Date of Hearing: June 23, 2026

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 957 (Pérez) – As Amended June 18, 2026

SENATE VOTE: 30-9

SUBJECT: PRIVACY: SOCIAL MEDIA COMPANIES: ADMINISTRATIVE SUBPOENAS: REMEDIES

SYNOPSIS

The Department of Homeland Security (DHS) has increasingly utilized "administrative subpoenas" as a method for targeting individuals on social media who are critical of the current administration. These administrative subpoenas are sent to social media companies, and request personal information, locations, and identifying details of users. Because these subpoenas go directly to social media companies, individuals may not be aware of their existence, and thus not able to challenge their validity. This bill, Stopping Harmful Information Exploitation and Lawless Data Sharing (SHIELD) Act, would require social media companies to notify users when they have received an administrative subpoena under the Tariff Act of 1930 or the Immigration and Nationality Act. The bill would require that individuals be given 30 days to respond to the request, and that social media companies review the subpoenas for validity. If a social media company discloses a user's information, they must report that disclosure to the Attorney General. Both the Attorney General and an individual who has had their information disclosed in violation of the bill may seek injunctive and declaratory relief.

This bill is sponsored by the California Legislative LGBTQ Caucus and is supported by the ACLU and privacy rights advocacy groups. The bill is opposed unless amended by TechNet. The bill passed out of the Assembly Committee on Privacy and Consumer Protection by a 11-2 vote.

SUMMARY: Places requirements and restrictions on social media companies with respect to their handling of specified administrative subpoenas. Specifically, **this bill**:

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

2) Requires a social media company, before disclosing personal information in response to the subpoena, 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 Immigration and Nationality Act or Tariff Act provisions described below, (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; and

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.

3) Requires a social media company, if it discloses personal information in response to a subpoena, 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; and

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

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

5) Defines the following terms:

a) "Administrative subpoena" means a subpoena issued pursuant to either of the following:

i) 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.

ii) 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.

b) "Individual" means a natural 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. "Personal information" does not include any record that is required by law or regulation for the entry of merchandise 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.

e) "Social media company" means a social media company, as defined in Business and Professions Code Section 22675.

EXISTING LAW:

1) Empowers, pursuant to federal law, 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. Section 1225 (d)(4)(A).)

2) Provides, pursuant to federal law, 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. (U.S.C. Section 1225 (d)(4)(B).)

3) Establishes, pursuant to federal law, the Tariff Act of 1930, also known as the Smoot-Hawley Tariff. (19 U.S.C. Section 1202 *et seq*.)

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; or

   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. Section 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; or

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. Section 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. Section 1510.)

7) 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. (Civil Code Section 1798.100 *et seq*.)

8) 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. (Civil Code Section 1798.105.)

9) 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. (Civil Code Section 1798.140 (v).)

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

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: Recent reporting has detailed the Department of Homeland Security's (DHS) increased targeting of Americans who track or criticize both DHS and Immigration and Customs Enforcement (ICE). (Sheera Frenkel & Mike Isaac, *Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts*, N.Y. Times (Feb. 13, 2026) available at: https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html.) Companies such as Google, Meta, Reddit, and Discord have received hundreds of administrative subpoenas from DHS, demanding personal information about users who have criticized ICE on their platforms (*Ibid*.) The use of these administrative subpoenas can have a chilling effect on speech critical of the current administration. 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 aims to enhance company transparency and privacy of social media users by requiring that social media companies inform their user when their personal information is being sought by the federal government. By ensuring that users are aware when social media companies have been subpoenaed to share their information, it allows individuals to determine next steps in response to these subpoenas, whether that be to challenge them in court or turn over their information. Additionally, given that these types of administrative subpoenas from DHS have been increasingly used to request information on individuals who criticize or share information about federal officers, this bill also provides additional protections to people's privacy and freedom of speech.

Use of Administrative Subpoenas. Administrative subpoenas are subpoenas issued without "judicial sign-off, active litigation, or even probable cause." (Nash, *The Immigration Subpoena Power* (2025) 125 Columbia L. Rev. 1, 4.) These subpoenas are not self-executing, meaning if the recipient fails to comply, the issuing agency must go to court to request a court order to compel a response to the subpoena. As mentioned above, DHS has been using these administrative subpoenas to target those critical of the federal government's actions. The targets of these subpoenas are often able to quash them, as detailed below. However, in order to quash, the targeted individual must be aware of the subpoena's existence.

In September 2025, DHS issued two administrative subpoenas to Meta related to customs investigations, under 19 U.S.C. Section 1509. The subpoenas requested personal information and IP addresses of users who engaged with the "MontCo Community Watch" Instagram and Facebook accounts. These accounts shared information about immigration enforcement activity in Montgomery County, Pennsylvania. The information requested in these subpoenas far exceeded the scope of anything related to a customs investigation. When the ACLU of Pennsylvania challenged these subpoenas, DHS withdrew them. (*Doe v. DHS*, ACLU Pennsylvania, available at: https://www.aclupa.org/cases/doe_dhs/.)

In October 2025, an individual read an article about an attempt by DHS attorneys to deport an Afghan asylum seeker. (*J Doe v. DHS*, ACLU Pennsylvania, available at: https://www.aclupa.org/cases/jdoe_dhs/.) Wanting to express concern, the individual contacted the lead DHS attorney, via email. Just hours later, Google received a subpoena from DHS, under 8 U.S.C. Section 1225, that requested the individual's private information, including about his email account and Google services activity.

In another instance, DHS issued an administrative subpoena, under 19 U.S.C. Section 1509 to Google requesting information and records related to a Gmail account of a user who is a frequent critic of President Trump and DHS on social media. (*Doe v. Mullin – Challenging DHS's Use of Administrative Summonses to Unmask Social Media Critics*, ACLU DC, available at: https://www.acludc.org/cases/challenging-dhs-action-to-unmask-social-media-critics/.) DHS has demanded the user's name, location, and data on online activity. Again, DHS has not provided any basis to connect the requested information to a valid customs investigation.

These are just a few examples of how DHS is using administrative subpoenas to target and intimidate critics. The ACLU of Pennsylvania has submitted a Freedom of Information Act (FOIA) request to obtain more information regarding how and why DHS is using these administrative subpoenas in its investigations. (*FOIA Request Regarding DHS "Unmasking" Subpoenas*, ACLU Pennsylvania, available at: https://www.aclupa.org/cases/foia-request-regarding-dhs-unmasking-subpoenas/.) At this time, DHS has not responded to the request.

This bill, the Stopping Harmful Information Exploitation and Lawless Data Sharing (SHIELD) Act, aims to alert individuals when an administrative subpoena has been issued to a social media company requesting their information. The bill specifies that administrative subpoenas at issue are those issued under the Tariff Act of 1930 and the Immigration and Nationality Act (19 U.S.C. Section 1509; 8 U.S.C. Section 1225.) These administrative subpoenas are supposed to only be issued if they are within the Acts' scope. For example, if an administrative subpoena is issued under the Tariff Act, and it is unrelated to issues of customs, then it would presumably be outside the scope of the administrative subpoena and warrant a challenge from the target of the subpoena.

This bill would require a social media company to promptly notify an individual who is the subject of one of these administrative subpoenas. Before responding to the subpoena, and providing any of the requested information, the social media company would need to wait 30 days, allowing the subject individual a chance to respond or challenge the administrative subpoena. In the event a social media company discloses personal information in response to one of these subpoenas, the social media company would need to provide the subject individual with the reason the information was disclosed, the basis for determining the subpoena was valid, and a description of the information disclosed.

Before a social media company responds to the administrative subpoena, it would be required to determine if the subpoena is invalid for any of the following reasons: (1) the subpoena is outside the scope of the Tariff Act or INA; (2) the subpoena is procedurally improper; (3) the information requested is irrelevant or immaterial; (4) the information is too indefinite or broad. Additionally, if a social media company has actual knowledge of a pending legal challenge to the subpoena, it is prohibited from responding. In the event the social media company responds to the subpoena, it must notify the Attorney General within five days of the response, but the bill

clarifies that any information submitted to the Attorney General will not be considered a public record and would not be disclosed in a public records request. The bill clarifies that if a court order is issued, pursuant to the INA, a social media company is not prohibited from responding. The bill allows for the Attorney General or an individual whose information has been shared to bring an action for injunctive or declaratory relief against a social media company for a violation of the bill.

The Supremacy Clause of the United States Constitution. Article VI, Clause 2 of the United States Constitution, generally referred to as the Supremacy Clause, provides that the U.S. Constitution and federal law is the supreme law of the United States. In other words, "when federal and state law conflict, federal law prevails and state law is preempted." (*See Murphy v. NCAA* (2018) 584 U.S. 453, 471.) Similarly, states are generally forbidden from imposing state legal requirements on the federal government. Because this bill is regulating the actions of a social media company, and not the federal government, there is likely no violation of the Supremacy Clause. Additionally, because the bill is tailored to specific administrative subpoenas, and not court orders, and does not prohibit social media companies from responding to court orders, the bill does not frustrate the purpose of federal law.

Opposition's Concerns. The opposition argues that social media companies may be caught in the middle between conflicting California and federal law. As discussed above, the bill's language does not prevent a social media company from responding to a court order. In fact, the bill is specific to the types of administrative subpoenas it applies to. The opposition states that, according to its member companies, about 90 percent of the subpoenas issued by DHS to them are related to child exploitation investigations. The Tariff Act prohibits goods that are produced or manufactured by forced labor to enter the United States. (19 U.S.C. Section 1307.) The opposition proposes removing the reference to the Tariff Act completely from the definition of "administrative subpoena." Seeing how DHS has utilized the Tariff Act to target individuals, this change appears to frustrate a significant purpose of the bill. *The author may consider including language that would exempt administrative subpoenas that specifically focus on forced labor investigations*. However, seeing the pattern of use by DHS, one could imagine that including this exemption would then lead to individuals being targeted under the false pretenses of a "forced labor" investigation. Therefore, it may not be prudent to include this carve out.

ARGUMENTS IN SUPPORT*:* This bill is sponsored by the California Legislative LGBTQ Caucus and supported by civil liberty and privacy advocacy organizations. The California Legislative LGBTQ Caucus write in support:

> For many LGBTQ+ individuals, social media platforms are more than just tools for communication – they are essential spaces for community building, identity exploration, access to affirming resources, and advocacy. Particularly for young people and those living in unsupportive environments, online platforms can serve as critical lifelines. However, these same platforms can also expose LGBTQ+ individuals to heightened risks when sensitive personal data, such as sexual orientation, gender identity, or associations with LGBTQ+ communities, is accessed without adequate safeguards.
>
> Recent reporting and research have highlighted how social media platforms collect and infer deeply sensitive information about users, including data related to gender identity, sexual orientation, and personal beliefs. In the wrong hands, this information can be used to target, harass, or even endanger LGBTQ+ individuals. The increasing use of administrative

subpoenas by the federal government without judicial oversight or probable cause raises serious concerns about the potential misuse of personal data, particularly when individuals are engaging in protected speech, advocacy, or community organizing.
These risks are especially acute for LGBTQ+ individuals who are also part of other vulnerable communities, including immigrants, people of color, and youth. The threat of surveillance or data disclosure can have a chilling effect, discouraging individuals from seeking support, participating in advocacy, or expressing their identities online. Without clear safeguards, users may have no knowledge that their personal information has been accessed or shared.

SB 957 provides critical protections by requiring transparency and accountability when government entities seek user data. By ensuring that individuals are notified, given time to respond, and informed about what information has been disclosed, this bill helps safeguard both privacy and First Amendment rights. These protections are essential to maintaining safe digital spaces where LGBTQ+ individuals can connect, organize, and express themselves without fear of unjustified surveillance or retaliation.

ACLU California Action write 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 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."

Later reporting revealed that these abusive administrative subpoenas were only the tip the iceberg. On February 13, 2026, the New York Times reported that social media platforms had "received hundreds of administrative subpoenas from the Department of Homeland Security," seeking "names, email addresses, telephone numbers and other identifying data behind social media accounts that track or criticize the agency."

ARGUMENTS IN OPPOSITION: TechNet opposes the bill, unless amended, and writes:

We recognize the importance of user notice and note that many companies already provide notice voluntarily. The bill's notice provisions need clear boundaries and exceptions for circumstances where notice would be legally prohibited or would create a risk of imminent harm. We are glad the bill now sets a specific 30-day window rather than the undefined "sufficient time," but several gaps remain:

- Tie the notice duty to a validity and disclosure determination. As written, the bill could be read to require notice even before a company has determined whether a subpoena is valid or decided whether it will actually disclose the requested information. We ask that the duty to notify apply only once the company has determined the subpoena is valid and intends to disclose the information requested.

- Allow a court to set a different response window. We ask that the bill allow a court of competent jurisdiction to order a different time period in place of the 30-day default, recognizing that a single fixed window will not fit every circumstance.

- Narrow what must be disclosed after the fact. The bill currently requires a company to tell the individual the specific "reason" their information was disclosed and the "basis for determining that the administrative subpoena was valid." Disclosing this level of detail could reveal sensitive investigative information. We ask that the post-disclosure notice instead simply state that the information was disclosed pursuant to an administrative subpoena, along with a description of the information disclosed.

- Add an exception for court-ordered non-disclosure. We ask that the bill make clear that none of the notice requirements apply when a company is subject to a court order prohibiting disclosure of the request, directly addressing the "legally prohibited notice" scenario.

- Add a clear exception for imminent harm and other urgent cases. We ask that the bill allow a company to disclose information without the notice and validity-review steps described above when it has a good faith belief that an emergency involving danger of death or serious physical injury, or a case involving child exploitation, human smuggling, or trafficking, requires disclosure without delay. This directly resolves the "risk of imminent harm" gap, and ensures the bill's procedural requirements do not stand in the way of urgent, good-faith cooperation with law enforcement in exactly the cases where speed matters most.

[…]

The bill currently asks a company to evaluate four separate, undefined standards before disclosing information — whether the subpoena is related to a lawful purpose, whether it is "procedurally improper," whether the information requested is "irrelevant or immaterial," and whether the request is "too indefinite or broad." None of these additional standards are defined, and a company has no clear way to apply them consistently. Asking a private company to make these kinds of legal judgment calls, with no guidance and potential liability for getting it wrong, is not a workable approach and lacks clear compliance standards.

[…]

The bill authorizes enforcement by both the Attorney General and private individuals without clearly defining the scope of liability or the standards for compliance. This creates uncertainty for regulated entities and increases litigation risk, particularly where companies are required to make complex legal determinations without adequate guidance. The bill, as currently drafted, also requires a company to notify the Attorney General within five business days of responding to any administrative subpoena, directs the Attorney General to create a process for receiving these notifications, exempts that information from public records requests, and creates two new causes of action, one allowing the Attorney General to seek injunctive or declaratory relief, and a second allowing an individual to bring a similar private civil action.

We ask that these provisions be removed. The notice, validity-review, and emergency-exception standards described above already give companies a clear set of obligations to follow. Layering a new mandatory reporting regime and two new causes of action on top of those standards adds administrative burden and litigation exposure without a clear, corresponding benefit to the individuals the bill is designed to protect. We believe the bill's purpose is better served by a clear, workable set of standards than by an additional enforcement structure built on top of them.

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

Oppose Unless Amended

TechNet

Analysis Prepared by: Griff Ryan-Roberts / JUD. / (916) 319-2334