

Date of Hearing: January 13, 2026

Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Rebecca Bauer-Kahan, Chair

AB 883 (Lowenthal) – As Amended January 7, 2026

SUBJECT: Elected officials and judges.

SYNOPSIS

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 families. The individual indicted for the murders allegedly was in possession of a list of more than 45 state and federal Minnesota officials' addresses that came from data brokers and was obtained by the individual using "people search" websites. In response to this event and the growing number of threats faced by public officials, this bill seeks to provide enhanced protections to elected officials and judges. Toward that end, the bill requires the California Privacy Protection Agency (CalPrivacy) to upload to the data broker deletion system lists of protected individuals and their personal information, which are provided by the Secretary of State and the Judicial Council. Data brokers are then required to delete the personal information for these individuals within five days.

Data brokers are businesses that purchase information about us from multiple sources, combine this information to build comprehensive datasets about us and our lives, and offer this information for sale to anyone able to pay for it. The key point to understand is that no consumer chooses to have a relationship with a data broker. The consumer is not involved in the sale or transfer of their personal information to data brokers, nor do they benefit from that transaction.

This bill is substantially similar to AB 302 (Bauer-Kahan), a two-year bill currently in the Senate Appropriations Committee, and is supported by Californians for Consumer Privacy. TechNet and the California Chamber of Commerce have an "oppose unless amended" position.

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 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 Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)
- 7) Defines "personal information" under 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. Personal information includes such information as:
 - i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.
 - ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
 - iii) Biometric information.

- iv) Internet activity information, including browsing history and search history.
 - v) Geolocation data.
 - vi) Audio, electronic, visual, thermal, olfactory, or similar information.
 - vii) Professional or employment-related information. (Civ. Code § 1798.140(v).)
- 8) Exempts from the definition of “personal information” publicly available information or lawfully obtained, truthful information that is a matter of public concern.
- 9) Defines “publicly available” as any of the following:
- a) Information that is lawfully made available from federal, state, or local government records.
 - b) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.
 - c) Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. (Civ. Code § 1798.140(v)(D)(2).)
- 10) 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 Privacy Agency, as provided. (Civ. Code § 1798.99.82.)
- 11) 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. The definition specifically excludes the following:
- a) An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.).
 - b) An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.
 - c) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act, Insurance Code § 1791 et seq. (Civ. Code § 1798.99.80.)
- 12) Aligns the definitions of “business,” “personal information,” “sale,” “collect,” “consumer,” and “third party” with those in the Privacy Agency. (Civ. Code § 1798.99.80.)
- 13) Requires data brokers to provide, and the Privacy Agency to include on its website, the name of the data broker and its primary physical, email, and website addresses as well as various other disclosures, including whether the broker collects consumers’ precise geolocation or reproductive health care data and whether they collect the personal information of minors. Data brokers may, at their discretion, also provide additional information concerning their data collection practices. (Civ. Code §§ 1798.99.82, 1798.99.84.)

- 14) Subjects a data broker that fails to register as required to administrative fines and costs to be recovered in an administrative action brought by the Privacy Agency. (Civ. Code § 1798.99.82.)
- 15) Requires the Privacy Agency 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.)
- 16) 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 of the information is otherwise permitted, as provided. Requires data brokers to undergo audits every three years to determine compliance with the data broker registry law. (Civ. Code § 1798.99.86.)

THIS BILL:

- 1) Requires the Secretary of State to provide CalPrivacy a list of all state and local officials that includes the officials' personal information and must be updated after each subsequent election.
- 2) Requires CalPrivacy to offer each elected official the opportunity to opt out of having their personal information removed from the deletion list.
- 3) Requires the Judicial Council to provide CalPrivacy a list of all California judges, which will serve as the judges' request to delete their personal information.
- 4) Requires CalPrivacy to upload the lists to the data broker deletion system and requires that the data brokers delete the personal information for that individual within five days.
- 5) Authorizes an elected official or judge who has requested deletion or a public attorney to bring a civil action for a violation of this statute.

COMMENTS:

- 1) **Author's statement.** According to the author:

California is on the cutting edge when designing laws to protect the privacy of individuals in the State. Over the last 5 years there have been documented examples of harassment, threats and even violence against elected officials in California and beyond. It is imperative that we continue to update our laws to ensure that elected and appointed officials' personal information is protected in a manner that protects the important principles of open government.

AB 883 makes various updates to the existing California Privacy Protection Agency to strengthen the ability for elected and appointed officials to protect their most personal

information when they are faced with a credible threat. Providing these tools to elected and appointed officials will help them reduce the exposure of sensitive information about themselves and their families, ensuring their safety when it is most critical.

2) The rise of political violence. On June 14, 2025, Vance Boelter, posing as a law enforcement officer, knocked on the door of Senator John Hoffman’s home and shot him and his wife, Yvette, over eight times. Boelter then drove to two other elected officials’ homes that were empty before arriving at Representative Melissa Hortman’s home, where he shot and killed her and her husband, Mark. Once arrested, Boelter was found with a list of 45 elected Minnesota officials, mostly Democrats who supported abortion rights.¹ The list containing these officials’ addresses allegedly came from data brokers and was obtained by Boelter using “people search” websites.²

Boelter’s night of terror was just the latest in a string of alarming, politically motivated violence against elected officials. On January 6th, 2021, thousands gathered outside the Capitol steps in Washington, D.C. to protest the 2020 election results in what would quickly turn into an all-out riot. Protesters broke into the Capitol, some armed with confiscated police batons and riot gear or firearms, where they faced off with over 100 Capitol police in efforts to reach elected officials who were holed up in the Senate Chamber.³ The January 6th insurrection, as it has come to be known, resulted in nearly \$3 million in damage and over 1,500 arrests, as well as several deaths of both protesters and Capitol police. U.S. Capitol Police Officer Stephen Sherman said of the event, “there’s a common thread of emotions amongst many officers who were defending the Capitol on January 6, 2021, which is that we all thought we were going to die.”⁴

Since the January 6th insurrection, threats of violence against elected officials have surged. In 2022, former House Speaker Nancy Pelosi’s home was broken into by a right-wing extremist who attacked her husband with a hammer. And several House Republicans claimed they experienced a barrage of threats and harassment in 2023 after voting against conservative Rep. Jim Jordan for speaker.⁵ A 2024 report from the Brennan Center for Justice surveyed over 1,700 officials from across the country and found that more than 40 percent of state legislators experienced threats or attacks from 2021-2024, and over half experienced harassment such as stalking.⁶ Officials who identify as women or people of color were more likely to experience threats and harassment related to their families, including threats against their children, than other officeholders. Women were also more likely to be deterred from running for reelection due

¹ Kevin Shalvey and Emily Shapiro, “Chilling details emerge in Minnesota shootings as Vance Boelter faces federal charges: ‘Stuff of nightmares.’” *ABC News* (June 16, 2025), <https://abcnews.go.com/US/minnesota-lawmakers-shooting-suspect-vance-boelter-due-court/story?id=122882740>

² Lily Hay Newman, “Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets’ Addresses.” *Wired* (June 16, 2025), <https://www.wired.com/story/minnesota-lawmaker-shootings-people-search-data-brokers/>.

³ “Jan. 6, 2021: A visual archive of the Capitol attack” NPR (Jan 4, 2026) <https://apps.npr.org/jan-6-archive/>

⁴ *United States v. ALBERTS*, 1:21-cr-00026. (D.D.C. Dec 28, 2023) ECF No. 190 <https://www.courtlistener.com/docket/53705217/190/united-states-v-alberts/> pg. 35

⁵ David Li and Mirna Alsharif, “David DePape, man who attacked Paul Pelosi with a hammer, sentenced to 30 years in prison” (May 17, 2024), <https://www.nbcnews.com/news/us-news/david-depape-man-attacked-paul-pelosi-hammer-sentenced-30-years-prison-rcna152614>; and Lauren Peller, Rachel Scott, and Benjamin Siegel, “Republicans who voted against Jordan for speaker say they’ve been threatened, harassed” *ABC News* (October 19, 2023) <https://abcnews.go.com/Politics/republicans-voted-jordan-speaker-threatened-harassed/story?id=104140363>

⁶ Gowri Ramachandran et al., *Intimidation of state and local officeholders* (Brennan Center for Justice, 2024), <https://www.brennancenter.org/our-work/research-reports/intimidation-state-and-local-officeholders>

to these threats than men (34 percent of men v. 48 percent of women), highlighting how political violence could significantly reshape California's legislative makeup⁷.

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 requires 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

Along with threatening the wellbeing of public servants, political violence has dramatically shifted the way that representatives engage with the public and controversial issues. Nearly 50 percent of state and local officials said that abuse made them less likely to engage with their constituents on social media and 20 percent of state legislators said that political violence has dissuaded them from voicing their opinions on controversial topics. Elected state and local officials are not alone in the barrage of threats. The Global Project Against Hate and Extremism reported an alarming 327 percent increase in instances of threats or calls for impeachment against judges between May 2024 and March 2025 on social media platforms.⁹ Thus, violence and intimidation of public servants has a dangerous cooling effect on the democratic process, leading to higher rates of attrition and lower rates of public engagement, especially for women and people of color, that will likely have lasting consequences on the democratic landscape if left unchecked.

3) Daniel's Law. In July 2020, Daniel Anderl was home from college celebrating his 20th birthday when he heard a knock at the door. The man on the other side, attorney Roy Den Hollander, was a self-proclaimed "anti-feminist" who posed as a FedEx employee to gain access to the home of Judge Esther Salas, Daniel's mother. Hollander had previously made disparaging comments about Judge Salas as a woman and Latina.¹⁰ When Daniel answered the door instead of his mother, Hollander raised a firearm and shot and killed Daniel in the entryway of the judge's home before fleeing, leaving Mark Anderl, Daniel's father, critically injured as well.

In response to the killing, the New Jersey Legislature passed Daniel's Law, which prohibits the disclosure of the home address or personal telephone number of active, formerly active, or

⁷ Ramachandran et al, *Officeholder intimidation*, 17.

⁸ *Assessing Threats and Harassment Towards Locally Elected Officials*, Joan B. Kroc School of Peace Studies, University of San Diego, <https://www.sandiego.edu/peace/institute-for-peace-justice/violence-inequality-power-lab/san-diego-threats.php>.

⁹ "Escalating online rhetoric reflects a violent authoritarian turn against the judiciary" Global Project Against Hate and Extremism (May 8, 2025), <https://globalextrmism.org/post/violent-authoritarian-turn-against-the-judiciary/>

¹⁰ Meredith Deliso, "Suspected gunman who killed Judge Esther Salas' son disparaged her as a Latina" ABC News (July 21, 2020), <https://abcnews.go.com/US/suspect-deadly-shooting-called-federal-judge-esther-salas/story?id=71901734>

retired law enforcement officers, judicial officers and prosecutors, child protective investigators, and the immediate family members residing in the same household (hereafter, “covered persons”). Daniel’s Law also prohibits state or local agencies from posting on the internet the home address or telephone number of covered persons without first obtaining written consent. Finally, the law established criminal and civil penalties for disclosing this information.¹¹ Covered persons can request redactions through the New Jersey Office of Information Privacy (OIP)’s portal. Since the creation of the OIP’s portal in 2022, nearly 9,000 covered persons have had their personal information redacted.¹²

Several companies were sued by plaintiffs alleging violations of Daniel’s Law. The companies moved to dismiss the lawsuits, alleging, among other things that the law conflicts with Section 230 of the federal Communications Decency Act of 1996, as well as the First Amendment to the United States Constitution. In August of 2025, a federal district court denied the motion to dismiss on these grounds.¹³ The decision is being appealed.

4) What is a data broker? The Federal Trade Commission (FTC) defines data brokers as “companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual’s identity, or detecting fraud.”¹⁴

California’s Data Broker Registration Law 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.”¹⁵

The common point in both of these definitions is that there is no direct relationship between a consumer and any data broker that has information about the consumer. In fact, it is unclear whether “consumer” is even an apt term in this context, since the person whose data is being collected generally does not directly consume any products or services produced by the data broker. Nevertheless, since “consumer” has become the default term in this context, it will be used in this analysis.

The key point to understand is that virtually no consumer chooses to have a relationship with a data broker. There is certainly a consensual transaction between the consumer and the websites the consumer accesses, the apps the consumer uses, and the consumer’s cell phone and internet service providers. Each of these transactions involves a transfer of the consumer’s personal information to these entities. But the consumer is not involved in the subsequent sale or transfer of their personal information to data brokers; there is no transaction between the consumer and the data broker involved with that sale or transfer.

5) Delete Request and Opt-out Platform (DROP). In 2023, the Legislature passed the Delete Act.¹⁶ The Act required the California Privacy Protection Agency (CalPrivacy) to develop a

¹¹ Daniel’s Law (P.L. 2021, c. 371)

¹² “Office of Information Privacy,” New Jersey Department of Community Affairs, <https://www.nj.gov/dca/oip/>

¹³ *Atlas Data Priv. Corp. v. We Inform, LLC* (D.N.J. Aug. 25, 2025, No. 24-4037) 2025 LX 301509, at *20.

¹⁴ FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014) p. 3, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

¹⁵ Civ. Code § 1798.99.80(d).

streamlined process that allows consumers to submit a request that every data broker that maintains any personal information delete the information related to that consumer held by the data broker. That ability for consumers to submit requests became active January 1 of this year. The Privacy Agency is then required to provide the requests to all registered data brokers. The Delete Act requires data brokers to honor those requests starting August 1, 2026. Once a data broker receives the request, it has 45 days to comply. In addition, the broker is required to check every 45 days to ensure the personal information has not been acquired again.

It is important to understand that the CCPA's definition of "personal information," which is incorporated in the Delete Act, excludes information that is "publicly available." Information is "publicly available" if it 1) comes from a local, state, or federal government source; 2) the broker reasonably believes the information was lawfully made available to the public; or 3) the information has been made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. Given the breadth of this exemption, even if a consumer asks that their personal information, including their most sensitive personal information, be deleted the data broker may decline the request and argue that the information was publicly available. This exemption could, in theory, even apply to hacked information that is made available on the internet. As a result, while the Delete Act provides important protections, its effectiveness and the effectiveness of this bill are limited by virtue of this broad exemption under the CCPA.

- 6) **What this bill would do.** This bill would create an expedited process for elected officials and judges to have their personal information held by data brokers deleted. The Secretary of State and the Judicial Council will be required to compile a list of elected officials and judges, respectively, to provide to CalPrivacy. Data brokers would be required to delete their personal information within five days of CalPrivacy uploading the list into the DROP system. If the data broker fails to comply, this bill allows for the elected official or judge who has requested deletion or a public attorney to bring a civil action against the broker.

This bill is substantially similar to AB 302 (Bauer-Kahan) which is currently a two-year bill in the Senate Appropriations Committee. The distinction between the two bills is that AB 302 is silent on what entity has the responsibility of creating the list of elected officials. This bill assigns that responsibility to the Secretary of State.

ARGUMENTS IN SUPPORT: Californians for Consumer Privacy writes in support:

Elected officials and judges have increasingly experienced threats of violence to themselves and their families. These threats are not theoretical. In 2020 Daniel Anderl was murdered when someone went to his home to confront his mother, a US District Court judge. This horrendous act of violence led to Daniel's Law in New Jersey, which limits access to key information in order to protect judges and others in law enforcement. In 2025, Minnesota elected officials and their families were attacked, and state Representative Hortman and her husband were assassinated, while state Senator Hoffman and his wife were shot and seriously injured by a gunman. In addition to these horrific incidents, research from the University of San Diego analyzed experiences of elected officials in San Diego, Riverside and Imperial Counties and found that 66% of elected officials found themselves being on the receiving end of threats and harassment.

¹⁶ Senate Bill 362, Chapter 709, Statutes of 2023.

Elected officials and judges are committed public servants who should be able to serve free of threats and harassment to them and their families. Dangers experienced by these officials and their families creates situations where our best and brightest are less likely to serve because of the potential for harm. That outcome is bad for our state and nation. AB 883 will create mechanisms to ensure that personal information held by data brokers about elected officials is deleted and not sold, and will be an important tool to limit the proliferation of this identifying information throughout society. This alone won't end threats and violence, but it will be an important step to protect those who we elect to serve the people.

ARGUMENTS IN OPPOSITION: With an “oppose unless amended” position, the California Chamber of Commerce, Computer and Communications Industry Association, TechCA, and TechNet write:

AB 883, as recently amended, causes confusion about what information the Secretary of State will provide to the CPPA, specifically in provision (a)(1). The bill should be amended to clarify that the SOS will give the CPPA a list of elected officials sufficient to verify their identities as required by the current Delete Act Regulations. Once the list of officials is provided to the CCPA and uploaded to the accessible deletion mechanism, data brokers must delete the personal information of the elected officials in accordance with the current language of the Delete Act.

Furthermore, this would require additional clarification, given that, as drafted, AB 883 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. Without narrowly tailored exceptions, this bill risks unintended harm to both consumers and the businesses that serve them.

The requested amendment below is included in the Delete Act in several instances, and the Committee, in their analysis of your AB 302 regarding the same deletion requests for elected officials and judges, acknowledged the “exemptions” continue to apply; we request that same certainty here, as well. Incorporating similar provisions into this bill would address our

concerns and strike a better balance between privacy protections and operational realities. Thus, we request the following amendment:

2) An entity receiving a notification that a deletion is required shall execute the deletion within ____ days *and as limited by Sections 1798.105, 1798.145, and 1798.146.*

REGISTERED SUPPORT / OPPOSITION:

Support

Californians for Consumer Privacy

Opposition

Cal Chamber
Computer and Communications Industry Association
Techca
Technet-technology Network

Analysis Prepared by: Julie Salley & Kate Davis / P. & C.P. / (916) 319-2200