the Fourth Amendment's prohibition against unreasonable searches and seizures. The California Supreme Court has interpreted the Fourth Amendment as requiring that "the inquiry [in an administrative subpoena] be one which the agency demanding production is authorized to make, that the demand be not too indefinite, and that the information sought be reasonably relevant." (*Brovelli v. Superior Court* (1961) 56 Cal.2d 524, 529.)

Moreover, according to the U.S. Supreme Court, "while the demand to inspect may be issued by the agency, in the form of an administrative subpoena, it may not be made and enforced by the inspector in the field, and the subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply." (*See*, *supra*, 387 U.S. at p. 544-545.)

In other words, to meet constitutional standards, an administrative subpoena must make an inquiry for records (i) that the state agency is authorized to make, (ii) that is sufficiently definite, and (iii) that is reasonably relevant to the purposes for which the inquiry is made. The person whose records are being subpoenaed must also have an opportunity to seek judicial review of the administrative subpoena.

This latter requirement can be met by ensuring that the person whose records are being sought has sufficient notice of the subpoena and the ability to move a court to quash (i.e., invalidate) or modify the subpoena, as provided for by this bill.

5. Argument in Support

According to the California Law Review Commission, the sponsor of this bill:

> Assembly Bill 522 would implement a recommendation of the California Law Revision Commission (available at http://clrc.ca.gov/pub/Printed-Reports/Pub244-G300.pdf).
>
> The proposed law would require that a customer of a communication service provider be given notice when a state agency seeks to obtain the customer's electronic communication information, by serving an administrative subpoena on the service provider. This requirement provides a meaningful opportunity for the

customer to object to the search in court, before records are provided to the agency.

As the Commission's recommendation explains, service of the administrative subpoena on the service provider without notice to the customer would likely violate the customer's Fourth Amendment right against unreasonable search and seizure.

Such a requirement already exists in other areas of the law. For example:

• Under the California Right to Financial Privacy Act a customer must be given notice when a financial institution is served with an administrative subpoena requesting the customer's records (see Gov't Code § 7474).

• In pretrial discovery, a "consumer" must be given notice when a subpoena is used to obtain the personal records of the "consumer" from a wide range of third parties who hold such records (see Code Civ. Proc. § 1985.3(b))

-- END –