Date of Hearing: March 21, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 522 (Kalra) – As Introduced February 7, 2023

SUBJECT: State departments: investigations and hearings: administrative subpoenas

SYNOPSIS

This author-sponsored measure enacts a recommendation of the California Law Review Commission. Under current law, state agencies have the power to subpoena (that is, order the production of) documents and other information when they are conducting an investigation or an enforcement proceeding. The person whose information is being sought has the power to oppose the subpoena by moving a court to modify or quash it on the grounds that it is unlawful in some respect.

A difficulty arises if the records being sought are in the possession of a third party. While the third party ought to receive timely notice of the subpoena, that party may lack the interest or ability to assert the right to modify or quash the subpoena on behalf of the person whose information is being sought.

This deficiency is particularly glaring if the information being sought is electronic communication information, such as emails, text messages, or a person's location while making telephone calls. Such information is protected from unauthorized seizure by law enforcement under the California Electronic Privacy Act (CalECPA), but CalECPA does not address administrative subpoenas.

This bill would address this gap by enacting procedures whereby a person whose records are subject to an administrative subpoena is given both notice and an opportunity to respond. These procedures appear to satisfy constitutional due process standards while enhancing privacy protections for electronic communication information.

If passed by this Committee, this bill will next be heard by the Assembly Public Safety Committee.

SUMMARY: Establishes procedures that the state must follow to administratively subpoena a person's electronic communication information while meeting constitutional due process requirements. Specifically, **this bill**:

1) Defines the following terms:

    a) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence, whether in whole or in part, by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

    b) "Electronic communication information" means information about an electronic communication, including but not limited to, its contents, sender, recipients, or format; the location of the sender or recipients; the time or date the communication was created

or sent; or any other information pertaining to any individual or device participating in the communication. The definition includes Internet Protocol (IP) addresses.

c) "Service provider" means a person or entity that offers an electronic communication service.

d) "Customer" means a person or entity that receives an electronic communication service from a service provider

2) Sets forth the following conditions that a state department must satisfy before it can use an administrative subpoena to obtain a customer's electronic communication information from a service provider using an administrative subpoena:

a) The department must properly serve the customer with notice of the administrative subpoena, following procedures outlined in the Code of Civil Procedure.

b) A copy of the administrative subpoena must be attached to the notice.

c) The administrative subpoena must include the department's name and the statutory purpose for obtaining the electronic communication information.

d) The notice must include the following statement: "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 must serve a proof of service on the service provider that states the department has complied with 2) a) – d).

3) Requires a service provider, if the requirements above are met, to produce the electronic communication information specified in an administrative subpoena 10 days or more after being served—unless a customer notifies the service provider of having filed a motion to quash or modify the subpoena.

4) Requires a court to give priority on its calendar to any motion to quash or modify an administrative subpoena for electronic communication information, so that the motion is heard within 10 days of its filing.

5) Clarifies that a service provider need not independently inquire into, or determine that, a state department has complied with this bill's requirements if the department provides the service provider with documents showing compliance.

6) Clarifies that a service provider may notify a customer that it has received a subpoena for the customer's electronic communication information.

7) Requires service providers to maintain, for a period of five years, a record of any disclosure of a customer's electronic communication information and to provide this record to the customer upon payment of the reasonable cost of reproduction and delivery.

EXISTING LAW:

1) Establishes the California Law Revision Commission (Commission). (Gov. Code § 8280.)

2) Specifies that the duties of the Commission include:

    a) Examining the common law and statutes of the state and judicial decisions for the purpose of discovering defects and anachronisms in the law and recommending needed reforms.

    b) Recommending, from time to time, such changes in the law as it deems necessary to modify or eliminate antiquated and inequitable rules of law, and to bring the law of this state into harmony with modern conditions. (Gov. Code § 8289.)

3) Provides, pursuant to the U.S. Constitution, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." (U.S. Const., 4th Amend.)

4) Establishes 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.)

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

6) 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(e).)

7) 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.)

8) 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(b).)

9) 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.)

FISCAL EFFECT: As currently in print this bill is keyed non-fiscal.

COMMENTS:

1) **Background.** The text of this bill originates with the California Law Revision Commission (Commission). 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, and much of the need for Commission action in this area obviated, when the Legislature enacted SB 178 (Leno, Chap. 651, Stats. 2015), the California Electronic Communications Privacy Act (CalECPA). CalECPA 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.

As observed by the Commission, "[CalECPA] addressed nearly all of the legal deficiencies that the Commission had identified in its study." (49 Cal. L. Revision Comm'n Preprint Recommendation #G-300 (2022) 1 (CLRC Report), *available at* http://clrc.ca.gov/pub/Printed-Reports/RECpp-G300.pdf.) Nevertheless, the Commission added, "a few minor matters [have] not been addressed by CalECPA[.]" (*Ibid.*) This bill addresses one of these unaddressed matters: establishing procedures through which the state may administratively subpoena a customer's electronic communications information in a manner that satisfies constitutional due process requirements.

2) **Author's Statement**. The author states:

> 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.

3) **What is an administrative subpoena?** In criminal and civil court cases, it is common for parties to exercise the court's authority to subpoena—this is, order the production of—records in the possession of third parties who are not otherwise involved in the case. The purpose of issuing such a subpoena, known as a subpoena *duces tecum* ("bring with you under penalty of law"), is to obtain evidence. Take the example of injured workers who sue their employer for failing to

provide adequate protective gear. In defending itself, the employer would ordinarily use a subpoena *duces tecum* to obtain medical records from doctors who treated the workers, to learn more information about the workers' injuries. (*See, generally*, Code of Civil Procedure §§ 1985-1997.)

A subpoena *duces tecum* may also be used to obtain evidence in an administrative proceeding, i.e., an investigation or an enforcement action brought by a state agency, rather than a dispute decided in court. In this context, subpoenas *duces tecum* are commonly known as "administrative subpoenas." (Note: throughout this analysis, the term "state agency" is intended to apply to any part of the executive branch, whether an agency, department, board, committee, or commission, that possesses administrative subpoena power under statute.)

The types of proceedings in which administrative subpoenas can be used vary widely, reflecting the many issues addressed by California state agencies. For example, the California Court of Appeal recently upheld the power of the State Water Resources Control Board to subpoena financial documents in order to determine the relationship between entities being investigated for water quality violations. (*State Water Resources Control Bd. v. Baldwin* (2020) 45 Cal. App. 5th 40.) In a much older case, the California Supreme Court authorized the issuance of administrative subpoenas in disciplinary hearings before the State Board of Medical Examiners. (*Shively v. Stewart* (1966) 65 Cal. 2d 475.)

State agencies are granted general authority to issue administrative subpoenas under Government Code § 11181:

> **11181.** In connection with any investigation or action authorized by this article, the department head may do any of the following:
>
> […]
>
> (e) 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.

Specific statutes may also provide procedures for issuing administrative subpoenas for particular types of information. For example, the California Right to Financial Privacy Act, Government Code §§ 7460-7493, regulates government access to customer records held by financial institutions. A state or local agency that wishes to obtain customer records held by financial institutions, e.g., to investigate alleged fraud or elder abuse, must follow the procedures in this Act, rather than the more-general Government Code § 11181, in order to administratively subpoena such records.

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, 544-5 (White, J).) 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 544-45.)

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.

5) **Why is this bill necessary?** Among the third-party records that a state agency may seek to obtain using an administrative subpoena are records of electronic communications. As explained by the California Law Review Commission:

> [W]hen a subpoena is served on a communication service provider for access to a customer's records…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 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. (CLRC Report 3)

The issue, then, is that a person may have a legal basis to quash or modify an administrative subpoena seeking their electronic communications information, but under current law, they will not be informed of the subpoena. While their communications provider will be notified, the provider likely has no interest in resisting the subpoena and/or may be unaware of the customer's legal basis for doing so. This arguably violates the customer's due process rights. Per the California Law Review Commission:

> 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. (*Ibid.*)

In order to remedy this deficiency, this bill would establish the following process to be followed by a state agency when administratively subpoenaing electronic communications information:

1. When an administrative subpoena is served on a communication service provider to obtain customer records, the subpoenaing agency would need to serve notice on the affected customer. The notice would include a copy of the subpoena and a specified advisory statement.

2. The subpoena would require that the service provider make and retain a copy of the requested records, to prevent spoliation [i.e., destruction of records], until the subpoena operates or is quashed.

3. Proof of service of the notice to the customer would be served on the communication service provider.

4. Unless the customer first moves to quash the subpoena and notifies the service provider of that fact, the requested records must be produced 10 days after the proof of service is served on the communication service provider. (CLRC Report 4.)

Under this bill, the subpoena would have to include the department's name and the statutory purpose for obtaining the electronic communication information. The advisory statement referenced in step 1 would read:

> 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.

6) **What are the implications of this bill for due process and for privacy protections?** The process this bill establishes would appear to meet Constitutional due process standards, by giving the person whose records are being subpoenaed sufficient notice of the records being sought, so that the person has an opportunity to move a court to modify or quash the subpoena.

The ten days' notice provided for in this bill is identical to the notice period in at least two other pertinent California laws that govern subpoenas of a person's information from third parties. The first is the California Right to Financial Privacy Act, Government Code §§ 7460-7493, mentioned above, which regulates government access to customer records held by financial institutions. The Act provides customers with ten days after notice to move to quash an administrative subpoena. (Gov. Code § 7474.) The ten-day notice period was first enacted into law in 1978. (*See* Chap. 1346, Stats. 1978.)

The second law providing a similar ten-day notice period is included in the procedures governing issuance of subpoenas *duces tecum* to third parties in court proceedings. A party who serves such a subpoena in order to compel the production of records containing the personal information of a consumer must provide notice to the consumer that their records are being sought. The customer then has ten days to object to production of the records or move to quash or modify the subpoena. (Code Civ. Proc. § 1985.3.) This provision was first enacted in 1980. (*See* Chap. 976, Stats. 1980.)

The fact that the processes established by these statutes have withstood Constitutional scrutiny for over four decades strongly suggests that the ten-day notice period under this bill will be found to provide adequate due process protections.

This bill is also commendable for enhancing privacy protections for people whose electronic communication information is the subject of an administrative subpoena.

7) **Related legislation**. AB 1242 (Bauer-Kahan, Chap. 627, Stats. 2022), among other things, amended CalECPA to prohibit corporations incorporated in, or whose principal offices are located in, California from providing information in response to a warrant or other legal process if the process relates to an investigation into, or enforcement of, a law creating liability for providing, facilitating, or obtaining an abortion that is legal under California law.

AB 928 (Grayson, 2019) would have created a CalECPA exemption by allowing law enforcement to use an administrative subpoena, rather than a warrant, to obtain information regarding a subscriber suspected of engaging in the exploitation or attempted exploitation of a child. The bill failed in the Assembly Public Safety Committee.

SB 811 (Public Safety, Chap. 269, Stats. 2017) created an exception to CalECPA's notice requirements if a government entity accesses information concerning the location or the telephone number of an electronic device in order to respond to an emergency 911 call from that device.

AB 165 (Cooper, 2017) would have created a CalECPA exemption by allowing local educational agencies to access information from electronic devices belonging to students enrolled in kindergarten through 12th grade. The bill failed in this Committee.

SB 1121 (Leno, Chap. 541, Stats. 2016) made a number of minor amendments to CalECPA in order to address unintended consequences and outstanding stakeholder concerns.

SB 178 (Leno, Chap. 651, Stats. 2015) enacted CalECPA.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200