

SENATE THIRD READING
SB 957 (Pérez)
As Amended August 13, 2026
Majority vote

SUMMARY

This bill, the Stopping Harmful Information Exploitation and Lawless Data Sharing (SHIELD) Act, imposes notice, review, and reporting requirements on social media companies that receive federal administrative subpoenas seeking a California resident's personal information, and creates civil remedies for violations.

Major Provisions

- 1) Requires a social media company to promptly notify an individual whose personal information is requested by an administrative subpoena.
- 2) 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 for specified reasons.
 - 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) If the social media company discloses the personal information, requires the social media company to:
 - a) Provide notice to the individuals, including a description of the information that was disclosed.
 - b) Provide the Attorney General (AG) notice within five business days of the response, pursuant to process the AG must develop.
- 4) Authorizes the AG 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.

COMMENTS

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burdening the federal government,¹ courts are required to "assume that the historic police powers of the states are not superseded unless that was the clear and manifest purpose of Congress."² Accordingly, "the mere fact that actions of the federal government are incidentally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

¹ *United States v. California* (2019) 921 F.3d 865.

² *Arizona v. U.S.* (2012) 567 U.S. 387, 400

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), Chapter 495, Statutes of 2017,⁴ 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:

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

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 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.

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

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.

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.)

Arguments in Support

The California Legislative LGBTQ Caucus writes:

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.

Arguments in Opposition

TechNet opposes the bill unless amended, contending that the validity-review standards are undefined and ask companies to make complex legal determinations without clear guidance, that the bill should include exceptions for court-ordered nondisclosure and for emergencies involving imminent harm or child exploitation, and that the reporting requirement and two new causes of action add administrative burden and litigation exposure.

FISCAL COMMENTS

According to the Appropriations Committee:

- 1) Costs of an unknown, but potentially significant amount over this committee's suspense threshold, to DOJ (General Fund) to develop the process by which social media companies submit the notices required by this bill, implement that process, and enforce compliance. DOJ's Civil Rights Enforcement Section and Consumer Law Section indicate the magnitude of costs will depend on complexities arising in the development and implementation of the submission process and in the enforcement of violations.

- 2) Court cost pressures of an unknown, but potentially significant amount (Trial Court Trust Fund) resulting from additional civil filings under the two causes of action the bill creates — actions for injunctive or declaratory relief brought by the Attorney General and by individuals whose information was disclosed in violation of the bill. Actual costs will depend on the number of cases filed and the amount of court time needed to resolve each case. It generally costs approximately \$1,000 to operate a courtroom for one hour. Although courts are not funded on the basis of workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for courts from the General Fund. The state budget provides annual General Fund backfills to the Trial Court Trust Fund to offset revenue reductions, totaling approximately \$117.3 million in 2025-26.

VOTES

SENATE FLOOR: 30-9-1

YES: Allen, Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Cortese, Durazo, Gonzalez, Grayson, Hurtado, Laird, Limón, McGuire, McNerney, Menjivar, Padilla, Pérez, Reyes, Richardson, Rubio, Smallwood-Cuevas, Stern, Umberg, Wahab, Weber Pierson, Wiener

NO: Alvarado-Gil, Choi, Dahle, Grove, Jones, Ochoa Bogh, Seyarto, Strickland, Valladares

ABS, ABST OR NV: Niello

ASM PRIVACY AND CONSUMER PROTECTION: 11-2-2

YES: Bauer-Kahan, Bryan, Irwin, Lowenthal, McKinnor, Ortega, Pellerin, Petrie-Norris, Ward, Wicks, Wilson

NO: Macedo, DeMaio

ABS, ABST OR NV: Hoover, Patterson

ASM JUDICIARY: 9-3-0

YES: Kalra, Bauer-Kahan, Bryan, Connolly, Harabedian, Pacheco, Papan, Stefani, Zbur

NO: Macedo, Dixon, Sanchez

ASM APPROPRIATIONS: 11-3-1

YES: Wicks, Arambula, Calderon, Caloza, Fong, Mark González, Krell, Pacheco, Pellerin, Sharp-Collins, Solache

NO: Dixon, Ta, Tangipa

ABS, ABST OR NV: Hoover

UPDATED

VERSION: August 13, 2026

CONSULTANT: Josh Tosney / P. & C.P. / (916) 319-2200

FN: 0003686