SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 957 (Pérez)
Version: March 26, 2026
Hearing Date: April 21, 2026
Fiscal: Yes
Urgency: No
AWM

SUBJECT

Privacy: social media companies: administrative subpoenas: remedies

DIGEST

This bill places requirements and restrictions on social media companies with respect to their handling of specified administrative subpoenas.

EXECUTIVE SUMMARY

Various state and federal statutes authorize agencies within their respective executive branches to issue "administrative subpoenas" to seek information within the agency's jurisdiction. Some administrative subpoenas are self-enforcing, meaning the recipient is legally obligated to comply with a served subpoena and can face sanctions for the failure to do so. Others are "non-self-enforcing," meaning they have no legal force in and of themselves; if a recipient fails to comply, the agency must go to court, defend the legality of the subpoena, and get a court order compelling the documents or testimony. Once a court order is issued, the recipient must comply or face contempt charges; but until then, they have no obligation to respond.

One such agency empowered to issue non-self-enforcing administrative subpoenas is Immigration and Customs Enforcement (ICE). While federal law grants ICE the authority to request information relating to matters governed by the Immigration and Naturalization Act (INA), reports indicate that ICE is using administrative subpoenas to track and locate persons who criticize their behavior—matter not only outside the scope of the INA, but likely a violation of those persons' First Amendment Rights.

This bill, as the author agreed to amend it in the Senate Privacy, Digital Technologies, and Consumer Protection Committee, seeks to respond to the increased utilization of these tactics by requiring social media platforms to notify an individual when the individual's personal information is being requested through non-self-enforcing administrative subpoenas issued pursuant to the INA and the Tariff Act of 1930. Social

media companies are required to provide sufficient time for the targeted individual to respond to or challenge the subpoena before the company responds. The bill authorizes companies to thereafter respond if they determine the subpoena is not invalid, as provided, but prohibit responses if the subpoena is invalid for specified reasons; if the company decides to respond after determining that a subpoena is invalid, it must notify the Attorney General and give the Attorney General time to determine whether to file an action. Enforcement is delegated to the Attorney General and right of action is provided to individuals whose information is shared in violation of these provisions. The bill does not require a social media company to violate a court order or other binding request. In addition to the amendments agreed to in the prior committee, the author has agreed to amendments to clarify the Attorney General's obligations under the bill and to ensure that any personal information obtained by the Attorney General remains confidential.

This bill is sponsored by the author and is supported by the Electronic Frontier Foundation. The Committee has not received timely opposition to this bill. The Senate Privacy, Digital Technologies, and Consumer Protection Committee passed this bill with a vote of 7-1. Should the bill pass this Committee, it will then be referred to the Senate Appropriations Committee.

PROPOSED CHANGES TO THE LAW

Existing constitutional law provides that the United States Constitution, the laws of the United States, and all treaties made under the authority of the United States are the supreme law of the land. (U.S. Const., art. VI, cl. 2.)

Existing federal law:

1) Empowers the Attorney General and any immigration officer to require by subpoena the attendance and testimony of witnesses before an immigration officer and the production of books, papers, and documents relating to the privilege of any person to enter, reenter, reside in, or pass through the United States or concerning any matter which is material and relevant to the enforcement of the Immigration and Nationality Act and the administration of the Immigration and Naturalization Service of the Department of Justice (now the U.S. Citizenship and Immigration Services (USCIS)), and to that end may invoke the aid of any court of the United States. (8 U.S.C. § 1225(d)(4)(A) ("Section 1225").)

2) Provides that any United States district court within the jurisdiction of which investigations or inquiries are being conducted by an immigration officer may, in the event of neglect or refusal to respond to a subpoena issued under 1) or refusal to testify before an immigration office, issue an order requiring such persons to appear before an immigration officer, produce books, papers, and documents if demanded

and testify, and any failure to obey such order of the court may be punished by the court as contempt thereof. (Section 1225(d)(4)(B).)

3) Establishes the Tariff Act of 1930, also known as the Smoot-Hawley Tariff. (19 U.S.C. ch. 4, §§ 1202 et seq; *see* Pub. L. 71-361 (Jun. 17, 1930) 46 Stat. 590.)

4) Pursuant to 3), authorizes the Secretary of Homeland Security or Customs and Border Patrol (CBP), in any investigation or inquiry conducted for the purpose of ascertaining the correctness of any entry, for determining the liability of any person for duty, fees and taxes due or duties, fees and taxes which may be due the United States, for determining liability for fines and penalties, or for insuring compliance with the laws of the United States administered by the CBP, to do any of the following:
    a) Examine, or cause to be examined, upon reasonable notice, any record described in the notice with reasonable specificity, which are relevant to that inquiry.
    b) Summon, upon reasonable notice, a person who imported, exported, transported, or stored merchandise subject to specified trade agreements, or filed a declaration, entry, or drawback claim with the CBP; such a person's officer or agent; any person having possession, custody, or care of records relating to such activity; or any other person, to appear before the appropriate customs office, to produce any records and give such testimony as may be relevant to the investigation or inquiry.
    c) Take, or cause to be taken, such testimony of the person concerned, under oath, as may be relevant to such investigation or inquiry. (19 U.S.C. § 1509(a).)

5) Provides that a failure to comply with a lawful demand under 4) can result in the following penalties:
    a) If the failure to comply is the result of a willful failure to maintain, store, or retrieve the demanded information, the person shall be subject to a penalty, for each release of merchandise, not to exceed $100,000, or an amount equal to 75 percent of the appraised value of the merchandise, whichever amount is less.
    b) If the failure to comply is a result of the negligence of the person in maintaining, storing, or retrieving the demanded information, such person shall be subject to a penalty, for each release of merchandise, not to exceed $100,000, or an amount of 40 percent of the appraised value of the merchandise, whichever amount is less.
    c) In addition to the penalties in (a) and (b), if the merchandise in question is related to the eligibility of merchandise for a column 1 special rate of duty under title I, the entry of such merchandise, if unliquidated, shall be liquidated at the applicable column I general rate of duty, or if unliquidated within the 2-year period preceding the date of the demand, shall be

reliquidated, notwithstanding specified time limitations. (19 U.S.C. § 1509(g).)

6) Provides that if a person summoned under 4) does not comply with the summons, the district court, upon application and a noticed hearing, shall have jurisdiction to issue an order requiring such person to comply with the summons; failure to comply may be punished by the court as contempt and the court may assess a monetary penalty, plus additional penalties relating to the right to import goods if the person remains in contempt. (19 U.S.C. § 1510.)

7) Provides that a district court will issue an order to comply with a non-self-executing administrative subpoena issued by a federal agency unless the subpoena exceeds Congress's grant of authority to the agency to investigate; the agency failed to follow procedural requirements; the evidence is irrelevant or immaterial to the investigation; or the subpoena is too indefinite or broad. (*E.g.*, *Golden Valley Elec. Ass'n* (9th Cir. 2012 689 F.3d 1108, 1113.)

Existing state law:

1) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to restrict the sale or sharing of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code, div. 3, pt. 4, tit. 1.81.5, §§ 1798.100 et seq.)

2) Provides a consumer the right, at any time, to request that a business delete any personal information about the consumer which the business has collected from the consumer, except as specified. Businesses must disclose this right to consumers. (Civ. Code, § 1798.105.)

3) Defines "personal information" within the CCPA as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household; the CCPA provides a nonexclusive series of categories of information deemed to be personal information, including identifiers, biometric information, and geolocation data. (Civ. Code, § 1798.140(v).)

4) Defines and provides, within the CCPA, additional protections for sensitive personal information, as defined, that reveals specified personal information about consumers, including immigration status. (Civ. Code, § 1798.140(ae).)

This bill, as the author has agreed to amend it:

1) Establishes the Stopping Harmful Information Exploitation and Lawless Data Sharing (SHIELD) Act.

2) Defines the following terms:
    a) "Administrative subpoena" means a subpoena issued pursuant to either (1) Section 1225, or (2) subparagraph (a) of paragraph (1) of subsection (a) of Title 19 of the United States Code.
    b) "Individual" means a person who is a California resident.
    c) "Maintain" includes maintain, acquire, use, or disclose.
    d) "Personal information" means any information that is maintained by a social media company that is reasonably capable of identifying or describing an individual, including, but not limited to, the individual's name, social security number, physical description, address, telephone number, IP address, online browsing history, location information, social media information, education, financial matters, and medical or employment history.
    e) "Social media company" has the same meaning as in Business and Professions Code section 22675.

3) Requires a social media company to promptly notify an individual whose personal information is requested by an administrative subpoena.

4) Requires a social media company, prior to disclosure of information in response to an administrative subpoena requesting the personal information of an individual, to provide the individual whose personal information is requested with at least 30 days to respond to or to challenge the administrative subpoena.

5) Requires a social media company that discloses personal information in response to an administrative subpoena to provide notice to the individual whose information was disclosed of all of the following:
    a) The reason the individual's information was disclosed.
    b) The basis for determining the administrative subpoena was valid.
    c) A description of the information that was disclosed.

6) Requires a social media company, notwithstanding any other law, prior to disclosing personal information in response to an administrative subpoena requesting the personal information of an individual, to determine if the administrative subpoena is invalid for any of the following reasons:
    a) The information requested is not related to any purpose lawfully authorized by Section 1225.
    b) The information is irrelevant to the purpose described in 6)(a).
    c) The information requested by the subpoena is overly broad or compliance would be unduly burdensome.

7) Requires a social media company that knows or reasonably should know, after conducting the analysis in 6) that an administrative subpoena is invalid, to notify the

Attorney General before disclosing personal information in response to the administrative subpoena.

8) Provides that a social company may disclose information in response to an administrative subpoena requesting the personal information of an individual without notifying the Attorney General if the social media company determines the administrative subpoena is not invalid as described in 6).

9) Provides that a social media company shall not respond to an administrative subpoena while a legal challenge to the subpoena is pending, or if the Attorney General requests a delay pending review of the administrative subpoena.

10) Permits the Attorney General or a person whose information has been shared in response to an administrative subpoena by a social media company in violation of the SHIELD Act may bring a civil action against the social media company for injunctive or declaratory relief.

11) Provides that nothing in the SHIELD Act shall be construed to prohibit a social media company from responding to an order issued by a court pursuant to Section 1225, as it read on January 1, 2026, or any other law.

COMMENTS

1. Author's comment

According to the author:

> Californians have the right to know when the federal government seeks access their personal information. Secret data seizures undermine trust, chill free expression and expose vulnerable communities to harm. We must protect people's privacy and their right to free speech.
>
> At a time of increased immigration enforcement across the country, many communities are living in fear. In response, people have increasingly turned to social media to stay informed and help keep one another safe. These platforms are used to track and crowdsource alerts about enforcement actions, as well as to share opinions, organize protests, and expose the behavior of ICE.
>
> As these online networks have become vital tools for community protection and public accountability, they have also drawn increased scrutiny from the federal government. Administrative subpoenas are increasingly being used recently to obtain information about individuals who operate accounts that post about or criticize ICE. In some cases, social media companies have disclosed sensitive user information without providing prior notice that a subpoena was issued.

People should be able to use social media to stay informed and keep one another safe without worrying that their activity could result in retaliation from the federal government. No one in this state should be intimidated into silence out of fear that their personal information will be secretly shared with federal authorities.

SB 957 would ensure that users are notified when their information is requested and given an opportunity to challenge or respond to the request before it is disclosed. Californians deserve transparency. The SHIELD Act provides a fair and necessary safeguard to ensure that individuals have a real chance to defend their rights in the face of federal overreach.

2. Federalism: the lines between state and federal power

The United States "Constitution established a system of 'dual sovereignty.' "[1] The Constitution's Supremacy Clause provides that the Constitution and federal laws are the supreme law of the land.[2] Section 8 of Article I of the United States Constitution enumerates Congress's specific powers,[3] and the Tenth Amendment states that "powers not delegated to the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[4] "This separation of the two spheres is one of the Constitution's structural protections of liberty…a healthy balance of power between the States and the Federal Government will reduce the risk of tyranny and abuse from either front."[5]

The interplay between Congress's enumerated powers and the states' retained powers makes the question of whether a state law conflicts with, and is therefore preempted by, a federal law a complex one. A state law will be deemed preempted if it directly contradicts a federal law, but also if the state law stands as an obstacle to Congress's purpose or objectives.[6] Additionally, the intergovernmental immunity doctrine of the Supremacy Clause prohibits state laws from discriminating against the federal government and burdening it in some way.[7] There is, however, a presumption against a finding that a state law is preempted: when determining whether a state law is preempted, "courts should assume that the historic police powers of the states are not superseded unless that was the clear and manifest purpose of Congress."[8]

---

[1] *Printz v. U.S.* (1997) 521 U.S. 898, 919.
[2] U.S. Const., art. VI, cl. 2.
[3] *Id.*, art. I, § 8.
[4] *Id.*, 10th amend. "Residual state sovereignty was also implicit, of course, in the Constitution's conferral upon Congress of not all governmental powers, but only discrete, enumerated ones…which implication was rendered express by the Tenth Amendment[]." (*Printz*, *supra*, 521 U.S. at p. 919.)
[5] *Printz*, *supra*, 521 U.S. at p. 921 (internal quotation marks omitted).
[6] *E.g.*, *Gade v. National Solid Waste Management Ass'n* (1992) 505 U.S. 88, 98.
[7] *E.g.*, *North Dakota v. U.S.* (1990) 495 U.S. 425, 436-438.
[8] *Arizona v. U.S.* (2012) 567 U.S. 387, 400

3. Background on "administrative subpoenas"

An "administrative subpoena," also known as a "regulatory subpoena," is a request from an agency to produce documents or testimony. Some administrative subpoenas that are self-enforcing, meaning the recipient is legally obligated to comply and can face sanctions for the failure to do so. Other administrative subpoenas are "non-self-enforcing" or "non-self-executing," meaning they have no legal force in and of themselves; if a recipient fails to comply, the agency must go to court, defend the legality of the subpoena, and get a court order compelling the documents or testimony.[9] Once a court order is issued, the recipient must comply or face contempt charges; but until then, they have no obligation to respond.[10] The term "subpoena" is thus a bit of a misnomer for these requests, since compliance with the initial request is entirely voluntary.

One federal agency authorized to propound non-self-executing administrative subpoenas is ICE.[11] Section 1225 authorizes ICE to request documents and information "relating to the privilege of any person to enter, reenter, reside in, or pass through" the U.S. or "any material which is material or relevant to the enforcement of the [Immigration and Nationality Act]."[12] Under the second Trump administration, however, ICE has been using administrative subpoenas broadly, for purposes unrelated to immigration enforcement:

> The Department of Homeland Security is expanding its efforts to identify Americans who oppose Immigration and Customs Enforcement by sending tech companies legal requests for the names, email addresses, telephone numbers and other identifying data behind social media accounts that track or criticize the agency.
>
> In recent months, Google, Reddit, Discord and Meta, which owns Facebook and Instagram, have received hundreds of administrative subpoenas from the Department of Homeland Security, according to four government officials and tech employees privy to the requests. They spoke on the condition of anonymity because they were not authorized to speak publicly.

---

[9] *See, e.g.*, 21 U.S.C. § 876 (Attorney General may issue an administrative subpoena in connection with an investigation in connection with controlled substances; in the event the subject does not comply, the Attorney General may seek a court order for compliance). A court reviewing a petition to enforce an administrative subpoena must determine "(1) whether Congress has granted the authority to investigate; (2) whether procedural requirements have been followed; and (3) whether the evidence is relevant and material to the investigation" as well as whether the subpoena satisfies a Fourth Amendment "reasonableness" inquiry. (*U.S. v. Golden Valley Elec. Ass'n* (9th Cir. 2012 689 F.3d 1108, 1113 (internal quotation marks omitted).)

[10] *E.g.*, *Twitter, Inc. v. Paxton* (9th Cir. 2022) 56 F.4th 1170, 1176.

[11] *See* Section 1225.

[12] *Ibid.*

> Google, Meta and Reddit complied with some of the requests, the government officials said. In the subpoenas, the department asked the companies for identifying details of accounts that do not have a real person's name attached and that have criticized ICE or pointed to the locations of ICE agents. The New York Times saw two subpoenas that were sent to Meta over the last six months.
>
> The tech companies, which can choose whether or not to provide the information, have said they review government requests before complying. Some of the companies notified the people whom the government had requested data on and gave them 10 to 14 days to fight the subpoena in court.…
>
> "When we receive a subpoena, our review process is designed to protect user privacy while meeting our legal obligations," a Google spokeswoman said in a statement. "We inform users when their accounts have been subpoenaed, unless under legal order not to or in an exceptional circumstance. We review every legal demand and push back against those that are overbroad."…
>
> Unlike arrest warrants, which require a judge's approval, administrative subpoenas are issued by the Department of Homeland Security. They were only sparingly used in the past, primarily to uncover the people behind social media accounts engaged in serious crimes such as child trafficking, said tech employees familiar with the legal tool. But last year, the department ramped up its use of the subpoenas to unmask anonymous social media accounts.
>
> In September, for example, it sent Meta administrative subpoenas to identify the people behind Instagram accounts that posted about ICE raids in California, according to the A.C.L.U. The subpoenas were challenged in court, and the Department of Homeland Security withdrew the requests for information before a judge could rule.[13]

The subject of such an administrative subpoena could, presumably, challenge the subpoena on the grounds that it both (1) is outside the scope of ICE's authority under Section 1225, and (2) requests information that seeks to punish and/or chill speech protected by the First Amendment. But the subject can't challenge the subpoena if they don't know about it.

---

[13] Frenkel & Isaac, *Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts* (Feb. 13, 2026) New York Times, https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html (link current as of April 17, 2026.)

4. This bill, as the author has agreed to amend it, establishes procedures a social media company must follow when it receives an administrative subpoena for an individual's personal data

This bill establishes the "Stopping Harmful Information Exploitation and Lawless Data Sharing Act," aka the SHIELD Act. The author agreed to a number of amendments in the Senate Privacy, Digital Technologies, and Consumer Protection Committee; those amendments are reflected in this analysis.

As the author agreed to amend it, the SHIELD Act requires a social media company to do the following when it receives an administrative subpoena under Section 1225 or the Tariff Act of 1930[14] requesting an individual's personal information:

- Promptly notify the individual whose information is sought by the request.
- Provide the individual whose information is sought at least 30 days to respond to or challenge the subpoena before providing information in response to the request.
- If the social media company discloses personal information in response to the request, notify the information whose information was disclosed (1) the reason for the disclosure, (2) the basis for determining the request was valid, and (3) a description of the information disclosed.
- Prior to disclosing information in response to a request, determine if the request is invalid on the basis that (1) the information sought is not related to any lawfully authorized purpose, (2) the information is irrelevant to the stated lawfully authorized purpose, or (3) the information requested is overly broad or compliance would be unduly burdensome.
- If the social media company determines that a request is invalid, as provided, but provides information anyway, notify the attorney general before disclosing the personal information; the social media company may not respond while the Attorney General is reviewing the request.
- If there is a legal challenge to the request, not respond to the request while the legal challenge is pending.

Because the administrative subpoenas covered by the bill are not self-executing, this bill does not require a social media company to disobey any binding federal demand, and the bill clarifies that nothing in the SHIELD Act prohibits a social media company from complying with a valid court order.[15] The bill authorizes the Attorney General or a

[14] *See* 19 U.S.C. §§ 1509, 1510.

[15] The CBP's subpoena authority under the Smoot-Hawley Tariff Act does authorize penalties for noncompliance when the recipient fails to produce records "required by law or regulation for the entry of the merchandise." (*See* 19 U.S.C. §§ 1508, 1509(a) & (g).) The amount of the penalty is calculated based off of "the apprised value of the merchandise." (*Id.* at § 1509(g).) In the unlikely event that CBP subpoenas a social media company for an individual's import or export records, and that individual actually stores those records on a social media platform, it does not appear that this bill's definition of

person whose information has been shared in violation of the SHIELD Act to bring an action for an injunction or declaratory relief against a social media company. The author has agreed to minor amendments to clarify the Attorney General's role and the social media company's obligation to inform the Attorney General when it responds to an administrative subpoena for an individual's records; to conform the list of factors a social media company should consider when determining the validity of an administrative subpoena to the factors established in case law; and to add privacy protections for any personal information provided to the Attorney General by a social media company; these amendments are set forth in Comment 5, below.

The Senate Privacy, Digital Technologies, and Consumer Protection Committee considered this bill from an overall policy standpoint and passed it with a vote of 7-1. For purposes of this Committee's jurisdiction, the primary questions are the remedy and the latent constitutional questions presented by the bill. The remedies created by the bill are, as noted above, straightforward and limited—the bill creates no action for damages—so the main issue is whether this bill can withstand constitutional muster.

As discussed in Comment 2, above, states generally retain their historic police powers under the Tenth Amendment. While the "Supremacy Clause generally immunizes the Federal Government from state laws that (1) directly regulate, or (2) discriminate against it,"[16] it is not clear that this bill does either. This bill regulates only the conduct of social media companies, and "the mere fact that actions of the federal government are incidentally *targeted*…does not mean that they are incidentally *burdened*."[17] Going forward, the author may wish to work with stakeholders to determine whether additional types of administrative subpoenas, including subpoenas established under state law, should be covered by the bill, to give Californians additional protections against fishing expeditions.

5. Amendments

As noted above in Comment 4, the author has agreed amendments which will be taken by this Committee in addition to the amendments the author agreed to in the Senate Privacy, Digital Technologies, and Consumer Protection Committee. The amendments are as follows, subject to any nonsubstantive changes the Office of Legislative Counsel may make:

- Add, to the definition of "personal information": "Personal information" does not include any record that is required by law or regulation for the entry of

---

"personal information" extends to such documents; out of an abundance of caution, however, the author has agreed to amend the bill to clarify this point.

[16] *Geo Group, Inc. v. Inslee* (9th Cir. 2025) 151 F.4th 1107, 1116, rehg. en banc den. (9th Cir. 2026) 166 F.4th 1188 (cleaned up).

[17] *United States v. California*, *supra*, 921 F.3d at p. 880 (upholding AB 450 (Chiu, Ch. 492, Stats. 2017), which prohibited private employers from providing voluntary consent to immigration enforcement agents to enter nonpublic areas of labor or access or review employee documents).

merchandise under subparagraph (A) of paragraph (1) of subdivision (a) of Section 1509 of Title 19 of the United States Code.

- In the list of factors in subdivision (d), add "The administrative subpoena was procedurally improper"; add "or immaterial" after "irrelevant"; and replace "The information requested by the administrative subpoena is overly broad or compliance would be unduly burdensome" with "The administrative subpoena is too indefinite or broad."
- Eliminate the provisions requiring a social media company to notify the Attorney General only when it responds to an administrative subpoena it deems invalid; and add a requirement that a social media company to notify the Attorney General each time it responds to an administrative subpoena for personal information within five days of its response, and a requirement for the Attorney General to develop a process for a social media to submit that information.
- Specify that a social media company is required to refrain from responding to an administrative subpoena while a challenge is pending only if the social media company has actual knowledge of the challenge.
- Eliminate the provision stating that a social media company shall not respond to an administrative subpoena if the Attorney General requests a delay pending review of the administrative subpoena.
- Provide that information submitted to the Attorney General by a social media company relating to the administrative subpoena for personal information is not a public record and shall not be disclosed under the California Public Records Act, and make findings and declarations relating to the necessity of that exemption.

6. Arguments in support

According to the Electronic Frontier Foundation:

> For decades, people have used their social media platforms as a space for personal expression, often engaging in activism, advocacy, and political discussion. Discussions around politics and government have been particularly prominent under the current federal administration, especially regarding the community impacts resulting from increased immigration enforcement activity. These actions have involved enforcement in and near locations, such as churches and schools, once considered sensitive areas, leading to widespread fear and confusion among impacted communities…
>
> In recent months, the federal government has increasingly issued administrative subpoenas to social media companies, requesting the personal information of individuals linked to accounts that have tracked or criticized ICE. These subpoenas do not require judicial approval or probable cause. The rise in requests for sensitive personal data, including names, addresses, phone numbers, and more, has raised significant privacy concerns. Some of these

administrative subpoenas have been challenged in court. In one example, the American Civil Liberties Union (ACLU) argued that the federal government was using subpoenas to target individuals whose speech they disagreed with. Although the Department of Homeland Security (DHS) claimed it was investigating threats to its officers, the subpoena at issue was ultimately withdrawn without comment or explanation. In another case, an administrative subpoena was challenged in federal court as a violation of the first amendment, and the court ultimately ruled that subpoenas cannot be used to intimidate individuals who criticize federal agencies.

While some social media companies review requests before complying and notify users when their information has been subpoenaed, this is not required. Companies may turn over user data without any independent review. It is essential that people's privacy and right to free speech are protected and reinforced. S.B. 957 implements safeguards that enhance user privacy and user data protections. This bill establishes guidelines for social media companies when responding to administrative subpoena requests.

SUPPORT[18]

Electronic Frontier Foundation

OPPOSITION

None received

RELATED LEGISLATION

Pending legislation: AB 1542 (Ward, 2026) prohibits, pursuant to the CCPA, a business, service provider, or contractor from selling or sharing the sensitive personal information of a consumer to a third party. AB 1542 is currently in the Assembly Privacy and Consumer Protection Committee.

Prior legislation:

SB 918 (Umberg, Ch. 985, Stats. 2024) required a social media platform, as defined, with one million or more discrete monthly users, to maintain a law enforcement contact process that, among other things, makes available a staffed hotline for law enforcement personnel for purposes of receiving, and responding to, requests for information; and to comply with a search warrant within 72 hours if the search warrant is provided to the social media platform by a law enforcement agency, the subject of the search warrant is

[18] The Committee received support for bill before it was gutted and amended to address the current subject matter; that support is irrelevant to the current bill and not reflected here.

information associated with an account on the social media platform, and that information is controlled by a user of the social media platform.

AB 522 (Kalra, 2023) would have added restrictions on when the head of a department in state government could obtain electronic communication information from a service provider, including a requirement that the department serves notice of the subpoena and a copy of the subpoena on the customer. AB 522 died in the Senate Appropriations Committee.

PRIOR VOTES:

Senate Privacy, Digital Technologies, and Consumer Protection Committee (Ayes 7, Noes 1)

****