

---

THIRD READING

---

Bill No: SB 957  
Author: Pérez (D)  
Amended: 4/27/26  
Vote: 21

---

SENATE PRIV., DIGITAL TECH. & CONS. PROT. COMMITTEE: 7-1, 4/13/26  
AYES: Cabaldon, Gonzalez, McNerney, Padilla, Reyes, Umberg, Wiener  
NOES: Ochoa Bogh  
NO VOTE RECORDED: Jones

SENATE JUDICIARY COMMITTEE: 12-0, 4/21/26  
AYES: Umberg, Niello, Allen, Ashby, Caballero, Durazo, Laird, Reyes, Stern,  
Wahab, Weber Pierson, Wiener  
NO VOTE RECORDED: Valladares

SENATE APPROPRIATIONS COMMITTEE: 5-2, 5/14/26  
AYES: Cervantes, Cabaldon, Grayson, Richardson, Wahab  
NOES: Seyarto, Dahle

---

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

**SOURCE:** Author

---

**DIGEST:** This bill places requirements and restrictions on social media companies with respect to their handling of administrative subpoenas issued pursuant to specified federal laws.

**ANALYSIS:**

Existing federal law:

- 1) Empowers the Attorney General and any immigration officer to require by subpoena the attendance and testimony of witnesses before 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 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) (hereinafter “Section 1225”).)

- 2) 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). (hereinafter “Section 1509”).)
- 3) Provides that the U.S. Constitution (Const.), and the Laws of the United States, are the supreme law of the land. (U.S. Const., art. VI, cl. 2.)

Existing state law:

- 4) Establishes the California Consumer Privacy Act, 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 (Civ.) Code § 1798.100 et seq.)

- 5) 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.)

This bill:

- 1) Establishes the “Stopping Harmful Information Exploitation and Lawless Data Sharing Act,” the SHIELD Act.
- 2) Requires a social media company to promptly notify an individual whose personal information is requested by administrative subpoena, as defined.
- 3) Requires a social media company, prior to disclosing personal information in response to an administrative subpoena, to provide the individual whose personal information is requested with at least 30 days to respond to or challenge the administrative subpoena.
- 4) Provides that, if a social media company discloses personal information in response to an administrative subpoena, the social media company shall provide notice to the individual whose personal information was disclosed of all of the following:
  - a) The reason the individual’s personal information was disclosed.
  - b) The basis for determining that the administrative subpoena was valid.
  - c) A description of the information that was disclosed.
- 5) Requires a social media company, prior to disclosing personal information, to determine if the administrative subpoena is invalid for any of the following reasons:
  - a) 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.
  - b) The administrative subpoena is procedurally improper.
  - c) The information requested by the administrative subpoena is irrelevant or immaterial to the purpose described.
  - d) The information requested by the administrative subpoena is too indefinite or broad.

- 6) Provides that, if a social media company responds to an administrative subpoena for personal information, it must notify the Attorney General within five business days of the response. The Attorney General must develop a process for a social media company to submit this notice.
- 7) Prohibits a social media company from responding to an administrative subpoena for personal information while a legal challenge to the subpoena is pending if the social media company has actual knowledge of the challenge.
- 8) Defines the relevant terms:
  - a) “Administrative subpoena” means a subpoena issued pursuant to Sections 1225 or 1509.
  - 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, except as specified.
  - e) “Social media company” means a social media company, as defined in Section 22675.
- 9) Authorizes the Attorney General to bring an action for injunctive or declaratory relief against any social media company who violates this chapter. An individual whose information has been shared in response to an administrative subpoena by a social media company in violation hereof may also bring such a civil action.
- 10) Makes clear that this does not interfere with the ability of a social media company to respond to a court order issued pursuant to Section 1225 or any other law.
- 11) Includes a severability clause.

## **Background**

Recently, immigration enforcement officials have turned to social media sites as a source for information in their investigations. Reports indicate that this has not been isolated to criminal matters or even civil matters within their statutory

authority, but veered into dragnets targeting anyone who tracks or criticizes Immigration and Customs Enforcement (ICE). One main tool used by ICE is administrative subpoenas served on social media companies to gather information on their targets.

This bill seeks to respond to the increased utilization of these tactics by requiring social media platforms to notify individuals before and after, if applicable, the company responds to specified administrative subpoenas. This bill requires social media companies to determine whether the subpoenas are valid and to notify the Attorney General when they respond. Enforcement is delegated to the Attorney General and right of action is provided to individuals whose information is shared in violation of these provisions.

This bill is author-sponsored. It is supported by several organizations, including Oakland Privacy. No timely opposition has been received.

### **Comment**

In addition to the blitzkrieg of immigration enforcement activities, the Department of Homeland Security has feverishly sought to obtain more and more data on Californians. Reports show that one new target has been social media platforms and the focus has not been limited:

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.<sup>1</sup>

This bill seeks to address the overbroad use of administrative subpoenas served on social media companies by requiring them to take the very actions identified by Google and discussed above. This bill establishes the “Stopping Harmful Information Exploitation and Lawless Data Sharing Act,” the SHIELD Act. It provides that social media companies receiving these administrative subpoenas are required to provide notice to the individuals, to assess the validity of the subpoenas, and to notify the Attorney General when the companies respond. The Attorney General is authorized to bring an action for injunctive or declaratory relief against a platform in violation. In addition, an individual whose information has been shared in violation hereof may also bring a civil action for the same relief.

---

<sup>1</sup> Sheera Frenkel & Mike Isaac, *Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts* (February 13, 2026) The New York Times, <https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html> [as of May 14, 2026].

According to the author:

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.

**FISCAL EFFECT:** Appropriation: No Fiscal Com.: Yes Local: No

According to the Senate Appropriations Committee:

Major costs annually for the AG to establish an information technology based process to receive and track notices.

Unknown, significant cost pressure on the trial courts to the extent there are additional civil filings for unlawful sharing of personal information by social media companies. Although courts are not funded based on workload, increased

pressure on the Trial Court Trust Fund may create a demand for increased funding for courts. The proposed FY 2026-07 Governor's budget would provide \$70 million General Fund support (Trial Court Trust Fund, General Fund).

**SUPPORT:** (Verified 5/14/26)

Electronic Frontier Foundation  
Oakland Privacy  
Stand With Survivors

**OPPOSITION:** (Verified 5/14/26)

None received

**ARGUMENTS IN SUPPORT:** Oakland Privacy writes:

The disclosure requirement in SB 957 allows people to know when a non-judicial information request has been sent to a social media platform about them. Since these are not court proceedings based on any cause, there is no reason for them to be a secret for the subject, who may well have to make preparations. In attempting to ensure that a person's personal information is sent to an agency before they have a chance to respond or legally challenge the subpoena, the bill asks the social media company to wait, but is not specific enough about how long they should wait. We recommend that the bill describe an interval between the date of notification and the date that a social media company can, if they wish, fulfill the administrative subpoena. Forty-five days seems reasonable.

Prepared by: Christian Kurpiewski / P., D.T., & C.P. / (916) 651-1548  
5/16/26 9:57:03

\*\*\*\* END \*\*\*\*