Date of Hearing: June 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 957 (Pérez) – As Amended April 27, 2026

PROPOSED AMENDMENT

SENATE VOTE: 30-9

SUBJECT: Privacy: social media companies: administrative subpoenas: remedies

SYNOPSIS

As individuals subjected to the increasingly militant tactics of federal immigration officers have turned to social media to help share information, protect communities, and organize protests, immigration officers have resorted to issuing "administrative subpoenas" – bureaucrat-issued requests for information – to social media companies to track down account holders. These subpoenas often aim to chill the exercise of constitutionally-protected rights and intimidate communities in a manner that is highly unlikely to withstand judicial scrutiny.

This bill, the Stopping Harmful Information Exploitation and Lawless Data Sharing (SHIELD) Act seeks to regulate social media companies' responses to immigration-related federal administrative subpoenas for personal information. Before responding to such subpoenas, social media companies must: (1) promptly notify individuals whose info was requested, (2) give them 30 days to respond or challenge the subpoena, (3) assess the subpoena's validity, and (4) refrain from responding if the company has actual knowledge of a pending challenge to the subpoena. After responding, the company must provide notice to the individual of the reason for the disclosure, the basis for determining the subpoena was valid, and a description of the information disclosed. The company must also notify the Attorney General (AG) of the disclosure within 5 days. The AG and individuals whose information was disclosed in violation of the bill may seek injunctive and declaratory relief.

The bill is sponsored by the California Legislative LGBTQ Caucus, and is supported by, among others, ACLU California Action, , Electronic Frontier Foundation, Oakland Privacy, and Public Counsel. The bill has no registered opposition.

A technical amendment is described in Comment #4.

If passed by this Committee, the bill will be re-referred to the Judiciary Committee.

EXISTING LAW:

1) Under the Smoot-Hawley Tariff Act (Tariff Act), sets forth procedures for the Secretary of Homeland Security or Customs and Border Patrol (CBP) to examine records relating to the importation of merchandise for purposes of assessing the correctness of entry or liability for duties, fees, or taxes, upon reasonable notice, if the record is required by law or regulation for the entry of merchandise, in which case it must be provided within a reasonable time after demand for its production is made, as specified. (19 USC § 1509(a)(1)(A).) Imposes

penalties of the lesser of: 75 percent of the appraised value of merchandise or $100,000 for willful violations, and 40 percent of the appraised value of merchandise or $10,000 for negligent violations. (*Id.* at (g)(2).)

2) In connection with the enforcement of the Immigration and Nationality Act (INA), authorizes the Attorney General of the United States and any immigration officer to require by subpoena the attendance and testimony of witnesses for immigration officers 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 that is material and relevant to the enforcement of immigration laws, as specified. (8 USC § 1225(d)(4)(A).)

3) Authorizes federal district courts, in the event of refusal to respond to such a subpoena, to issue an order requiring such persons to appear before an immigration office and produce records; makes failure to obey such orders punishable as contempt of court. (*Id.* at (B).)

4) Defines "social media platform" as a public or semipublic internet-based service or application that has users in California and that meets both of the following criteria:

    a. A substantial function of the service or application is to connect users to allow users to interact socially with each other within the service or application. A service or application that provides email or direct messaging services is not considered to meet this criterion based on that function alone.

    b. The service or application allows users to do all the following:

        i. Construct a public or semipublic profile for purposes of signing into and using the service or application.
        ii. Populate a list of other users with whom an individual shares a social connection within the system.
        iii. Create or post content viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users. (Bus. & Prof. Code § 22675(f).)

5) Defines "personal information" within the California Consumer Privacy Act (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).)

THIS BILL:

1) Defines:

    a. "Administrative subpoena" as a subpoena issued pursuant to the Tarriff Act or INA provisions described above.

    b. "Personal information" as 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. Specifically excludes any record that is required by law or regulation for the entry of merchandise pursuant to the Tariff Act provision described above.

c. "Social media company" by incorporating the existing definition described above.

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

3) Before disclosing personal information in response to the subpoena, requires the social media company to:

   a. Provide the individual at least 30 days to respond or challenge the administrative subpoena.

   b. Determine whether the administrative subpoena is invalid because it is (1) not lawfully authorized pursuant to the INA provision described above; (2) procedurally improper, (3) seeking information not relevant to the valid purpose of the subpoena; or (4) seeking information that is too indefinite or broad.

   c. Refrain from disclosing the information while a legal challenge to the subpoena is pending if the social media company has actual knowledge of the challenge.

4) If the social media company discloses the personal information, requires the social media company to:

   a. Provide notice to the individuals of (1) the reason for disclosing the information, (2) the basis for determining that the administrative subpoena was valid, and (3) a description of the information that was disclosed.

   b. Provide the AG notice within five business days of the response, pursuant to process the AG must develop. Such information is exempted from the Public Records Act.

5) Authorizes the AG and individuals whose information were disclosed in violation of the bill to bring an action for injunctive or declaratory relief against a social media company that violates the bill.

COMMENTS:

1) **Author's statement**. 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) **Background**. The Constitution of the United States establishes a system of dual sovereignty between the federal and state governments. While state are prohibited from unduly burdening the federal government,[1] courts are required to "assume that the historic police powers of the states are not superseded unless that was the clear and manifest purpose of Congress."[2] Accordingly, "the mere fact that actions of the federal government are incidentally *targeted*…does not mean that they are incidentally *burdened*."[3] Thus, courts have upheld as valid exercises historic police power some of California's efforts to protect immigrants from an overreaching administration, including the California Values Act (SB 54, De León, Stats. 2017, Ch. 495),[4] which limited local law enforcement agencies' sharing of inmate information with federal immigration agencies, and prohibited law enforcement agencies from using their resources for immigration enforcement or from cooperating in immigration enforcement activities.

One particular example of federal overreach has come in the form of immigration-related administrative subpoenas.[5] Recent reports indicate that ICE has been using these for purposes unrelated to immigration enforcement:

---

[1] *United States v. California* (2019) 921 F.3d 865.
[2] *Arizona v. U.S.* (2012) 567 U.S. 387, 400
[3] *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).
[4] *United States v. California* (2019) 921 F.3d 865; United States v. California (2020) 141 S. Ct. 124.
[5] As described in the Senate Judiciary Committee's analysis of this bill:

> 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. Once a court order is issued, the recipient must comply or face

> 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.
>
> 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.[6]

3) **What this bill would do.** This bill, the Stopping Harmful Information Exploitation and Lawless Data Sharing (SHIELD) Act seeks to regulate social media companies' responses to immigration-related federal administrative subpoenas for personal information. "Administrative

---

contempt charges; but until then, they have no obligation to respond. The term "subpoena" is thus a bit of a misnomer for these requests, since compliance with the initial request is entirely voluntary.

[6] 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.)

subpoenas" for these purposes are limited to two specific types. First, the INA authorizes administrative subpoenas for any matter relevant to the enforcement of immigration laws. These subpoenas are not self-executing,[7] so a company does not face liability unless a separate court order is obtained. Second, the Tariff Act authorizes the CBP to examine records relating to the correctness of entry or liability for duties, fees, or taxes related to the entry of merchandise. Requests for personal information about social media accountholders seem far afield of the scope of this subpoena authority.

Before responding to such subpoenas, social media companies must: (1) promptly notify individuals whose info was requested, (2) give them 30 days to respond or challenge the subpoena, (3) assess the subpoena's validity, and (4) refrain from responding if the company has actual knowledge of a pending challenge to the subpoena. After responding, the company must provide notice to the individual of the reason for the disclosure, the basis for determining the subpoena was valid, and a description of the information disclosed. The company must also notify the Attorney General (AG) of the disclosure within 5 days. The AG and individuals whose information was disclosed in violation of the bill may seek injunctive and declaratory relief.

4) **Amendment.** The author has agreed to amend the bill to clarify that the requirement that a social media company assess the validity of an administrative subpoena expressly includes subpoenas issued pursuant to the Tariff Act. The amendment is as follows:

> (1) The information requested by the administrative subpoena is not related to any purpose lawfully authorized pursuant to subparagraph (A) of paragraph (4) of subsection (d) of Section 1225 of Title 8 of the United States Code, as that section read on January 1, 2026, ***or pursuant to subparagraph (A) of paragraph (1) of subsection (a) of Section 1509 of Title 19 of the United States Code, as that section read on January 1, 2026.***

ARGUMENTS IN SUPPORT: ACLU California Action writes in support:

> Over the past year, armed federal agents have appeared in communities around the country to carry out a series of violent and repressive raids. Agents have snatched people from churches, carwashes, and ordinary places of business, spreading fear through families and communities. People's response to the horror of these raids has been to come together in community and solidarity, recording the actions of those armed agents and speaking out against their abuses.
>
> DHS has responded with threats and intimidation. In June 2025, DHS issued an internal bulletin titled, "Recent Anti-Law Enforcement Tactics Used in Unlawful Civil Arrest." The bulletin identified use of cameras, "note taking," "livestreaming" law enforcement officers, and posting videos on social media as examples of "suspicious activity," "unlawful civil unrest" tactics or "threats." A month later, then-DHS Secretary Kristi Noem stated that "violence" includes "anything that threatens [DHS agents] and their safety. So it is doxing them. It is videotaping them where they're at." DHS later told reporters that "videotaping

---

[7] Courts 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.)

ICE law enforcement and posting photos and videos of them online is doxing our agents . . . We will prosecute those who illegally harass ICE agents to the fullest extent of the law."

DHS has responded with the same pattern of threats and intimidation when people monitor the government's conduct online. In September and October 2025, for example, DHS issued administrative subpoenas to Meta in an attempt to unmask anonymous social media accounts that have been critical of recent DHS actions. Following motions to quash filed by the ACLU, magistrate judges in the Northern District of California ordered Meta not to disclose the information requested by those administrative subpoenas. After being challenged in court, DHS withdrew the subpoenas.

Even though these few subpoenas that were challenged in court were withdrawn, they still caused lasting harm. As one anonymous ACLU client stated in their declaration, "I am haunted by the possibility that the government will find out who I am using this subpoena. I imagine armed agents smashing through the door of my home in the middle of the night. I imagine agents breaking down the door of my family's home and abducting people I love dearly. I imagine the children in my family seeing people who care for them harmed and taken. I imagine those children being harmed. Those images fill me with dread."

REGISTERED SUPPORT / OPPOSITION:

Support

California Legislative LGBTQ Caucus (Sponsor)
ACLU California Action
Cair California
Electronic Frontier Foundation
Oakland Privacy
Public Counsel
Western Center on Law & Poverty

Opposition

None on file.

Analysis Prepared by: Josh Tosney / P. & C.P. / (916) 319-2200