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

AB 302 (Bauer-Kahan)
Version: July 3, 2025
Hearing Date: July 8, 2025
Fiscal: Yes
Urgency: No
AM

SUBJECT

Protected individuals

DIGEST

This bill seeks to provide enhanced privacy protections for elected official and judges by, among other things, requiring businesses and government agencies to delete their personal information upon request subject to a civil enforcement action for noncompliance.

EXECUTIVE SUMMARY

The recent events in Minnesota where elected politicians and their spouses were targeted in their homes and, in one instance, tragically killed provides a stark reminder that serving in public office poses risks for those who choose to serve and their family.[1] In response to these recent events, this bill seeks to provide enhanced protections to protected individuals, defined as a former and current representative elected in this state, an appointed officer of a court or magistrate in this state, and the spouse, child, or dependent who resides in the same household. These protections include allowing a requirement that businesses and government agencies delete their personal information upon request subject to a civil enforcement action for noncompliance. The bill also requires the California Privacy Protection Agency, on behalf of a protected individual, to request a business to refrain from selling their personal information. Though the purpose of the bill is well intentioned and seeks to address a very timely and important issue, it raises constitutional issues and has several operational hurdles, which are described below. In response to these issues, the author has proposed amends to scale the bill back to allow the California Privacy Protection Agency to facilitate the uploading of elected officials and California judges to the accessible deletion

[1] Steven Karnowski, et. al, *The man suspected of shooting 2 Minnesota lawmakers is in custody after surrendering to the police*, AP News, (June 16, 2025), available at https://apnews.com/article/minnesota-lawmakers-shot-8ce70a94c9eb90688baaa1a71faef6cc.

mechanism established under SB 362 (Becker, Ch. 709, Stats. 2023.) These amendments are discussed below and a mock-up is provided.

The bill is author sponsored. The bill is opposed by a diverse group of organizations, including first amendment advocacy organizations, organizations that advocate for business, realtors, and technology, and the California Land Title Association.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides that the home addresses, home telephone numbers, personal cellular telephone numbers, and birthdates of all employees of a public agency are not public records and are not open to public inspection. (Gov. Code § 7928.300(a).)

2) Prohibits a person from knowingly posting the home address or telephone number of any elected or appointed official, or of the official's residing spouse or child, on the internet knowing that person is an elected or appointed official and intending to cause imminent great bodily harm that is likely to occur or threatening to cause imminent great bodily harm to that individual, and provides that a violation is a misdemeanor, unless the violation leads to the bodily injury of the official, or their residing spouse or child, in which case the violation is a misdemeanor or a felony. (Gov. Code § 7928.210.)

3) Prohibits any person, business, or association from soliciting, selling, or trading on the internet the home address or telephone number of an elected or appointed official with the intent to cause imminent great bodily harm to the official or to any person residing at the official's home address. Authorizes an official whose home address or telephone number is solicited, sold, or traded in violation of this prohibition to bring an action in court and provides that they can get specified damages. (Gov. Code § 7928.230.)

4) Prohibits a state or local agency from publicly posting the home address, telephone number, or both the name and assessor parcel number of any elected or appointed official on the internet without first obtaining the written permission of that individual. (Gov. Code § 7928.205.)

5) Defines an "elected or appointed official" to include, but not be limited to, all of the following:
    a) A state constitutional officer.
    b) A Member of the Legislature.
    c) A judge or court commissioner.
    d) A district attorney.
    e) A public defender.

f) A member of a city council.
g) A member of a board of supervisors.
h) An appointee of the Governor.
i) An appointee of the Legislature.
j) A mayor.
k) A city attorney.
l) A police chief or sheriff.
m) A public safety official.
n) A state administrative law judge.
o) A federal judge or federal defender.
p) A member of the United States Congress or appointee of the President of the United States.
q) A judge of a federally recognized Indian tribe. (Gov. Code §§ 7920.500.)

6) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the California Consumer Privacy Act (CCPA) and creates the California Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code §§ 798.100 et seq.; Proposition 24 (2020).)

7) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

8) Provides that a business or service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business or service provider to maintain the consumer's personal information in order to do certain things, including to comply with a legal obligation. (Civ. Code § 1798.105(d).)

9) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting or selling personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

10) Provides consumers the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer the following:
    a) the categories of personal information that the business collected about the consumer;
    b) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
    c) the categories of personal information that the business disclosed about the consumer for a business purpose. (Civ. Code § 1798.115.)

11) Provides a consumer the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold or shared and that consumers have the right to opt out of the sale or sharing of their personal information. (Civ. Code § 1798.120.)

12) Provides that these provisions do not restrict a business' ability to collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information. (Civ. Code § 1798.145(a)(6).)

13) Defines "personal information" 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 biometric information, geolocation data, and "sensitive personal information." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

14) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information such as genetic data and the processing of biometric information for the purpose of uniquely identifying a consumer. (Civ. Code § 1798.140(ae).)

15) Provides various exemptions from the obligations imposed by the CCPA, including where they would restrict a business' ability to comply with federal, state, or local laws. (Civ. Code § 1798.145.)

16) Requires a business, on or before January 31 following each year in which it meets the definition of a data broker, to register with the PPA, as provided. (Civ. Code § 1798.99.82.)

17) Defines "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, except as specified.
    a) Aligns the definitions of "business," "personal information," "sale," "collect," "consumer," and "third party" with those in the CCPA. (Civ. Code § 1798.99.80.)

18) Requires data brokers to provide to the PPA, and the PPA to include on its website, the name of the data broker and its primary physical address, email, and website. Data brokers may, at their discretion, also provide additional information concerning their data collection practices. (Civ. Code §§ 1798.99.82, 1798.99.84.)

19) Requires the PPA to establish an accessible deletion mechanism, as provided, that allows consumers, through a single request, to request all data brokers to delete any personal information related to the consumer, as specified. Data brokers are required to regularly access the mechanism and process requests for deletion, as specified. (Civ. Code § 1798.99.86.)

20) Provides that after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant hereto, the data broker must delete all personal information of the consumer, except as provided, beginning August 1, 2026. After a consumer has submitted a deletion request and a data broker has deleted the consumer's data, the data broker shall not sell or share new personal information of the consumer unless the consumer requests otherwise or the selling or sharing is otherwise permitted, as provided. (*Id*. at subd. (c)-(d).)
    a) Requires data brokers to undergo audits every three years to determine compliance with the data broker registry law beginning January 1, 2028. (*Id*. at subd. (e).)

This bill:

1) Defines the following terms:
    a) "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, nonprofit entity, or other legal entity that collects individuals' personal information, or on the behalf of which that information is collected, and that alone, or jointly with others, determines the purposes and means of the processing of personal information and does business in the state.
    b) "Governmental entity" means a state or local agency, including, but not limited to, a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission, or any individual acting or purporting to act for or on behalf of a state or local agency.
    c) "Personal information" means any of the following:
        i. A residential address.

ii. A personal email address.
iii. A personal telephone number.
iv. A driver's license number.
v. A passport number.
vi. Geolocation data.
vii. A license plate number or unique identifier of a vehicle.
viii. A birth, marital, or divorce record.
ix. A child, spouse, parent, or sibling's name.
x. A school or daycare.
xi. A place of worship.
xii. A place of employment.

d) "Personal information" does not include:
   i. Information that has been publicly disclosed with the informed consent of the protected individual.
   ii. Information that is relevant to, and displayed as part of, a news story, commentary, editorial, or any other speech on a matter of public concern.
   iii. Information that is required by law to be made publicly available by a governmental entity.

e) "Protected individual" means any of the following:
   i. A current or former representative elected in the state, as determined by the Secretary of State.
   ii. An appointed officer of a court or a magistrate in the state.
   iii. A spouse, a child, or a dependent who resides in the same household as an individual described in (i) or (ii).

f) "Sell" means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a protected individual's personal information to a third party for monetary or other valuable consideration.

2) Authorizes a protected individual, or the PPA on behalf of a protected individual, to request a business to do either of the following:
   a) refrain from selling the protected individual's personal information; and
   b) delete the protected individual's personal information.

3) Requires, on receipt of a request under (2), above, a business to delete the personal information within 72 hours of receiving the request.

4) Requires the PPA to obtain a list of all state and local elected officials that includes their contact information. Requires the Judicial Council to provide the PPA with a list of all California judges that includes their contact information.

5) Requires the PPA to submit a request on behalf of any elected official or judge to any registered data broker to delete the personal information of those individuals upon receipt of the lists described in 4), above.

6) Authorizes a protected individual to provide a list of businesses that they want the PPA to request deletion of their personal information or any other deletion request. Requires the PPA to provide an elected official or judge with a notice regarding the process for requesting the deletion of the personal information of that individual's family members and the process for requesting assistance with requesting the deletion of personal information from a business that is not a registered data broker.

7) Authorizes a representative to request a governmental entity to do the following:
    a) refrain from publishing the protected individual's personal information; and
    b) remove the protected individual's personal information from any existing publication.

8) Requires a governmental entity to promptly acknowledge receipt of the request in writing by certified mail or by email and do both of the following:
    a) take steps reasonably necessary to ensure that the personal information is not published; and
    b) if the personal information is already published, remove the personal information within 72 hours after receipt of the request.

9) Prohibits a business from knowingly selling the personal information of a protected individual if both of the following are true:
    a) the business knows, or reasonably should know, that selling the personal information poses an imminent and serious threat to the protected individual; and
    b) the selling of the personal information results in an assault in any degree, harassment, trespass, or malicious destruction of property.

10) Provides that a person who violates 9), above, is subject to a civil penalty not exceeding $5,000 in an action brought only by the Attorney General.

11) A protected individual, the Attorney General, a county counsel, or a city attorney may bring an action for a violation of 2)-3), above, and 8), above, for any of the following:
    a) declaratory relief;
    b) injunctive relief;
    c) reasonable attorney's fees; and
    d) actual damages.

12) If a court finds, in an action under 11), above, that a business or governmental entity willfully refused to provide for the removal of personal information knowing that

the individual on behalf of whom the request was made was a protected individual, the court may award punitive damages.

COMMENTS

1. Stated need for the bill

The author writes:

> On June 14th, a gunman entered the home of two Minnesota lawmakers, killing House Speaker Emerita Melissa Hortman, her husband Mark Hortman and wounding State Senator John Hoffman and Yvette Hoffman. After the alleged shooter was apprehended, law enforcement found notes listing the names of dozens of Minnesota State and federal elected officials along with their home addresses. Along with the names and addresses was a list of search platforms used for finding home addresses and other personal information. Sites like these and the broader data broker industry have made nearly all personal information available with a few clocks of a button.
>
> With the rising political violence in our country, elected officials are particularly at risk given the public nature of their roles. At a time when democratic representation is more important than ever, we must ensure that as elected representatives, we can keep your selves and our families safe. AB 302 authorizes an elected official and members of their family to request that a company or government entity stop publishing or selling personal information. This bill strengthens privacy protections, ensuring that all elected representatives are safe to serve their communities.

2. Intimidation and threats against elected officeholders and public officials is on the rise

A report published by the Combating Terrorism Center at West Point found that threats against public officials have steadily increased since 2017, which corresponds with an increase in polarization in this country since the 2016 presidential election.[2] The report found that in 2013-2016 there were an average of 38 federal charges per year, but that number almost doubled during 2017-2022. Several high profile incidents have occurred against federal officials. In 2017, U.S. Representative Steve Scalise was shot at a congressional baseball practice. There was the January 6 insurrection at the Capitol and the hammer attack on U.S. Representative Nancy Pelosi's husband in their home. The California Legislature has also had its fair share of violent incidents. In late August of

[2] Pete Simi, et. al, *Rising Threats to Public Officials: A Review of 10 Years of Federal Data*, Vol. 17, Issue 5, (May 2024), available at https://ctc.westpoint.edu/rising-threats-to-public-officials-a-review-of-10-years-of-federal-data/.

2019, former Senator Richard Pan was shoved by an anti-vaccine activist who was videotaping Senator Pan while walking in downtown Sacramento.[3]
A little over a month ago, two Minnesota legislators—Senator John Hoffman and Representative Melissa Hortman— were shot in their homes. Senator Hoffman and his wife Yvette survived the attack, but were hospitalized for needed medical care. Representative Hortman and her husband Mark succumbed to their injuries. The suspect was apprehended and faces federal and state murder charges. Minnesota Governor Tim Walz called the shooting an "act of targeted political violence."[4] Court documents in the case show that the suspect used "online people search services to find the home addresses of his intended targets. Police found the names of 11 registered data brokers—or companies that gather and sell people's information, including addresses, emails and phone numbers—in [the suspect's] abandoned car after the shootings. Police also found a list of dozens of state and federal lawmakers, and their addresses, according to the criminal complaint."[5] On the last night of the 2019 legislative session, the Senate had to shut down for several hours after a protestor in the Senate Gallery "threw a feminine hygiene device containing what appeared to be blood onto the Senate floor."[6]

A 2024 report from the Brennan Center for Justice that conducted surveys in October 2023 from over 1,700 local and state elected officials from all 50 state and across ages, party affiliations, ideologies, genders, sexual orientations, racial and ethnic identities, and religions found alarming rates of threats against elected officials. The report highlights:

> Officeholders across these demographic categories reported experiencing threats or attacks within the past three years. And the volume and severity of abuse have increased in recent years, they said. More than 40 percent of state legislators experienced threats or attacks within the past three years, and more than 18 percent of local officeholders experienced threats or attacks within the past year and a half. The numbers balloon to 89 percent of state legislators and 52 percent of local

---

[3] KCRA Staff, '*I don't regret pushing him': Man cited for shoving California state senator*, KCRA News, (Aud. 22, 2019), available at https://www.kcra.com/article/california-state-senator-richard-pan-assault/28777200.
[4] Meg Anderson & Avie Schneider, *Suspect named in targeted shootings of Minnesota lawmakers*, NPR, (Jun. 14, 2025), available at https://www.npr.org/2025/06/14/nx-s1-5433645/minnesota-state-legislators-lawmaker-shootings.
[5] Alfred Ng, *Alleged shooter found Minnesota lawmakers' addresses online, court docs say*, Politico, (Jun. 16, 2025, available at https://www.politico.com/news/2025/06/16/alleged-shooter-found-minnesota-lawmakers-addresses-online-court-docs-say-00409260.
[6] Angela Hart & Colby Bermel, *Protester throws apparent blood at legislators, shutting down California Senate*, Politico, (Sept. 13, 2019), available at https://www.politico.com/states/california/story/2019/09/13/protester-throws-red-liquid-at-legislators-shutting-down-california-senate-1188537.

officeholders when less severe forms of abuse — insults or harassment such as stalking — are included.[7]

A report conducted by the Joan B. Kroc School of Peace Studies at the University of San Diego that focused on local elected officials in San Diego, Riverside, and Imperial Counties found:

- 66% of all elected officials reported being on the receiving end of threats and harassment.
- 69% of women report experiencing threats and harassment monthly, compared to 38% of their male counterparts.
- 83% of respondents said that threats and harassment are a major issue that require a public response.
- 46% of women and 39% of men have considered leaving public service as a direct result of the threats and harassment they have experienced.[8]

As the Brennan Center for Justice Report explains, "threats and attacks [on elected officials] constrain how freely officeholders interact with constituents, narrow the spectrum of policy positions they feel safe to support, and make them less willing to continue in public service. Unaddressed, the problem stands to endanger not just individual politicians but, more broadly, the free and fair functioning of representative democracy — at every level of government."[9]

3. <u>This bill seeks to provide enhanced protections for elected officials and judicial officers and their family</u>

The bill is intended to provide enhanced protections for elected officials and judicial officers by requiring the PPA to make deletion requests of personal information for a protected individual to a registered data broker. The bill also authorizes a protected individual or the PPA, on behalf of the protected individual, to request a business to do either of the following: a) refrain from selling the protected individual's personal information; and b) delete the protected individual's personal information. The bill requires a business to delete the personal information within 72 hours of receiving the request, or the business is subject to a civil cause of action brought by a protected individual, the AG, or other public prosecutors. Business under the bill is defined very broadly, more broadly than under the CCPA, and includes nonprofits.

---

[7] *Intimidation of State and Local Officeholders*, Brennan Center for Justice, (Jan. 25, 2024), available at https://www.brennancenter.org/our-work/research-reports/intimidation-state-and-local-officeholders.
[8] *Assessing Threats and Harassment Towards Locally Elected Officials*, Joan B. Kroc School of Peace Studies, University of San Diego, available at https://www.sandiego.edu/peace/institute-for-peace-justice/violence-inequality-power-lab/san-diego-threats.php.
[9] *Intimidation of State and Local Officeholders*, Brennan Center for Justice, (Jan, 25, 2024), available at https://www.brennancenter.org/our-work/research-reports/intimidation-state-and-local-officeholders.

Under the bill, the PPA is required to obtain a list of all state and local elected officials that includes their contact information. The bill does not specify how the PPA will obtain this information, nor does it authorize this information to be shared by either the Secretary of State or local election officials with the PPA. Additionally, the bill requires the Judicial Council to provide the PPA a list of all California judges that includes their contact information, and provide an updated list after the appointment or election of any additional judge. The bill does not provide any confidentiality provisions to the list either obtained by the PPA or provided by the Judicial Council. Additionally the bill does not provide for consent of a protected individual to have their information sent or not sent to the PPA.

The bill provides civil liability for a business that knowingly sells the personal information of a protected individual if both of the following are true:

- the business knows, or reasonably should know, that selling the personal information poses an imminent and serious threat to the protected individual; and
- the selling of the personal information results in an assault in any degree, harassment, trespass, or malicious destruction of property.

A governmental entity is also subject to the provisions of the bill and must refrain from publishing a protected individuals personal information and remove their information from any existing publication upon a request from the protected individual or their authorized representative. A request must be made in writing by certified mail or email. Upon receipt of a request, the governmental entity must take steps to ensure the information is not published and, if already published, remove it within 72 hours. A government entity that does not comply is subject to a civil action brought by brought by a protected individual, the AG, or other public prosecutors. "Government entity" is defined as a state or local agency, including, but not limited to, a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission, or any individual acting or purporting to act for or on behalf of a state or local agency. This definition does not seem to encompass the Legislature. The mechanism for submitting a request under this provision lacks guardrails. First, there is no requirement for the governmental entity to verify that the requester is a protected individual. Additionally, simply allowing any government employee to receive an email and that triggering a 72-hour timeline to remove personal information is problematic. Existing law already prohibits a state or local agency from publicly posting the home address, telephone number, or both the name and assessor parcel number of any elected or appointed official on the internet without first obtaining the written permission of that individual. (Gov. Code § 7928.205.) There is no liability attached to this existing provision of law.

4. This bill raises First Amendment issues

a. First Amendment jurisprudence

The federal and state Constitutions prohibit the government from abridging the freedom of speech and the right to peaceably assemble.[10] "The vitality of civil and political institutions in our society depends on free discussion…it is only through free debate and free exchange of ideas that government remains responsive to the will of the people and peaceful change is effective. The right to promote diversity of ideas and programs is therefore one of the chief distinctions that sets us apart from totalitarian regimes."[11] And "[i]f there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[12]

Although the First Amendment's speech guarantee is written as an absolute, there are certain narrow categories of speech that fall outside of the First Amendment's protections.[13] Relevant to this analysis, these categories include:

- "True threats" of violence: "[w]hen a reasonable person would foresee that the context and import of the words will cause the listener to believe he or she will be subjected to physical violence, the threat falls outside First Amendment protection."[14] While the rationale behind the true threats doctrine is based on the harm to the listener—"[t]rue threats subject individuals to 'fear of violence' and to the many kinds of 'disruption that fear engenders' "—the Court recently held that "the First Amendment precludes punishment, whether civil or criminal, unless the speaker's words were 'intended' (not just likely) to produce imminent disorder."[15]
- Inciting imminent lawless action: a state may "forbid advocacy of the use of force or of law violation" "where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[16] The "mere abstract teaching of the moral propriety or even moral necessity for a resort to force and violence, is not the same as preparing a group for violent action and steeling it to such action."[17]

[10] U.S. Const., 1st & 14th Amends.; Cal. Const., art. I, §§ 2, 3.
[11] *Terminiello v. City of Chicago* (1949) 337 U.S. 1, 4 (1949) (*Terminiello*).
[12] *Texas v. Johnson* (1989) 491 U.S. 397, 414 (*Johnson*).
[13] *Counterman v. Colorado* (2023) 600 U.S. 66, 73.
[14] *In re M.S.* (1995) 10 Cal.4th 698, 711.
[15] *Counterman*, *supra*, 600 U.S. at pp. 74, 76.
[16] *Brandenburg v. Ohio* (1969) 395 U.S. 444, 447 (*Brandenburg*).
[17] *Id.* at p. 448 (cleaned up).

These doctrines have been used to uphold state laws criminalizing false bomb threats;[18] hate speech, where the speech itself threatened violence and the speaker had the apparent ability to carry out the threat;[19] and other threats that cause the listener to believe they will be subjected to physical violence.[20]

"First Amendment freedoms need breathing space to survive."[21] "The threat of sanctions may deter their exercise almost as potently as the actual application of sanctions,"[22] because people will necessarily give a wide berth to any speech that might run afoul of the law—which leads to the chilling of legitimate speech.[23] As a result, prohibitions on matters that closely touch on First Amendment-protected activities must be both so clear as to clearly inform individuals as to what conduct is proscribed and so precise so as not to sweep in protected conduct.[24]

b. Prior similar statute was held in violation of the First Amendment

Under the California Public Rerecords Act a statute was enacted to prohibit a person, business, or association from publicly posting or publicly displaying on the internet the home address or telephone number of any elected or appointed official if that official has, either directly or through an agent, made a written demand of that person, business, or association to not disclose the official's home address or telephone number. (Gov. Code § 7928.215(b); previously Gov. Code § 6254.21(c)(1).)[25] In 2017, this statute was challenged on several grounds, including that it violates the First Amendment of the U.S. Constitution. (*Publius v. Boyer-Vine* (E.D. Cal. 2017) 237 F.Supp.3d 997.) In *Publius*, the plaintiff, maintained a political blog and in response to the Legislature enacting gun control legislation posted the names, home addresses and phone numbers of all Legislators who voted for the legislation. (*Id*. at 1004.) The legislation in question required the creation of a database that would contain the driver's license, residential address, telephone number, and date of birth of anyone who purchased or transferred ammunition in California. (*Id*. at 1003-04.) Shortly after the plaintiff posted the Legislator's personally identifying information, members of the Legislature received threatening phone calls and social media messages. (*Id.* at 1004-05.) Representatives for the Legislature sent a written demand seeking the immediate take down of the posted information and WordPress, the blogging platform, immediately removed the blog entry. (*Id*. at 1005-06.)

---

[18] *In re J.M.* (36 Cal.App.5th 668, 677-679 (speech was a true threat that fell outside First Amendment protections).
[19] *In re M.S.*, *supra*, 10 Cal.4th at pp. 714-715.
[20] *People v. Toledo* (2001) 26 Cal.4th 221, 223.
[21] *National Ass'n for the Advancement of Colored People v. Button* (1963) 371 U.S. 415, 433 (*Button*).
[22] *Ibid.*
[23] *Keyishian v. Bd. of Regents of University of State of N.Y.* (1967) 385 U.S. 589, 604.
[24] *Button*, *supra*, 371 U.S. at p. 433.
[25] In 2021 the CPRA was recodified by AB 473 (Chow, Ch. 614, Stats. 2021). Prior to the recodification, the equivalent to Section 7928.215 of the Government Code was Section 6254.21(c)(1) of that code. As such, the *Plubius* case refers to Section 6254.21(c)(1) throughout.

The plaintiff brought a suit alleging several causes, including that the statute violated the First Amendment of the U.S. Constitution. The basis for enacting this provision was to protect the personal safety of covered officials and their families, which is a state interest of the highest order; however, a federal district court held that the statute violated the First Amendment's overbreadth doctrine. (*Id*. at 1019.) The district court found that the statute was not narrowly tailored; and that is was both overinclusive because it prohibited publication of the information, regardless of whether the information was widely available to the public or had previously been disclosed, and underinclusive because it irrationally punished just publication on the internet but did not address other forms of publication, such as in newspapers. (*Id*. at 1020.)
This bill raises the same issues as highlighted in the *Plubius* case above. In fact, AB 1521, the Assembly Judiciary Committee civil law omnibus bill, is removing the preempted statute in the CPRA form the codes specifically because it has been found to be unconstitutional. Under this bill, a protected individual can request a business delete their personal information, subject to civil penalties for noncompliance. The term delete is not defined under the bill. Merriam Webster's dictionary defines it as "to eliminate especially by blotting out, cutting out, or erasing."[26] Under the plain meaning of this statute a business would be required to erase or remove and personal information, whether from the internet or other publication, document, or writing. Some of the information included under the definition of "personal information" in the bill is a public record or readily accessible otherwise, such as birth, marital, and divorce records. Additionally, as demonstrated by the *Plubius* case, a statute that prohibits publication of information, regardless of whether the information was widely available to the public or had previously been disclosed, makes a statute overbroad and violative of the First Amendment. The author has noted that this bill was modeled off Daniel's Law form New Jersey, which did survive a challenge at the New Jersey Supreme Court, but is currently being challenge on First Amendment grounds in the U.S. 3rd Circuit Court of Appeals.

c. Prior restraint

Concerns have been raised to the Committee that the fact a court could order a business to remove information under the bill essentially allows courts to issue a censorship order, which could be considered a prior restraint on speech. The courts are highly suspect of prior restraints and they bear "a heavy presumption against its constitutional validity."[27] Additionally, allowing an elected official to require that their place of employment not be provided to the public may raise concerns that this is infringing on a person's right to petition the government under the First Amendment.

[26] Definition of "Delete", Merriam Webster, available at https://www.merriam-webster.com/dictionary/delete.
[27] *Epona v. County of Ventura* (9th Cir. 2017) 876 F.3d 1214, 1222.

5. Section 230 and federal preemption issues

Section 230 of the Communications Decency Act, also known as Section 230, was enacted in 1996. Designed to prevent burgeoning internet sites from being liable for material posted by users, Section 230 (1) prohibits a website from being treated as the publisher or speaker of information provided by users, and (2) clarifies that, if a website engages in content moderation of objectionable content, it does not lose its protection under (1). Section 230 expressly preempts state law, stating that "[n]o cause of action may be brought and no liability may be imposed under any State law that is inconsistent with this section."

This provision has been hailed as the law that created the modern internet, fostering free expression online and allowing an array of innovative services and spaces to flourish, from search engines to social media.[28] To summarize:

> For a statute that has caused so much confusion, the basic idea behind § 230 is simple. Generally speaking, the law shields websites from being held legally responsible for content that others post—a protection not available for print material or television broadcasts. If I post something defamatory about you on Twitter, for example, you can sue me, but you can't sue Twitter.
> . . .
> In brief, as courts have interpreted the law, § 230 (c)(1) protects platforms from civil liability for leaving content up; § 230 (c)(2) protects them if they choose to take content down.[29]

Relevant here, Section 230 not only provides protection against federal civil claims, but it also protects against litigation "under any State or local law that is inconsistent with this section." This preemptive effect has kept states from meaningfully regulating in this space, absolving platforms of responsibility for virtually all third-party harms arising from the use of their services. Some advocates have argued that the bill could violate Section 230 if it places liability on a platform for not deleting information that it did not post.

6. Proposed Author Amendments

In light of the issues raised above, the author has proposed to amend the bill to remove all provisions related to businesses and governmental entities and instead require the PPA to upload an elected official's or a judge's information into the accessible deletion mechanism. The bill would amend the data broker registry statutes to require the PPA to obtain a list of all state and local elected officials, which is to serve as the elected official's request to delete their information under the accessible deletion mechanism.

---

[28] *See e.g.*, Kosseff, *The Twenty-Six Words that Created the Internet* (2019).
[29] Quinta Jurecic, *The politics of Section 230 reform: Learning from FOSTA's mistakes* (Mar. 1, 2022) Brookings, https://www.brookings.edu/articles/the-politics-of-section-230-reform-learning-from-fostas-mistakes.

By placing this provision in the data broker registry law, all existing definitions, exceptions, and understandings of what personal information entails will apply.

The proposed amendments require the list obtained by the PPA to include the elected official's name and profile data as defined by the PPA. The PPA is required allow an elected official the opportunity to be removed from the list. The bill requires the Judicial Council to also provide a list to the PPA of judges and their information, and provide an opportunity to remove their name from the list before submitting it.

After receipt of the lists described above, the PPA is required to upload the lists to the accessible deletion mechanism the PPA is required to establish by January 1, 2026. (*see* Civ. Code § 1798.99.86.) Under the proposed amendments, an entity receiving a notification that deletion is required must do so within five days beginning August 1,2026, which is when existing law currently requires a data broker to delete information of a person registered on the accessible deletion mechanism. (*see* Civ. Code § 1798.99.86(d).) The proposed amendments authorize an elected official or judge, the Attorney General, a county counsel, or a city attorney to bring an action for a violation for any of the following relief: declaratory relief; injunctive relief; reasonable attorney's fees; and actual damages. For a willful refusal to delete, punitive damages can be awarded.

Lastly, the proposed amendments provide that all information sharing is to be a secure and confidential exchange, and that the lists and the information contained therein are confidential and subject to disclosure under the California Public Records Acts. California generally recognizes that public access to information concerning the conduct of the people's business is a fundamental and necessary right. At the same time, the state recognizes that this right must be balanced against the right to privacy. The general right of access to public records may, therefore, be limited where the Legislature finds a public policy reason necessitating the limit on access. In light of the purpose of this bill, it seems imminently reasonable to ensure that the lists and the information in the lists are not public records and are kept confidential and exchanged in a confidential manner.

A mock-up of the proposed amendments can be found at the end of this analysis.

7. <u>Statements in opposition</u>

The First Amendment Coalition and Freedom of the Press Foundation write in opposition, stating:

> […] AB 302 runs up against the protections of the First Amendment because it directly prohibits speech based on its content.

The Supreme Court has said that " state action to punish the publication of truthful information seldom can satisfy constitutional standards." "More specifically, [the Supreme Court] has repeatedly held that 'if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order.'" Any such law must also be narrowly tailored, meaning it is "the least restrictive means to further a compelling interest."

In addition, the Supreme Court has held that "[c]ontent-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." As the Court recently confirmed, this strict scrutiny for content-based laws "is fatal in fact absent truly extraordinary circumstances." Free Speech Coal., Inc. v. Paxton, No. 23-1122, 2025 U.S. LEXIS 2497, at *25 (Jun. 27, 2025).

Under the First Amendment, the Supreme Court has repeatedly prohibited attempts to bar or punish the publication of truthful information on matters of public concern, including when privacy interests are at stake. In Cox Broadcasting v. Cohn, for instance, the Court held that the First Amendment barred holding a newspaper civilly liable under a state statute that made it a crime to publish the name of a rape victim in order to protect the privacy of the victim and the victim's family, citing the risk of "self-censorship" and likely "suppression of many items that would otherwise be published and that should be made available to the public."20

In addition, a federal court in California has held that a state law that restricted publishing the home addresses and telephone numbers of certain California government officials was likely unconstitutional. In Publius v. Boyer-Vine, the Eastern District of California held that California Government Code § 6254.21(c) was a content-based restriction on speech and was not narrowly tailored in part because it made "no attempt to prohibit or prevent true threats" and because it did not "differentiate between acts that 'make public' previously private information and those that 'make public' information that is already publicly available."21 (This statute is being repealed in AB 1521, the Assembly Judiciary Committee's Omnibus bill.)

Although it contains an ostensible carveout for speech of public concern, AB 302 is not narrowly tailored under strict scrutiny because it is not limited to attempting to prohibit or prevent true threats. While Section 3273.79 appears to be aimed at prohibiting the sale of personal information that poses an imminent and serious threat to an individual and results in certain specified harms, the rest of the bill is not so limited. For instance, Section 3273.76 applies regardless of whether the personal information could contribute to a true threat or result in harm to a protected individual.

> To the extent that AB 302 applies to personal information that has previously been made publicly available, it is not narrowly tailored. It is also not narrowly tailored because it prohibits publication of information that is not normally considered private, such as place of employment. […]

A coalition of business organizations, including the California Chamber of Commerce and TechNet, write in opposition unless amended, stating:

> As drafted, AB 302 would prohibit businesses from retaining information solely used for security and integrity purposes, such as fraud prevention and consumer protection. The bill also does not include necessary exceptions for federally regulated transactions under the Gramm-Leach-Bliley Act (GLBA), Driver's Privacy Protection Act (DPPA), Fair Credit Reporting Act (FCRA), and Health Insurance Portability and Accountability Act (HIPAA). These transactions are non-public facing and are critical for identity verification, fraud detection, and other essential services.
>
> Personal information is routinely exchanged between businesses to fulfill contractual obligations and comply with existing regulatory requirements. These exchanges do not risk public exposure of data and include use cases such as validating identity for financial transactions or accessing government benefits. For example, information collected and processed under the FCRA or GLBA is necessary to meet legal requirements and ensure system integrity.
>
> While we recognize the highly visible and sensitive nature of serving in public office, elected officials and appointed court officers, like all individuals, participate in financial and economic activities that require lawful data transfers—such as paying taxes, purchasing homes, or verifying insurance claims. Prohibiting the sale or transfer of such information, even when done in compliance with federal law, would disrupt essential services and economic participation.
>
> Additionally, requiring the deletion of records used solely for verification and fraud prevention within 72 hours of a request could degrade our members' ability to communicate with their customers and clients. Without narrowly tailored exceptions, this bill risks unintended harm to both consumers and the businesses that serve them. […]

SUPPORT

None received

OPPOSITION

California Chamber of Commerce
California Association of Realtors

California Chamber of Commerce
California Land Title Association
Computer & Communications Industry Association
Computer and Communications Industry Association
First Amendment Coalition
Freedom of the Press Foundation
State Privacy and Security Coalition
TechCA
TechNet
Technology Industry Association of California

RELATED LEGISLATION

Pending Legislation:

AB 789 (Bonta, 2025) allows candidates for office and elected officials to use unlimited amounts of campaign funds for security purposes until January 1, 2029, and $10,000 per year thereafter. AB 789 is set to be heard in the Senate Elections and Constitutional Amendment Committee on the same day as this bill.

AB 1392 (Sharp-Collins, 2025) exempts the residence address, telephone number, and email address of a federal, state, or local elected official or candidate for an elected federal, state, or local office from being disclosed on voter rolls, as specified. AB 1392 is set to be heard in this Committee on the same day as this bill.

Prior Legislation:

SB 362 (Becker, Ch. 709, Stats. 2023), among other things, required the PPA establish an accessible deletion mechanism, as provided, that allows consumers, through a single request, to request all data brokers to delete any personal information related to the consumer, as specified.

AB 1202 (Chau, Ch. 753, Stats. 2019) established California's data broker registry.

PRIOR VOTES

Assembly Floor (Ayes 56, Noes 11)
Assembly Appropriations Committee (Ayes 11, Noes 4)
Assembly Judiciary Committee (Ayes 9, Noes 3)
Assembly Health Committee (Ayes 12, Noes 2)
****

MOCK-UP OF PROPOSED AUTHOR AMENDMENTS[30]

The proposed author amendments would delete the current contents of the bill and instead add a new Section to Title 1.81.48 of the Civil Code, which will read as provided under Amendment 1.

Amendment 1

(a) (1) On or before March 1, 2026, the California Privacy Protection Agency shall obtain a list of all state and local elected officials, which shall serve as the elected official's request to delete their information pursuant to Section 1798.99.86(b)(1). The list shall include the elected official's name and profile data as defined by the California Privacy Protection Agency.

(2) The California Privacy Protection Agency shall provide an elected official an opportunity to request that their name and information be removed from the list.

(3) Following the certification of a final election, the California Privacy Protection Agency shall obtain a list of elected officials as provided under paragraph (1) and (2).

(b) (1) The Judicial Council shall provide the California Privacy Protection Agency with a list of all California judges, which shall serve as the judge's request to delete their information pursuant to Section 1798.99.86(b)(1). The list shall include the judge's name and other profile data as defined by the California Privacy Protection Agency that has been shared voluntarily by the judges.

(2) Prior to providing the list to the California Privacy Protection Agency, the Judicial Council shall provide the judge an opportunity to request that their name and information be removed from the list. The list submitted to the California Privacy Protection Agency shall only include those judges that did not request to be removed from the list.

(3) The Judicial Council shall provide an updated list after the appointment or election of any additional judge.

(c) (1) After receipt of the lists required by this section, the California Privacy Protection Agency shall upload the lists required by this section to the accessible deletion mechanism established pursuant to Section 1798.99.86.

(2) Beginning August 1, 2026, entities receiving a notification that such a deletion is required, shall do so within five days.

[30] The amendments may also include technical, nonsubstantive changes recommended by the Office of Legislative Counsel as well as the addition of co-authors.

d) All information sharing in this section shall be a secure and confidential exchange. The lists and the information in the lists shall be confidential and not subject to disclosure under the California Public Records Act (commencing with Section 7920.000 of the Government Code).

(e) An elected official or judge who is on the list described in subdivision (a) or (b), the Attorney General, a county counsel, or a city attorney may bring an action for a violation of this section for any of the following relief:

(1) Declaratory relief.

(2) Injunctive relief.

(3) Reasonable attorney's fees.

(4) Actual damages.

(b) In addition to the other relief provided under this section, if a court finds that an entity willfully refused to provide for deletion as required under this section, the court may award punitive damages.

Amendment 2

The Legislature finds and declares that Section 1 of this act imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

In order to protect the confidential and private information of an elected official or judge, it is necessary that this act limit the public's right of access to that information.