ASSEMBLY THIRD READING
AB 522 (Kalra)
As Introduced February 7, 2023
Majority vote

SUMMARY

Establishes procedures that the state must follow to administratively subpoena a person's electronic communication information while meeting constitutional due process requirements.

Major Provisions

1) Defines the following terms:

   a) "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.

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

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

2) Sets forth requirements 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, including properly serving the customer with notice of the administrative subpoena. The notice must include a copy of the subpoena, the department's name, and the statutory purpose for obtaining the electronic communication information.

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) 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.

5) 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.

COMMENTS

Background. Eight years ago, the Legislature enacted SB 178 ((Leno), Chapter 651, Statutes of 2015), the California Electronic Communications Privacy Act (CalECPA). CalECPA established a legal framework governing how state and local law enforcement agencies can 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 text of this bill originates with the California Law Revision Commission (Commission). Before the passage of CalECPA, the Commission had issued recommendations addressing how electronic communications could be lawfully obtained. But, 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.

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 Sections 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." (Throughout this document, the term "state agency" is intended to apply to any part of California's 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 Section 11181. Among the third-party records that a state agency may seek to obtain using an administrative subpoena are records of electronic communications.

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.

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. (*Brovelli v. Superior Court* (1961) 56 Cal. 2d 524, 529.) The person whose records are being subpoenaed must also have an opportunity to seek judicial review of the administrative subpoena. (*See*, *supra*, 387 U.S. at 544-45.)

What this bill would do. 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.

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 Sections 7460-7493, which regulates government access to customer records held by financial institutions. That Act provides customers with ten days after notice to move to quash an administrative subpoena. (Government Code Section 7474.) The ten-day notice period was first enacted into law in 1978. (*See* Chapter 1346, Statutes of 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. (Civil Protections Code Section 1985.3.) This provision was first enacted in 1980. (*See* Chapter 976, Statutes of 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.

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.

Arguments in Support

None on file.

Arguments in Opposition

None on file.

FISCAL COMMENTS

According to the Assembly Appropriations Committee:

1) Costs of an unknown, but significant amount, likely in the high hundreds of thousands of dollars to low millions of dollars annually, for the Department of Justice (DOJ) to perform consumer and privacy protection investigations to obtain the information necessary to satisfy the bill's proposed notice requirements. For its part, the DOJ estimates these costs to be approximately $3 million annually to fund four deputy attorney generals, four legal analysts, two investigators, five legal secretaries and $200,000 in consultant costs.

2) Collective costs of an unknown, but presumably significant amount, for state agencies to produce notice documents, notify customers of requests for records and present proof of such notice to service providers (various funds).

VOTES

ASM PRIVACY AND CONSUMER PROTECTION: 11-0-0
YES: Gabriel, Joe Patterson, Bauer-Kahan, Bennett, Essayli, Vince Fong, Irwin, Lowenthal, Papan, Wicks, Wilson

ASM PUBLIC SAFETY: 8-0-0
YES: Jones-Sawyer, Alanis, Bonta, Bryan, Lackey, Ortega, Santiago, Zbur

ASM APPROPRIATIONS: 15-0-1
YES: Holden, Megan Dahle, Bryan, Calderon, Wendy Carrillo, Dixon, Mike Fong, Hart, Lowenthal, Mathis, Papan, Pellerin, Sanchez, Weber, Ortega
ABS, ABST OR NV: Robert Rivas

UPDATED

VERSION: February 7, 2023

CONSULTANT: Jith Meganathan / P. & C.P. / (916) 319-2200 FN: 0000527