SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

AB 522 (Kalra)
Version: February 7, 2023
Hearing Date: June 27, 2023
Fiscal: Yes
Urgency: No
CK

SUBJECT

State departments: investigations and hearings: administrative subpoenas

DIGEST

This bill requires administrative subpoenas seeking to obtain a customer's electronic communication information from a service provider to meet certain conditions, including that notice and a right to object be provided to the customer.

EXECUTIVE SUMMARY

A subpoena is a writ or order directed to a person and requiring the person's attendance at a particular time and place to testify as a witness. It may also require a witness to bring any books, documents, electronically stored information, or other things under the witness's control which the witness is bound by law to produce in evidence. The heads of state departments are authorized to issue subpoenas in connection with investigations and the prosecution of actions within their jurisdiction.

The California Electronic Communications Privacy Act (CalECPA) generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information, as defined, from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions. Concerns have arisen that the protections afforded by CalECPA do not sufficiently protect electronic communication information when sought by an administrative subpoena that is served on a service provider.

This author-sponsored bill requires such administrative subpoenas to also be served on the customer whose electronic communication information is being sought, providing them a right to move to quash or modify the subpoena. It is based on a recommendation by the California Law Revision Commission. There is no known

support or opposition. If this bill passes this Committee, it will be referred to the Senate Public Safety Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information, as defined, from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. CalECPA also generally specifies the only conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, consent of the owner of the device, or emergency situations, as specified. (Pen. Code § 1546 et seq.)

2) Defines "electronic communication information," for purposes of CalECPA, to mean 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. (Pen. Code § 1546.)

3) Provides that the process by which the attendance of a witness is required is the subpoena. It is a writ or order directed to a person and requiring the person's attendance at a particular time and place to testify as a witness. It may also require a witness to bring any books, documents, electronically stored information, or other things under the witness's control which the witness is bound by law to produce in evidence. (Code Civ. Proc. § 1985.)

4) Authorizes state department heads to issue subpoenas for the attendance of witnesses and the production of papers, books, accounts, documents, any writing, tangible things, and testimony pertinent or material to any inquiry, investigation, hearing, proceeding, or action conducted in any part of the state, in connection with any authorized investigation or action, as provided. (Gov. Code § 11181.)

5) Establishes the California Law Revision Commission (CLRC). (Gov. Code § 8280.) Directs the CLRC to study any topic that the Legislature, by concurrent resolution or statute, refers to it for study. (Gov. Code § 8293(a).)

This bill:

1) Provides that, in addition to any other requirements that govern the use of an administrative subpoena, 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:
    a) The department has served notice of the administrative subpoena on the customer, as specified.
    b) A copy of the administrative subpoena is attached to the notice.
    c) 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.
    d) The notice includes a statement in substantially the following form:
        i. "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."
    e) The department has served a proof of service on the service provider stating its compliance with the above.

2) Requires the service provider to produce the electronic communication information specified in the subpoena, as provided, unless the customer has notified the service provider that a motion to quash or modify the subpoena has been filed.

3) Requires the relevant proceeding to be afforded priority if a customer files a motion to quash or modify an administrative subpoena issued pursuant hereto. The matter shall be heard within 10 days from the filing of the motion to quash or modify.

4) Provides that a service provider is not required to inquire whether, or to determine that, the department has complied with these requirements if the documents served on the service provider facially show compliance. However, the service provider is not precluded from notifying a customer of the receipt of the administrative subpoena.

5) Requires a service provider to maintain, for a period of five years, a record of any disclosure of its customers' electronic communication information pursuant hereto, including a copy of the administrative subpoena.

6) Requires a service provider to provide to the customer any part of the record maintained pursuant hereto that relates to the customer, upon customer request and the payment of the reasonable cost of reproduction and delivery.

7) Provides that if an administrative subpoena is served on a service provider pursuant hereto, 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. The copy shall be preserved only until it is disclosed pursuant to the subpoena or the subpoena is quashed or modified.

8) Defines "electronic communication information" and "service provider" with cross-references to CalECPA.

COMMENTS

1. The California Electronic Communications Privacy Act (CalECPA)

In 2015, the Legislature enacted CalECPA to protect Californians from intrusive government searches in the digital era.[1] Senator Mark Leno, the author of the bill, argued that "clear warrant standards for government access to electronic information" needed to be instituted in order "to properly safeguard the robust constitutional privacy and free speech rights of Californians." He stated the case:

> SB 178 updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information. Each of these categories can reveal sensitive information about a Californian's personal life: her friends and associates, her physical and mental health, her religious and political beliefs, and more. The California Supreme Court has long held that this type of information constitutes a "virtual current biography" that merits constitutional protection. SB 178 would codify that protection into statute.[2]

[1] SB 178 (Leno, Ch. 651, Stats. 2015), Pen. Code § 1546 et seq.
[2] Senate Public Safety Committee (2015) *Committee Analysis of SB 178*.

CalECPA prohibits a government entity from the following:

- 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; or
- accessing electronic device information by means of physical interaction or electronic communication with the electronic device.

(Pen. Code § 1546.1.) CalECPA provides an exclusive list of exceptions to these prohibitions, including the issuance of a valid warrant or wiretap order. A government entity may access electronic device information by means of physical interaction or electronic communication with the device under certain circumstances, including with the specific consent of the authorized possessor of the device or the owner of the device, when the device has been reported as lost or stolen. It can also be accessed if the entity has a good faith belief that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

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.

2. <u>The limitations of CalECPA in protecting electronic communication information</u>

Although CalECPA applies broadly to "government entities," it generally restricts access via subpoena only when connected to criminal investigations. It authorizes a government entity to compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device under certain circumstances, including:

> Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law.

(Pen. Code § 1546.1(b).)

Existing law authorizes state department heads to investigate and prosecute actions concerning all matters relating to the business activities and subjects under the jurisdiction of the department, violations of any law or rule or order of the department, and such other matters as may be provided by law. (Gov. Code § 11180.) In connection with such investigations or actions, these departments are authorized to carry out certain acts, including issuing subpoenas for the attendance of witnesses and the production of papers, books, accounts, documents, writings, 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.)

Therefore, CalECPA does not adequately apply its due process protections when these administrative subpoenas are issued by government entities.

3. Filling the gap in protections

This bill is sponsored by the California Law Revision Commission. CLRC was initially tasked with studying and reporting on the constitutional concerns in connection with government access to electronic communication information. Many of the opportunities for reform were accomplished by the passage of CalECPA; however, CLRC believes that there is one specific area that was not resolved by CalECPA, the need for notice to a customer when an administrative subpoena is served on a service provider seeking to obtain the customer's electronic communication information.

The issue stems from the fact that when a customer's electronic communication information is sought by a government entity through service of an administrative subpoena on a service provider, the customer receives no notice and does not have an opportunity to object or assert its rights.

The CLRC explains the issue in a report[3] issued last year, entitled *State and Local Agency Access to Electronic Communications: Notice of Administrative Subpoena*:

> A warrant supported by probable cause is not the only constitutionally sufficient authority to conduct a search that is governed by the Fourth Amendment of the United States Constitution and Section 13 of Article I of the California Constitution. In some circumstances, a search pursuant to a subpoena duces tecum, issued by a state administrative agency, can also be constitutionally reasonable.
>
> The use of an administrative subpoena to compel the production of evidence (rather than a warrant) does not violate the Fourth Amendment,

[3] *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 17, 2023].

> so long as the subpoena is authorized, sufficiently definite, and reasonable:
>
> > Insofar as the prohibition against unreasonable searches and seizures can be said to apply at all it requires only that the inquiry 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.[4]
>
> However, courts have held that a search pursuant to an administrative subpoena is constitutionally permissible only if the person whose records would be searched has notice and an opportunity to move to quash or modify the subpoena before any records are actually produced.[5]

The CLRC report goes on to explain courts' reasoning that issuance of a subpoena starts an adversarial process that ensures adequate due process is afforded. However, the CLRC reports points out that this reasoning is only sound when a subpoena is served on the person whose records will be searched:

> [T]hat will not necessarily be the case when a subpoena is served on a communication service provider for access to a customer's records. In the latter situation, the customer may not be notified of the subpoena and might have no real opportunity to object before records are produced. That would undermine or negate the above argument for the constitutionality of a search by administrative subpoena. In particular, if the customer is not separately notified of the subpoena, then only the communication service provider will have an opportunity to object to the subpoena through an adversarial judicial process. That will often be insufficient to protect the interests of the customer, because the interests of the service provider and customer are not the same. The service provider will mostly be concerned with unreasonable burdens created by the subpoena; the customer is concerned with privacy. In order to ensure that the use of an administrative subpoena to obtain customer records from a communication service provider is constitutional, the customer must be given notice and an opportunity to challenge the subpoena in court before the customer's records are produced.

Therefore, the constitutional concerns that prompted the passage of CalECPA continue to apply where administrative subpoenas seek to gain access to customer electronic

---

[4] Citing *Brovelli v. Superior Court* (1961) 56 Cal.2d 524, 529.

[5] Citing *In re Subpoena Duces Tecum* (4th Cir. 2000) 228 F.3d 341, 347-48; *People v. West Coast Shows, Inc.* (1970) 10 Cal.App.3d 462, 470 ("The Government Code provides an opportunity for adjudication of all claimed constitutional and legal rights before one is required to obey the command of a subpoena duces tecum issued for investigative purposes.").

communication information without adequate notice and process afforded the customer.

This bill addresses this issue by requiring certain conditions be satisfied before an administrative subpoena can be used to obtain a customer's electronic communication information from a service provider.[6] First, the relevant state entity must serve notice of the administrative subpoena on the customer and attach a copy of the actual subpoena. The subpoena must include certain information, including the name of the department that issued it; the statutory purpose for which the electronic communication information is to be obtained; and a statement informing the customer of their rights to this effect:

> "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 must provide proof of service to the subpoenaed service provider and the provider is not required to otherwise establish such compliance. However, the provider is authorized to notify the customer of the subpoena.

The service provider is required to turn over the information unless the customer informs it that the customer has moved to quash or modify the subpoena. If such motion is made, it shall be given priority in the court and be heard within 10 days of filing. Service providers are required to maintain records of any such disclosures and provide them to a customer upon demand, as specified.

These protections are already largely afforded in the context of accessing customers' financial records through administrative subpoenas served on financial institutions. The California Right to Financial Privacy Act (the Act) provides that an officer, employee, or agent of a state or local agency or department thereof, may obtain financial records pursuant to an administrative subpoena or summons otherwise authorized by law and served upon the financial institution only if certain conditions are met, including that a copy of the subpoena or summons be served on the customer. (Gov. Code § 7474.) Similar to this bill, the Act also requires that the subpoena include the name of the agency or department in whose name the subpoena is issued and the statutory purpose for which the information is to be obtained. The customer must then be given 10 days to move to quash the subpoena and notify the financial institution.

---

[6] The definitions used in the bill for "electronic communication information" and "service provider" cross-reference those in CalECPA.

4. Stakeholder positions

According to the author:

> 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.

SUPPORT

None known

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation: AB 561 (Chen, 2023) allows service of process and subpoenas to incarcerated individuals on the first try at a state prison or county jail if the prison or county jail is the recipient party's only reasonably known address by leaving a copy with the warden, sheriff, or jailer of that state prison or county jail. AB 561 is currently in the Assembly Public Safety Committee.

Prior Legislation:

SB 178 (Leno, Ch. 651, Stats. 2015) established CalECPA.

SCR 54 (Padilla, Ch. 115, Stats. 2013) directed the CLRC 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.

PRIOR VOTES:

Assembly Floor (Ayes 80, Noes 0)
Assembly Appropriations Committee (Ayes 15, Noes 0)
Assembly Public Safety Committee (Ayes 8, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

****