SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 883 (Lowenthal)
Version: June 3, 2026
Hearing Date: June 15, 2026
Fiscal: Yes
Urgency: No
BD

SUBJECT

Data brokers: deletion of personal information of elected officials and judges.

DIGEST

This bill requires the Secretary of State, local filing officials, and the Judicial Council to provide the California Privacy Protection Agency (CalPrivacy) with a list of all available personal information of state or local elected officials and judges for the purpose of data deletion using CalPrivacy's accessible data deletion mechanism.

EXECUTIVE SUMMARY

Political violence is on the rise, with the Pew Research Center noting that 85 percent of adults believe that politically motivated violence is increasing. This form of violence is frequently directed at elected officials and judges, and multiple studies note that attacks, threats, and harassment are commonplace for these public servants. Oftentimes, these acts of violence are facilitated by the ability of offenders to easily find and locate elected officials' and judges' personal information, particularly through data brokers.

To address this uptick in political violence, this bill requires the Secretary of State, local filing officers, and the Judicial Council to create and update, after every election or appointment, a list of elected officials and judges, including specified personal information. This list must then be sent to CalPrivacy to be uploaded to CalPrivacy's accessible deletion mechanism. Data brokers are required to delete elected officials' and judges' personal information within 10 days.

This bill is sponsored by Californians for Consumer Privacy and is supported by organizations such as the California Special District Association and Public Citizen. This bill is opposed by various advertising industry groups and ACLU California Action. Should the bill pass out of this Committee, it will next be heard by the Senate Judiciary Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides that all people are, by nature, free and independent and have inalienable rights, among these are a right to privacy. (Cal. Const., art. 1 § 1)

2) Provides that an "elected or appointed official" includes, but is not limited to, a state constitutional officer, a Member of the Legislature, an active or retired judge, court commissioner, judge of the State Bar Court, a district attorney, a public defender, a member of a city council, a member of a board of supervisors, an appointee of the Governor, an appointee of the Legislature, a mayor, a city attorney, a police chief or sheriff, a public safety official, a state administrative law judge, an active or retired federal judge or federal defender, a member of the United States Congress, appointee of the President of the United States, an active or retired judge of a federally recognized Indian tribe, and an appointee of a court to serve as children's counsel in a family or dependency proceeding. (Gov. Code § 7920.500)

3) Provides that the home addresses, home telephone numbers, personal cellular telephone numbers, and birthdates of all employees of a public agency shall not be deemed public records, subject to certain exemptions. (Gov. Code § 7928.300)

4) Provides that no state or local agency shall publicly post the home address, telephone number, or both the name and assessor parcel number associated with the home address of any elected or appointed official on the internet without written consent from the individual. (Gov. Code § 7928.205).

5) Defines "personal information" to mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could, directly or indirectly, reasonably be linked to a particular consumer or household and includes, but is not limited to, all of the following:
    a) Identifiers such as a postal address, social security number, or passport number.
    b) Commercial information, including records of personal property.
    c) Biometric data.
    d) Internet or other electronic network activity.
    e) Geolocation data.
    f) Sensitive personal information. (Civ. Code § 1798.140)

6) Provides that "personal information" does not include publicly available information. (Civ. Code § 1798.140)

7) Defines "publicly available" to mean the following:

a) Information that is made lawfully 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)

8) Provides a consumer with the right to request that a business delete any personal information that the business has collected from the consumer. (Civ. Code § 1798.105)

9) Provides a consumer with 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. (Civ. Code § 1798.120)

10) Requires a business that knowingly collects and sells consumer information to third parties, subject to certain exceptions, to register with CalPrivacy as a data broker. (Civ. Code § 1798.99.80)

11) Provides that data brokers do not include entities covered by the federal Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Insurance Information and Privacy Protection Act. (CIV § 1798.99.80)

12) Requires CalPrivacy to establish an accessible deletion mechanism that does all the following:
    a) Implements and maintains security procedures and practices that include, but are not limited to, administrative, physical, and technical safeguards.
    b) Allows a consumer to request that every data broker delete any maintained personal information that they have, within 45 days.
    c) Allows a consumer to exclude specific data brokers from their deletion request to data brokers.
    d) Allows a consumer to alter a previous deletion request to data brokers, if 45 days have passed since the consumer last made their request. (Civ. Code § 1798.99.86)

13) Requires data brokers to access the accessible deletion mechanism at least once every 45 days to process all deletion requests; delete a consumer's personal information if the request is verified; treat all unverified deletion requests as an opt-out of the sale or sharing of personal information; direct all service providers or contractors associated with a data broker to delete all personal information if a consumer requested it; and direct all service providers or contractors associated with

a data broker to treat all unverified deletion requests as an opt-out of the sale or sharing of personal information. (Civ. Code § 1798.99.86)

This bill:

1) Requires the Secretary of State to provide CalPrivacy with a list of all state elected officials that, if available, includes each official's personal information.

2) Requires a filing officer for a local government to provide CalPrivacy with a list of all local elected officials within the filing officer's jurisdiction that, if available, includes each official's personal information.

3) Requires the Secretary of State and filing officers for a local government to provide the list described above after the certification of a final election.

4) Requires CalPrivacy to provide each elected official with an opportunity to request the removal of their name and profile data from the list.

5) Requires the Judicial Council to provide CalPrivacy with a list of all California judges that includes each judge's name and other profile data, as defined by CalPrivacy, that has been voluntarily shared by the judge.

6) Requires the Judicial Council to provide each judge an opportunity to request that the judge's personal information be removed from the list prior to it being sent to CalPrivacy.

7) Requires CalPrivacy to upload the lists provided by the Secretary of State and Judicial Council to the accessible deletion mechanism administered by CalPrivacy. Requires an entity required to delete the personal information of a person on the above lists to do so within 10 days.

8) Requires the lists and the information on the lists to be exempt from the California Public Records Act.

9) Provides that an elected official or judge who is on a list, the Attorney General, a county counsel, or a city attorney may bring a civil action to enforce the provisions of this bill. Provides that relief consists of declaratory relief, injunctive relief, reasonable attorney's fees, and actual damages.

10) Provides that willful violations of this bill may result in punitive damages.

11) Becomes operative on July 1, 2027

COMMENTS

1. Political Violence Against Elected Officials

Political violence, which broadly refers to the threat or use of physical force to enforce or disrupt a particular order, has captured the nation's attention.[1] The Pew Research Center notes that 85 percent of adults believe that politically motivated violence is increasing, with nearly identical percentages for both Republicans and Democrats.[2] Reflective of this, the nation has seen numerous examples of political violence in recent years. A report by The Armed Conflict Location & Event Data Project (ACLED) highlights some of these cases:

> Amid intensely polarized political discourse at the national level, attacks on state officials in Pennsylvania and Minnesota reflect the broader rise of high-profile politically motivated attacks by individuals without ties to wider movements, including the killing of political activist Charlie Kirk by a lone gunman in September and assassination attempts on President Donald Trump in 2024.
>
> Pennsylvania Governor Josh Shapiro and his family were targeted by a man who, armed with a hammer, broke into the Governor's Residence in Harrisburg on 13 April and set it alight. The arsonist later turned himself in and cited Shapiro's support for Israel as motivation, claiming that Shapiro needed to "stop the killing of Palestinians."
>
> Several Minnesota state lawmakers and their families were also targeted for assassination by a lone gunman in June. The gunman, disguised as a police officer and wearing a silicone mask, drove to the homes of at least four Democratic elected officials in the Twin Cities area. He carried out shootings at two of these homes, wounding State Senator John Hoffman and his wife and killing State Representative Melissa Hortman and her husband, before being apprehended by police. The gunman had a "hit list" that included 45 elected officials — all of whom were Democrats — as well as doctors who provide abortions and Planned Parenthood clinics,

---

[1] Ruggeri et al., *Political violence in democracies: An Introduction* (August 22, 2025) Journal of Peace Research 62*(5)*, https://journals.sagepub.com/doi/10.1177/00223433251351251?__cf_chl_tk=fUd6ch2VAt3hgH4LkAlzUqAoWa2zxhuJPtLgRaOgXwc-1777951076-1.0.1.1-cNFZ.5Jq84YHo5VrQgzVhvoGuYrF3y6rZ9FRocSuO4g. All internet citations are current as of May 22, 2026.

[2] Joseph Copeland & Jocelyn Kiley, *Americans say politically motivated violence is increasing, and they see many reasons why* (October 23, 2025) Pew Research Center, https://www.pewresearch.org/short-reads/2025/10/23/americans-say-politically-motivated-violence-is-increasing-and-they-see-many-reasons-why/.

> pointing to anti-abortion views as a possible motive. Hortman was the first state legislator to be assassinated in the US in a decade.[3]

These events reflect the troubling reality of being an elected official. When focusing solely on state legislators, more than 40 percent have experienced threats or attacks within the past three years. Similarly, over 18 percent of local elected officials have experienced threats or attacks. When expanded to include less severe forms of abuse, 89 percent of state legislators and 52 percent of local officeholders note experiencing some form of harassment, insults, or stalking.[4] It would appear that these experiences will only continue, as 38 percent of state legislators reported that the amount of abuse they have experienced has increased since they were first elected.[5] Additionally, a University of San Diego study that examined threats and harassment against elected officials in San Diego, Riverside, and Imperial Counties found that 66 percent of elected officials have received some form of threats and harassment.[6] Women elected officials appear to face a higher risk, with 69 percent of women experiencing threats and harassment on a monthly basis compared to 38 percent of men.[7] Concerningly, 46 percent of women and 39 percent of men have considered leaving public office due to the harassment that they endure.[8]

2. Political Violence Against Judicial Officers

In addition to local and elected officials, state judges also face the unique risk of elevated threats of violence. As noted by the New York Times:

> For judges across the country, threats and harassment have become an inescapable occupational hazard. The Department of Homeland Security issued a nationwide alert late last year to law enforcement agencies: Harassment of judges has surged, and the trend is likely to continue.
>
> The New York Times has identified thousands of threats targeting state judges in the past three years alone, among more than 14,000 broader security incidents involving state courts and their employees across the country. These figures offer a look at a problem that has historically gone

---

[3] Kieran Doyle, *United States and Canada: Deadly attacks on local officials reflect the rise of the longe gunman,* (April 23, 2026) ACLED, https://acleddata.com/report/united-states-and-canada-deadly-attacks-local-officials-reflect-rise-lone-gunman.
[4] Ramachandran et al., *Intimidation of State and Local Officeholders* (January 25, 2024) The Brennan Center for Justice, https://www.brennancenter.org/our-work/research-reports/intimidation-state-and-local-officeholders.
[5] *Ibid.*
[6] John Porten & Rachel Locke, *California Threats and Harrassment Initiative* (2024) Joan B. Kroc Institute for Peace and Justice at the University of San Diego, https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1097&context=ipj-research
[7] *Ibid.*
[8] *Ibid.*

> uncounted because of a lack of record-keeping; they almost certainly understate the true scale, given that many states fail to formally track the issue.
>
> Some of the violence is high-profile: In January, Judge Steven Meyer and his wife survived a shooting at their home in Lafayette, Ind., an attack that the police said was orchestrated by a defendant in an upcoming domestic battery case. In 2023, a Maryland state judge was shot and killed in his driveway, and in 2022, a retired Wisconsin state judge was killed in another targeted home attack.
>
> But many more incidents never reach the public. Records show that state judges have been subjected to stalking, death threats, physical assaults, and assassination plots. They have reported being struck in the head, shot, and pelted with feces.
>
> Threats are also on the rise against federal judges, of which there are around 2,700. Such threats have more than doubled in four years, from 224 cases in 2021 to 564 in 2025, according to the U.S. Marshals Service.
>
> But there is no centralized security force that tracks threats against the estimated 30,000 state judges who are on the front lines of some of the most contentious cases in the country. Nor is there the same mandate to protect them.[9]

In 2020, Daniel Anderl, the son of a federal judge, was shot and killed in his home after a vengeful attorney was able to find his home address on the internet.[10] This sparked the New Jersey state legislature to pass "Daniel's Law", which prohibits any person from posting or otherwise making available the home address of any current and former judicial officers, law enforcement personnel, prosecutors, and their immediate family members.[11] Since its passage, Daniel's Law has been challenged numerous times, with plaintiffs arguing First Amendment and Section 230 of the Communications Decency Act violations. To date, the efforts have been largely unsuccessful; however, some challenges are currently pending.

3. The Role of Data Brokers and California's Response

With political violence in the headlines seemingly occurring more frequently, the importance of shielding elected officials' and judges' personal information is ever

[9] Katie J.M. Baker, *State Judges Turn to Guns in New Era of Judicial Threats* (April 10, 2026), *New York Times,* https://www.nytimes.com/2026/04/10/us/state-judges-threats.html.
[10] Philip Yannella & Tom Dickens, *Daniel's Law: the next wave in privacy litigation* (March 20, 2024), Reuters, https://www.reuters.com/legal/legalindustry/daniels-law-next-wave-privacy-litigation-2024-03-20/.
[11] *Ibid.*

apparent. For instance, in the horrifying case of Minnesota Speaker Melissa Horton, the aggressor was able to find her personal information online, with the information allegedly originating from data brokers.[12]

The Federal Trade Commission (FTC) describes data brokers as "companies that collect consumers' personal information and resell or share that information with others".[13] The collection of this data, combined with advanced technologies and the use of sophisticated algorithms, can create incredibly detailed and effective profiling and targeted marketing from this web of information.

Some of the largest data brokers include Experian, Equifax, TransUnion, LexisNexis, Epsilon (formerly Acxiom), and CoreLogic, as well as people-search services like Spokeo and Intelius.[14] Just one company, Epsilon, provides information on hundreds of millions of people, culled from voter records, purchasing behavior, vehicle registration, and other sources.[15]

A report by the FTC found that data brokers "collect and store a vast amount of data on almost every U.S. household and commercial transaction," most of them "store all data indefinitely," and that "many of the purposes for which data brokers collect and use data pose risks to consumers."[16]

The Electronic Privacy Information Center has detailed its concerns with the secrecy and depth of the industry:

> Data brokers use secret algorithms to build profiles on every American citizen, regardless of whether the individual even knows that the data broker exists. As such, consumers now face the specter of a "scored society" where they do not have access to the most basic information on how they are evaluated. The data broker industry's secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs. In one instance, a

---

[12] 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/.
[13] FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[14] Barbara Booth, *What internet data brokers have on you — and how you can start to get it back* (October 11, 2024) CNBC, https://www.cnbc.com/2024/10/11/internet-data-brokers-online-privacy-personal-information.html.
[15] Nitasha Tiku, *Europe's New Privacy Law will Change the Web, and More* (March 19, 2018) Wired, https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/.
[16] FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

> consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage. Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[17]

The rapidly advancing capacity of AI technology only heightens the concerns around the industry and the feeling of helplessness on the part of consumers:

> The rise of artificial intelligence tools poses the risk of even more personal information being scraped from the internet and an already opaque world of data brokering becoming even more aggressive, and that is heightening data privacy concerns. A 2023 study from Pew Research found that the American public increasingly says it does not understand what companies do with their data. According to Pew, 67% of Americans say they "understand little to nothing about what companies are doing with their personal data, up from 59% in its previous survey on the subject in 2019. A majority of Americans (73%) think they have "little to no control" over what companies do with their data.
>
> Many people are unaware that something as simple as their phone number can be used by data brokers and bad actors to uncover highly sensitive information, including a Social Security number, address, email, and even family details . . . . [18]

In light of these concerns, California has responded in kind. SB 362 (Becker, Ch. 709, Stats. 2023) required CalPrivacy to create and administer a comprehensive, holistic method to request data deletion from data brokers.[19] This mechanism is known as the Delete Request and Opt-Out Platform (DROP). DROP allows consumers to securely input data that is immediately hashed and submit it for data brokers to compare to their records. Following the submission of a request, data brokers have 45 days to delete a consumer's personal information from their records. Californians have been able to submit DROP requests since January, 2026, with the Delete Act not requiring actual deletion until August 1, 2026. In the first 20 days of the tool being available, over 150,000 Californians have made a request through DROP.[20] As of June 2, 2026, over 300,000 Californians have signed up for the tool.[21]

---

[17] *Data Brokers*, Electronic Privacy Information Center, https://epic.org/issues/consumer-privacy/data-brokers/.
[18] *Barbara Booth, What internet data brokers have on you — and how you can start to get it back (October 11, 2024) CNBC, https://www.cnbc.com/2024/10/11/internet-data-brokers-online-privacy-personal-information.html.*
[19] Civ. Code § 1798.99.86.
[20] Cecilio Padilla, *California sees 150,000+ sign-ups for new data broker deletion request tool* (January 20, 2026) CBS, https://www.cbsnews.com/sacramento/news/california-drop-tool-data-broker-deletion/.
[21] *Privacy Momentum Builds: 300,000+ Californians Sign Up for DROP as Registered Data Brokers Hit a Record High* (June 2, 2026) California Privacy Protection Agency, https://privacy.ca.gov/2026/06/privacy-momentum-builds-300000-californians-sign-up-for-drop-as-registered-data-brokers-hit-a-record-high/.

It is important to note that DROP, while groundbreaking, does have certain limitations. Specifically, the "personal information" that data brokers are required to delete if a consumer makes a deletion request has an exception for "publicly available information". As aptly put by the Assembly Privacy and Consumer Protection Committee, this broad exemption may lead to situations where a data broker may decline to delete certain pieces of information, using this exemption as justification. This is especially relevant for public officials and judges, as data that was obtained via hacking or doxing could, in theory, be considered "publicly available information".

4. What this Bill Does

This bill requires the Secretary of State, local filing officers, and the Judicial Council to compile a list of all state or local elected officials and California judges that contains these individuals' personal information. The bill specifies that state or local elected officials and California judges be given the opportunity to remove themselves from this list, should they so choose. After compiling their respective lists, the bill requires the Secretary of State, local filing officers, and the Judicial Council to send the list to CalPrivacy so that the agency can upload the lists to its accessible deletion mechanism for data brokers. The bill provides an expedited timeline for deletion, requiring data brokers to execute the deletion within 10 days. This provides elected officials and California judges with a privacy-by-default mechanism to ensure that their personal information is adequately protected at a time when political violence is frequently observed.

To ensure compliance with this section, this bill authorizes elected officials and judges who are on the lists generated by the Secretary of State, local filing officers, and the Judicial Council to bring a civil action for declaratory relief, injunctive relief, reasonable attorney's fees, and actual damages. The bill also extends this authorization to the Attorney General and local public prosecutors. Furthermore, if a court finds that an entity willfully refused to delete an elected official's or a judge's personal information, then the court may award punitive damages.

Lastly, in recognition of the sensitivities of the data on the lists, this bill provides that any shared information resulting from the shared lists be transferred in a secure and confidential exchange and exempts the lists from disclosure under the California Public Records Act.

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 also 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.

Californians for Consumer Privacy, this bill's sponsor, 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.
>
> 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.

5. Concerns with this Approach

While it is of the utmost importance to safeguard the personal information of elected officials and judges, especially given the aforementioned rise in political violence, the bill in print has raised some operational, equity, and potential privacy concerns.

As it relates to the operational concerns, this bill would effectively create two different timelines and operations for the deletion of personal information through DROP. By requiring the deletion of the data list in ten days rather than the standard 45-day timeline under existing law, this bill requires the creation of a separate, accelerated portal for the deletion of elected officials' and judges' data. This presents both CalPrivacy and data brokers with compliance challenges.

Additionally, this approach raises an equity question of why elected officials and judges are subject to an expedited deletion process when many groups suffer from similar levels of violence. For instance, this bill does not apply to federal officials who operate in California, despite them being subject to the same threat of political violence. Furthermore, many entities that offer sensitive services, such as reproductive healthcare, also face increased risk of threats, harassment, cyberattacks, and violence.[22] While it is certainly evident that elected officials and judges face an increased risk of violence, this is true of many occupations, making it unclear why only state and local elected officials and judges deserve this privilege. Oakland Privacy highlights these concerns:

> We want to be clear that we understand that this effort is motivated by the horrific assassinations and attacks on elected officials, particularly in Minnesota on June 14, 2025 which resulted in the deaths of State Senator Melissa Hortman and her spouse Mark, and severe injuries to state senator Mark Hoffman, and his spouse Yvette. This was a violent and terrifying attack and made much worse by the plain fact that these were public servants who were simply doing their jobs and were shot for it.
>
> But it is important in this moment to acknowledge that while elected officials and judges may certainly be targets for deranged or radicalized assailants, they certainly aren't the only ones. As the Legislature has recognized in the past, election officials can also be targets as well as non-elected public officials who are appointed to their positions, as well as doctors and nurses performing reproductive or gender affirming health care, teachers, and journalists.
>
> All are public servants and all have witnessed devastating and fatal attacks against members of their profession. And in many cases have less resources and existing security measures than elected officials and judges.

[22] *Resource Booklet for Reproductive Care Providers and Their Staffs* (November 7, 2022), National Task Force on Violence Against Reproductive Health Care Providers, https://www.fbi.gov/file-repository/criminal-investigative/resource-booklet-for-reproductive-health-care-providers-and-their-staffs_052722.pdf

ACLU California Action, writing in opposition, notes similar concerns:

> While we understand the threat of political violence that some politicians and judges live under, we can see no principled basis for elevating the concerns of a privileged few over the protection of everyone—particularly where privacy harms, and the attendant violations of other civil and human rights that flow from them, are uniquely felt and experienced by those at the margins of our society.

This bill also requires that CalPrivacy and the Judicial Council provide elected officials and judges the opportunity to request their removal from the lists. However, the bill does not define or provide any guidance on how that would work in practice. This does raise a question of whether an elected official or judge fully understands what it means to opt out. Oakland Privacy notes:

> The entire point of DROP was to make it as simple as possible to do this and that in particular, people who are busy and have demanding work, family or care taking responsibilities would be able to utilize the system easily.
>
> We are not sure why we are concluding in this bill that elected officials and judges are unable to utilize the system directly and requiring the privacy agency to do it for them. That seems contrary to the entire point of DROP.

Lastly, how this bill achieves its intended goal may actually create privacy concerns: the very problem this bill attempts to avoid. When a consumer submits a deletion request under the Delete Act, CalPrivacy does not store or keep any of the actual data provided by consumers. Rather, they transform the input data into digital hashes as soon as the data is entered into a request. This ensures robust data protection. Contrastingly, the bill provides for 1) the creation of a list containing the personal information of all elected officials and judges, 2) the upload of the list to facilitate its transfer, and 3) the storage of the list to input the data to DROP. All of these steps represent potential security vulnerabilities. While the bill does provide that the data transfer be done securely and confidentially, it still opens potential vulnerabilities that could expose the information of every elected official and judge in one fell swoop, as the information is exchanged one additional time. As noted by CalPrivacy:

> As currently drafted, the bill requires the Secretary of State and the Judicial Council to collect and transfer to the Agency data to create deletion requests. Both processes require that personal data is collected and transferred among various parties prior to being submitted into DROP, introducing new privacy and security concerns. Under the current DROP configuration, CalPrivacy staff does not have access to personal

> information submitted through DROP — such information is immediately hashed, which makes the information unreadable at all times. However, under AB 883, CalPrivacy staff would, at least initially, have access to personal information provided by the Secretary of State and the Judicial Council…

In opposition, a coalition of advertising industry groups, including the Association of National Advertisers, notes the following:

> AB 883 would require registered data brokers receiving a deletion notification to effectuate data deletion within ten days, a substantially shorter time period than the forty-five day period permitted for other deletion requests submitted through the Delete Request and Optout Platform under the Delete Act. 3 AB 883's shortened timeline would present significant operational challenges, as data brokers have mapped compliance processes to the existing fortyfive day timeline. By requiring deletion pertaining to elected officials and judges to be completed within ten days, the bill would increase the risk of error for well-meaning data brokers intending to comply and may lead to conflicts with other legal obligations that require retention of data for particular purposes.
>
> Clarity and consistency in legal requirements are essential to ensuring that Californians have understandable and predictable rights while minimizing unnecessary compliance costs for businesses. The Committee should take steps to align AB 883's deletion timeline with the existing forty-five day standard in the Delete Act. Doing so would promote consistency across California privacy laws and support implementation efforts that protect state residents.

In response to the aforementioned concerns, the author has agreed to significantly amend the bill. The bill, as amended, does not require the Secretary of State, local filing officers, or the Judicial Council to send a list of all elected officials' and judges' personal information to CalPrivacy. Instead, CalPrivacy must create informational material detailing how elected officials and judges can use DROP. They then send this information to the Secretary of State, local filing officers, and the Judicial Council to be distributed to elected officials and judges. Additionally, solely elected officials and judges would not receive an expedited timeline for deletion; rather, the bill would reduce the deletion timeline for all Californians from 45 days to 30 days.

SUPPORT

Californians for Consumer Privacy (sponsor)
California Initiative for Technology & Democracy, a Project of California Common CAUSE

California Special Districts Association
Public Citizen

OPPOSITION

ACLU California Action
American Advertising Federation (AAF)
American Association of Advertising Agencies (4A's)
Association of National Advertisers
Digital Advertising Alliance

RELATED LEGISLATION

SB 923 (Becker, 2026) would expand consumers' deletion rights to include information that a business has collected about a consumer. SB 923 is pending before the Assembly Privacy and Consumer Protection Committee.

AB 1785 (Pacheco, Ch. 551, Stats. 2024) prohibited a state or local agency from publicly posting both the name and assessor parcel number of any elected or appointed official on the internet without written permission.

SB 362 (Becker, Ch. 709, Stats. 2023) established the Delete Act and required CalPrivacy to create an accessible deletion mechanism where California consumers could request the deletion of their personal information from data brokers.

AB 375 (Chau, Ch. 55, Stats. 2018) enacted the California Consumer Privacy Act of 2018, which gave California consumers the right to delete their personal information from businesses that sell their data.

PRIOR VOTES:

Assembly Floor (Ayes 75, Noes 0)
Assembly Appropriations Committee (Ayes 15, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 14, Noes 0)

****