Date of Hearing: April 25, 2023
Counsel: Andrew Ironside

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Reginald Byron Jones-Sawyer, Sr., Chair

AB 522 (Kalra) – As Introduced February 7, 2023

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

1) Establishes the following conditions that a state department must satisfy before it can 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 specified procedures;

    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"; and,

    e) The department must serve a proof of service on the service provider that states that the department has complied with the above conditions.

2) Requires the service provider to produce the electronic communication information specified in an administrative subpoena 10 days or more after being served, unless the customer has notified the service provider that a motion to quash or modify the subpoena has been filed.

3) Requires a court, if a customer files a motion to quash or modify an administrative subpoena, to give the motion priority on its calendar and to hear the matter within 10 days of the filing of the motion.

4) Provides that a service provider need not inquire into, or determine that, a state department has complied with these requirements if the department provides the service provider with documents showing compliance.

5) Provides that a service provider may notify a customer that it has received an administrative subpoena for the customer's electronic communication information.

6) 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.

7) Defines "customer" as a person or entity that receives an electronic communication service from a service provider.

8) Defines "electronic communication" as 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.

9) Defines "electronic communication information" as 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, including Internet Protocol (IP) addresses.

10) Defines "service provider" as a person or entity that offers an electronic communication service.

**EXISTING FEDERAL LAW**:Provides 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.)

**EXISTING STATE LAW:**

1) Provides that the right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized. (Cal. Const., art. I, § 13.)

2) Provides that all people are by nature free and independent and have inalienable rights, including privacy. (Cal. Const., Art. I, § 1.)

3) 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.)

4) 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.)

5) 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.)

6) 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.)

7) 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).)

8) 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).)

9) 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).)

10) 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).)

11) 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).)

12) 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).)

13) 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.)

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

15) 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).)

16) 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.)

17) 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).)

18) 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**: Unknown

**COMMENTS**:

1) **Author's Statement**: 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."

2) **Background:** 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." (Cal. L. Revision Comm'n Preprint Recommendation #G-300 (June 21, 2022) p. 1 (CLRC Report), <http://clrc.ca.gov/pub/Printed-Reports/RECpp-G300.pdf> [last visited Apr. 17, 2023].) Nevertheless, the Commission added, "a few minor matters [have] not been addressed by CalECPA[.]" (*Ibid.*) This bill would address 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.

3) **Administrative Subpoenas:** 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 Civ. Proc. §§ 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."[1]

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 & Sons, Inc.* (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 section 11181:

---

[1] 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.

> 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 (CRFPA), regulates government access to customer records held by financial institutions. (See Gov. Code §§ 7460-7493.) 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 the CRFPA, rather than Government Code section 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, 544-545.) 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) **Need for the Bill:** 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, *supra*, at p. 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. (CLRC report, *supra*, at p. 3.)

In order to remedy this deficiency, this bill would require a subpoenaing agency, when an administrative subpoena is served on a communication service provider to obtain customer records, to serve notice of the subpoena on the affected customer. The notice must include a copy of the subpoena and a specified advisory statement, which states:

> 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.

This bill would require the service provider to make and retain a copy of the requested records until the subpoena operates or is quashed. It also requires that a state agency serve proof of service of the notice to the customer on the communication service provider. Moreover, unless the customer first moves to quash the subpoena and notifies the service provider of that fact, the service provider must produce the requested records no sooner than 10 days after the proof of service is served on it.

6) **Implications for Due Process and 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 10-day notice requirement 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. Gov. Code § 7474; Code Civ. Proc. § 1985.3.) The fact that the processes established by these statutes have remained in effect for over four decades suggests that the ten-day notice period under this bill will be found to provide adequate due process protections.

7) **Argument in Support**: According to the *California Law Revision Commission*, "Assembly Bill 522 (Kalra), would implement a recommendation of the California Law Revision Commission on State and Local Agency Access to Electronic Communications: Notice of Administrative Subpoena (March 2022).

   "The California Law Revision Commission has been directed to prepare proposed legislation on government access to customer records of communication service providers, in order to protect customers' constitutional rights.

   "Most of the areas for possible reform that the Commission identified were addressed by the California Electronic Communication Privacy Act ("Cal-ECPA"), which was enacted before the Commission could complete its work on this study.

   "This recommendation addresses one issue that was not resolved by Cal-ECPA, the need for notice to a customer when an administrative subpoena is served on a communication service provider to obtain the customer's information. The proposed law would require such notice."

8) **Related Legislation**: AB 793 (Bonta), would prohibit a government entity from seeking or obtaining information from a reverse-location demand or a reverse-keyword demand, and prohibits any person or government entity from complying with a reverse-location demand or a reverse-keyword demand. AB 793 is pending hearing in the Assembly Judiciary Committee.

9) **Prior Legislation**:

   a) AB 1242 (Bauer-Kahan), Chapter 627, Statutes of 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.

   b) AB 928 (Grayson), of the 2019-2020 Legislative Session, 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. AB 928 failed passage in the Assembly Public Safety Committee.

   c) SB 811 (Committee on Public Safety), Chapter 269, Statutes of 2017, createed 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.

   d) AB 165 (Cooper), of the 2017-2018 Legislative Session, 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. AB 165 failed passage in the Assembly Public Safety Committee.

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

f) SB 178 (Leno), Chap. 651, Statutes of 2015, enacted CalECPA.

**REGISTERED SUPPORT / OPPOSITION**:

**Support**

California Law Revision Commission

**Opposition**

None submitted.

**Analysis Prepared by**: Andrew Ironside / PUB. S. / (916) 319-3744