

MEMORANDUM 2025-8

Notice of Subpoena: Stakeholder Feedback **(Draft of Tentative Recommendation)**

This memorandum¹ provides an analysis of stakeholder feedback and additional proposed revisions to the draft proposed language addressing notice requirements for government-issued subpoenas in civil actions. At its October 2024 meeting the Commission considered draft proposed language and informally approved the staff's recommended approach for developing a draft tentative recommendation for approval by the Commission based on continued stakeholder outreach to discuss potential revisions to the Commission's recommendation.²

The California Department of Justice (DOJ) and the Electronic Frontier Foundation (EFF) provided letters³ to the Commission in response to the draft provided in Memorandum [2024-48](#). The staff appreciates the DOJ and EFF's participation and technical assistance in refining the draft legislation.

DEPARTMENT OF JUSTICE CONCERNS

The DOJ's comments resulted in several important amendments to the attached tentative draft. The proposed new code section now contains several subdivisions clarifying the existing authority of government entities in relation to the section, mirroring similar provisions in the California Electronic Communications Privacy Act (CalECPA).⁴ DOJ also noted and appreciated the flexibility in the methods available to serve the notice.

However, the DOJ objects to the definition of electronic communications. They note the current definition:

¹ Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

² Memorandum [2024-48](#); Minutes (October 2024), p. 5.

³ EX 01-07.

⁴ Cal. Pen. Code §§ [1546 – 1546.5](#). The attached draft legislation now contains proposed Gov't Code § 7455 (j) – (l), which mirrors Cal. Pen. Code § [1546.1](#)(i)(2), (j), and (k), respectively.

...might be read to cover an array of communications that are not private. They include advertisements displayed to the public on a digital billboard over a highway, commercials and campaign ads broadcast via radio, television, or on streaming services, banner ads, keyword advertisements, and other forms of online advertising, spam emails and robo-texts, and the like. This overbreadth is not benign, and the draft should be revised to avoid creating barriers to legitimate civil law enforcement and regulatory investigations.⁵

As noted in the prior memo,⁶ AB 522 was modeled on the California Right to Financial Privacy Act (CRFPA)⁷ and incorporates definitions from CalECPA⁸ and the federal Stored Communications Act,⁹ which the staff noted “simplifies the drafting of the proposed law, improves its readability, and would create useful uniformity between this statute and CalECPA.”¹⁰ It is unclear, however, why the definition for electronic communications should be altered in reference to civil cases. While the DOJ accurately notes privacy may not be the same level of concern for notices broadcast widely versus individual correspondence, the current ability to hyper-target online ads and emails to individuals blurs the division between mass and personal communications. Absent a more surgical definition striking a balance between these two categories, the staff recommends retaining the present definition.

DOJ also recommended limiting the draft’s scope to investigations of a customer/subscriber to prevent the language from being “a barrier to investigations where the customer/subscriber is a victim rather than the target.” The staff does not interpret a notice requirement as a barrier to investigation and found nothing in the study’s record indicating a desire to protect the privacy of only those suspected of a crime.

Lastly, DOJ requested additional procedural clarifications to align with those for subpoenas issued pursuant to Government Code Section 11180.¹¹ Informal conversations with staff negated that concern because of the draft’s subdivision (h), which expressly exempts pretrial investigative subpoenas.

DOJ’s remaining concerns relate to serving the notice requirement and are discussed further below.

⁵ EX 01-02.

⁶ Memorandum [2024-48](#), p. 2.

⁷ Memorandum [2021-32](#) and Gov’t Code §§ [7460-7493](#).

⁸ Penal Code §§ [1546-1546.5](#).

⁹ [18 U.S.C. §§ 2701 - 2710](#).

¹⁰ Memorandum [2021-38](#), p. 2.

¹¹ Gov’t Code § [11180](#) pertains to pretrial investigative subpoenas.

ELECTRONIC FRONTIER FOUNDATION CONCERNS

The EFF also provided feedback that strengthens the draft. As a result of their comments, the staff made amendments to expand the definition of “subscriber” to include a “user.” This prevents a government entity from circumventing the notice requirement by accessing electronic communications information from a source with which an individual does not have an account.¹²

EFF also noted a service provider may have independent reasons from a subscriber for contesting a subpoena, and the staff made commensurate changes.

The staff also deleted the requirement to pay additional costs to get a copy of a subscriber’s record from service provider, as such costs are likely minimal, and it is the subscriber’s own information being requested.

Finally, EFF argued convincingly to shift the obligation to provide subscriber notice back to the government entity, particularly given the more flexible means for sending notice and precedent in existing law.¹³ If, in limited circumstances, the government is unable to provide notice, the staff amended the draft to allow DOJ to petition the court to require the service provider to send notice.

However, EFF suggested a reading of current law appears more restrictive than the wider understanding of the ability of government to subpoena electronic communications in civil cases.¹⁴ To allay these concerns, the staff included a new subdivision (i) that clarifies this draft proposal does not presume to expand any authority under state law to compel the production of electronic communication information or subscriber information. EFF also suggested amendments to require the government to make a showing that preservation is required; given how easily electronic communications may be deleted (particularly following notice of investigation), the staff recommends retaining this provision absent contrary law.

The draft tentative recommendation is attached, which includes revisions to the draft language previously provided to the Commission. **The Commission needs to decide whether to approve it for release as a tentative recommendation, with or without changes.**

¹² For example, if a government entity is searching for an email from X to Y, under the prior draft, the government entity could subpoena Y’s service provider instead of X’s and avoid the notice requirement.

¹³ See e.g., Penal Code §§ [1546.2\(a\)\(1\)](#) (CalECPA), [1524.3\(d\)\(1\)](#) (requiring a government entity to provide notice when receiving subscriber records, as specified), and Gov’t Code § [7474](#) (CFRA).

¹⁴ EX 04-07. EFF believes a warrant or court order is necessary to obtain electronic communications information pursuant to the California and federal Constitution, certain federal caselaw and the federal Stored Communications Act.

Respectfully submitted,

Sarah Huchel
Chief Deputy Counsel

New Chapter 19.5 is added to Division 7 (Miscellaneous) of Title 1 the Gov't Code, titled "Governmental Access to Electronic Communication Information"

Section 7455:

(a) For purposes of this section:

~~(1) "Customer" means a person or entity that receives an electronic communication service from a service provider.~~

~~(2)~~ (1) "Electronic communication information" has the meaning provided in subdivision (d) of Section 1546 of the Penal Code. [means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.]

~~(3)~~ (2) "Electronic communication service" has the meaning provided in subdivision (e) of Section 1546 of the Penal Code.

~~(3)~~ (3) "Government entity" has the meaning provided in subdivision (i) of Section 1546 of the Penal Code.

~~(4)~~ (4) "Service provider" has the meaning provided in subdivision (j) of Section 1546 of the Penal Code.

~~(5)~~ (5) "Subscriber" means a person who has an account with a service provider or a user of a service provider.

(b) In addition to any other requirements that govern the use of an ~~administrative~~ subpoena by a government entity, ~~an administrative~~ subpoena may be used to obtain a ~~customer-subscriber's~~ electronic communication information from a service provider only if all of the following conditions are satisfied:

(1) The ~~department~~ service provider government entity has served upon, or delivered to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, notice of the ~~administrative~~ subpoena ~~on to the customer-subscriber pursuant to Chapter 4 (commencing with Section 413.10) of Title 5 of Part 2 of the Code of Civil Procedure within 5 days of receiving the government entity's subpoena.~~

(2) A copy of the ~~administrative~~ subpoena is attached to the notice.

(3) The ~~administrative~~ subpoena includes the name of the ~~department~~ government entity that issued it and the statutory purpose for which the electronic communication information is to be obtained.

(4) The notice includes contact information for the service provider and 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 was required to make ~~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."

~~(5)~~ (5) The department service provider has sent a proof of service delivery on to the service provider government entity stating its compliance with paragraphs (1) to (4), inclusive.

(c) If the ~~department~~ government entity is not able to deliver notice to the subscriber, the department may petition the court to order the service provider to provide notice on behalf of the government entity with the notice information in (b)(4).

(~~e~~d) Unless the ~~subscriber~~ customer has notified the service provider that a motion to quash or modify the subpoena has been filed, or the service provider has filed a motion to quash or modify the subpoena, the service provider shall produce the electronic communication information specified in the subpoena no sooner than 10 days after the ~~department~~ service provider government entity sent notice of the subpoena to the subscriber. ~~served the proof of service required by paragraph (5) of subdivision (b).~~

(~~d~~e) If a ~~subscriber~~ or service provider customer files a motion to quash or modify an administrative subpoena issued pursuant to subdivision (b) or (d), 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.

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

~~(f) This section does not preclude a service provider from notifying a customer of the receipt of an administrative subpoena pursuant to subdivision (b).~~

(g) (1) ~~A service provider shall maintain, for a period of five years, a record of any disclosure of its subscriber's customer's electronic communication information pursuant to this section.~~

(2) ~~The record maintained pursuant to this subdivision shall include a copy of the administrative subpoena.~~

(3) (~~f~~) Upon ~~subscriber~~ customer request and the payment of the reasonable cost of reproduction and delivery, a service provider shall provide to the ~~subscriber~~ customer any part of the record maintained pursuant to this subdivision that relates to the ~~subscriber~~ customer.

(~~h~~g) (1) If an administrative subpoena is served on a service provider pursuant to this section, 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 prior to giving notice to the subscriber.

(2) The copy made pursuant to this subdivision shall be preserved only until it is disclosed pursuant to the subpoena, ~~or the subpoena is quashed or modified, or until the subpoena is withdrawn and no other subpoena requesting the information remains pending, or until any action to enforce the subpoena, or any other subpoena requesting the information is fully resolved.~~ This subdivision does not prevent a service provider from preserving electronic communication information as otherwise provided by law.

(h) This chapter shall not apply to any subpoenas issued in connection with a pretrial investigation.

(i) Nothing in this section shall be construed to expand any authority under state law to compel the production of or access to electronic communication information or subscriber information.

(j) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication.

(k) This section does not limit the authority of the Public Utilities Commission or the State Energy Resources Conservation and Development Commission to obtain energy or water supply and consumption information pursuant to the powers granted to them under the Public Utilities Code or the Public Resources Code and other applicable state laws.

(l) This chapter shall not be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity's possession.



1300 I STREET, SUITE 125
P.O. BOX 944255
SACRAMENTO, CA 94244-2550

Telephone: (916) 210-6033
Facsimile: (916) 322-2630
E-Mail: Anthony.Lew@doj.ca.gov

December 18, 2024

Sarah Huchel, Staff Counsel
California Law Revision Commission
c/o Legislative Counsel Bureau
925 L Street, Suite 275
Sacramento, CA 95814

RE: Department of Justice Technical Advice re Staff Memorandum 2024-48
California Law Revision Commission Study G-300

Dear Ms. Huchel:

Thank you for the opportunity to provide technical advice in support of the Commission's study regarding State and Local Agency Access to Customer Information from Communication Service Providers (G-300). The following comments relate to the proposed legislative text accompanying Staff Memorandum 2024-48.

As a preliminary matter, we thank the Commission's staff for incorporating technical feedback provided by our office in the course of this study, which has broad implications for the work of law enforcement, regulatory, and other officers and agencies across California state and local government that use investigative authority provided by state or local law to obtain information. The current staff proposal, which recognizes that the government may not be aware of the identity of individuals using an email or other electronic communications account that has been involved in fraudulent or other illegal conduct, and therefore requires the communication service provider to provide notice, is a significant improvement on the prior draft.

We also recommend the following with respect to the current draft:

- We understand the desire to accord protection to private communications, such as emails or text chats. However, the draft's expansive definition of electronic communications ("the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system") might be read to cover an array of communications that are not private. They include advertisements displayed to the public on a digital billboard over a highway, commercials and campaign ads broadcast via radio, television, or on streaming

services, banner ads, keyword advertisements, and other forms of online advertising, spam emails and robo-texts, and the like. This overbreadth is not benign, and the draft should be revised to avoid creating barriers to legitimate civil law enforcement and regulatory investigations.¹

- Section 7455, subdivision (b), of the proposed bill should be revised to affirmatively require the service provider provide timely notice to the subscriber. In the absence of such a requirement, a service provider could defeat a subpoena by intentionally failing to provide notice. It seems unlikely that this was the intent of the author.
- We appreciate the draft providing the service provider with flexibility to serve notice via electronic mail or other means. This flexibility is essential to making the proposed bill workable, particularly in instances where a communication service provider, for example a company that provides free email accounts to members of the public, might have no other contact information for the subscriber.
- The draft omits categorial exclusions that the Legislature incorporated into CalECPA. For example, it omits CalECPA’s exclusion of communications that officers or employees of a business make via corporate email systems, as well as its exclusion of certain requests by utility and energy regulators. (Pen. Code, § 1546.1, subds. (i)(2), (j).). The draft should be revised to include these and other exceptions from CalECPA.
- The draft borrows from the California Right to Financial Privacy Act (CFFPA), Gov’t Code § 7460 et seq. Like the CRFPA, the draft bill should be limited to requests made in the course of investigating the customer/subscriber. (Gov’t Code, § 7470(a) (limiting the CRFPA’s requirements to requires made “in connection with a civil or criminal investigation *of a customer*.”). The draft should not be a barrier to investigations where the customer/subscriber is a victim rather than the target.
- We appreciate the draft’s exclusion of civil and administrative discovery and other “subpoenas issued in connection with a pretrial investigation.” To the extent that the draft is revised to bring investigative subpoenas issued under Section 11180 et seq. of the Government Code within its scope, the notice, duty to produce, and motion to quash procedure contemplated by the draft should be revised to align with the process for issuing and enforcing subpoenas under Section 11180. For example, these investigative subpoenas are not self-enforcing, and the draft’s proposed notice that “the service provider will disclose the information pursuant to the subpoena” and its command that service provider “shall produce the electronic communication information” absent a motion by the customer to quash are therefore inaccurate. The service provider would be under no obligation to produce the requested communications unless the government

¹ This issue of overbreadth could, as previously suggested, also be largely addressed by limiting the draft to communications by subscribers who are natural persons and not extending it to communications by corporations or other types of business entities.

brought an action to compel compliance and the court ordered the service provider to comply. The motion to quash procedure envisioned by the draft is also unworkable, as these subpoenas are issued by executive agencies, rather than by a court, and there would therefore be no action pending before the courts in which the subscriber could bring a motion to quash. As provided by existing law, any objection would instead be heard in the context of a subsequently filed action by the government to enforce compliance with the subpoena. (Gov't Code, § 11187, subd. (d)). We would welcome the opportunity to provide further technical assistance if the draft is revised to encompass these investigative subpoenas.

Thank you again for the opportunity to provide technical advice in connection with this study. Please do not hesitate to contact us if you have questions or if we can otherwise be of assistance.

Sincerely,

A handwritten signature in black ink that reads "Anthony Lew". The signature is written in a cursive, flowing style.

ANTHONY LEW
Deputy Attorney General
Office of Legislative Affairs

For ROB BONTA
Attorney General

December 6, 2024

Re: Flaws and Recommendations to Improve Proposal Regarding User Notice of Subpoenas in California

The Electronic Frontier Foundation is a nonprofit that fights to ensure that technology supports freedom, justice, and innovation for all people of the world.

EFF supports increased notice to internet users whose personal information is compelled by the government.¹ But the new proposed Government Code Section 7455² in California suffers from a number of flaws.

The proposal would require service providers to give notice to their users when the government uses a subpoena to compel providers to turn over their users' personal information, including the content of their communications. However, the government cannot use a mere subpoena to compel this information, and a warrant is typically required. This means that the proposal aims to address a scenario that does not—and should not—exist in the first place. At best, this proposal is superfluous. At worst, it confuses the government into believing that it has authority that it does not.

Below are recommendations to improve the proposal.

1. Replace the term “electronic communications information” with “subscriber information.”

Under state, federal, and constitutional law, the government cannot use a mere subpoena to compel a service provider to turn over a subscriber's electronic communications information. This proposal might confuse that point. You can eliminate some of that confusion by replacing the term “electronic communications information” with “subscriber information.”

Under CalECPA, the government generally needs a warrant to compel a service provider to produce a subscriber's electronic communications information. Penal Code

¹ <https://www.eff.org/deeplinks/2022/04/ndo-fairness-act-important-step-towards-transparency>

² It is currently titled: New Chapter 19.5 is added to Division 7 (Miscellaneous) of Title 1 the Gov't Code, titled “Governmental Access to Electronic Communication Information.” <https://clrc.ca.gov/pub/2024/MM24-48.pdf>.

1546.1(b)(1). There is a narrow subpoena exception when a government entity is both not investigating or prosecuting a criminal offense and the subpoena is “not otherwise prohibited by state or federal law.” Penal Code 1546.1(b)(4). However, federal and constitutional law prohibit it in this instance. Under the federal Stored Communications Act, government entities need a court order or warrant to compel analogous providers to produce anything other than basic subscriber information. 18 U.S.C. 2702(a); 18 U.S.C. 2703(a)-(c). The Fourth Amendment similarly requires a warrant for the content of communication from a provider. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Carpenter v. United States*, 585 U.S. 296, 318 (2018) (citing *Warshak*).³ This applies equally to the government’s civil investigations.⁴ And California’s stronger search and seizure clause requires a warrant for subscriber records from a provider, in addition to content. *People v. Chapman*, 36 Cal. 3d 98, 108 (1984).

On the other hand, CalECPA does not limit the authority of government entities to use a subpoena to require a service provider to turn over subscriber information. Penal Code 1546.1(i)(3). Though other authorities likely do.⁵ The current proposal may be useful to require user notice in instances where the government attempts to obtain subscriber information without a warrant.

2. Remove the definition of “subscriber”

The proposal’s definition of “subscriber” should be deleted, so as not to unintentionally narrow the scope of that term in CalECPA. While CalECPA does not define “subscriber,” it defines “subscriber information” to include information about “subscribers to” and “users of” a service provider. Penal Code 1546(l). The proposal’s current definition of “subscriber” does not protect “users of” a service provider who have not created an account.

3. As a proposal intended to provide subscribers with more notice, it should not create extra powers for law enforcement.

Below are recommendations to help ensure that this proposal does not give the government more power:

³ A subpoena with notice to the user is not an adequate substitute for a warrant based on probable cause, when compelling user content from a provider. *Compare Warshak* and *Carpenter*, with CLRM, Preprint Recommendation #G-300 (2022) <https://clrc.ca.gov/pub/Printed-Reports/Pub244-G300.pdf>.

⁴ <https://www.eff.org/deeplinks/2017/06/eff-sec-get-warrant>

⁵ *See People v. Chapman*, 36 Cal. 3d 98, 108 (1984). *See also* 1524.3(a) (requiring a warrant for subscriber information).

- The proposal should include a clause that explicitly states this point, similar to Penal Code 1546.1(4): “Nothing in this law shall be construed to expand any authority under state law to compel the production of or access to electronic communication information or subscriber information.”
- Government Code Section 7455(b) should be reframed in the negative: “In addition to any other requirements that restrict the use of a subpoena by a government entity, no subpoena may be used to obtain subscriber information from a service provider unless all of the following conditions are satisfied:”
- The proposal says a service provider “shall” turn over the information if the subscriber doesn’t object in 10 days. Government Code Section 7455(c). That should be removed or changed to “may.” That is because service providers themselves can object to the subpoena for their own reasons, and the proposal as written, seems to override or overlook that.

4. The government should be responsible for issuing notice, as originally written

The person responsible for issuing the subpoena—the government entity in this case—should have the obligation to provide notice to the user. Changing “service provider” back to “department” is consistent with how notice is provided in existing state and federal law. *See* Penal Code 1546.2(a)(1); 1524.3(d)(1); 18 U.S.C. 2703(b)(1)(B). The bill could also include a provision that in certain limited cases where the government does not know the identity of the subscriber and cannot provide service on its own, the government can petition the issuing court to order the service provider to provide notice on behalf of the government entity.

5. Do not require subscribers to pay money to learn more information.

It is unfair to put the burden on a subscriber to pay “reasonable costs” to obtain more information about the subpoena at issue. Government Code Section 7455(d). The original notice to a subscriber should include any available information that is needed to effectively evaluate and challenge the subpoena.

6. Require the government to make a showing that preservation is required.

The government entity responsible for issuing the subpoena should be required to apply for and make a showing that preservation is required under the particular facts of the case. *See* Government Code Section 7455(e)(1). Existing federal law currently requires the government entity to explicitly request preservation, 18 U.S.C. 2704(a)(1), and there

F. Mario Trujillo (EFF)
December 6, 2024
Page 4 of 4

is increasing recognition that preservation requirements constitute a seizure under the Fourth Amendment that limits a person's control over their information.⁶

Sincerely,

F. Mario Trujillo
Staff Attorney
Electronic Frontier Foundation
mario@eff.org

⁶ Orin Kerr, The Fourth Amendment Limits of Internet Content Preservation, 64 St. Louis Law R 753 (2021); Paul Ohm, The Fourth Amendment Right to Delete, 129 Harv. L. Rev. F. 10 (2005).