



September 4, 2026

The Honorable Gavin Newsom
Governor, State of California
State Capitol, Suite 1173
Sacramento, CA 95814

RE: SB 923 (Becker) – Consumer Privacy Requests: Deletion Request Records and Request Submission Methods — REQUEST FOR VETO

Dear Governor Newsom:

The California Chamber of Commerce and undersigned respectfully request a veto of **SB 923 (Becker)**. Throughout this bill's passage through the Legislature, we consistently raised two amendments necessary to make the bill workable, and neither the author nor the sponsor—the California Privacy Protection Agency—accepted either change at any point in the process. As a result, SB 923 reaches your desk with two significant, unresolved defects: it vastly expands deletion obligations under the California Consumer Privacy Act (CCPA) without a workable compliance path, and it mandates an email-only channel for submitting deletion requests that creates unnecessary cybersecurity risk for California consumers.

SB 923 Vastly Expands CCPA Deletion Obligations Without a Workable Compliance Path

Under the CCPA, the scope of “personal information” is exceedingly broad. While the CCPA's existing right of deletion is limited to personal information received **directly from a consumer**, SB 923 expands that right to any personal information a business has **about a consumer**, regardless of source — a material change to what compliance will entail.

Twenty states have an operative right-to-delete mandate for businesses. **SB 923** is modeled in part on a law from **16 states¹ that recognize two distinct compliance methods for third-party data:** (1) retaining a record of the deletion request and the minimum data necessary to ensure the information stays deleted, or (2) opting the consumer out of further processing of that information for non-exempt purposes. **SB 923 inexplicably omits the second option offered in those states**, making compliance unnecessarily confusing

¹ AL, CO, CT, FL, KY, LA, MN, MT, NE, NH, OK, OR, RI, TN, TX, VA.

and onerous for California businesses. Notably, the four states² that the Agency has pointed to in defense of its choice to omit this second safe harbor are nowhere near the size of California's population and do not need to handle the volume of data that will have to be handled by California businesses when expanding the right of deletion to information "about the consumer".

Without an opt-out mechanism, data that re-enters a business's systems from external partners — even where the business itself never uses, sells, discloses, or shares it — triggers a fresh deletion obligation. This creates a costly "whack-a-mole" cycle: businesses must delete the same data over and over as it flows back in from third-party sources, even though the consumer has already exercised their deletion right and the business has already functionally excluded that data from further processing. Large-scale deletion across distributed systems, logs, and backups is operationally complex and expensive, and it provides no additional privacy benefit to the consumer once the data has already been suppressed from use.³ The new Data Broker Deletion Request and Opt-Out Platform (DROP) system illustrates this same operational challenge for registered data brokers, who must continuously compare deletion requests against newly collected records. Without the opt-out safe harbor, SB 923 would extend that same burden that exists for data brokers to ordinary, non-broker businesses.

The opt-out safe harbor we requested would not diminish consumer rights. It gives businesses a clear, scalable way to honor a deletion request — preventing further processing of the consumer's information — while retaining only the minimum data necessary to keep that information suppressed, prevent its re-collection, and satisfy fraud-prevention, security, and legal-compliance obligations that businesses are separately required to meet. Fraud prevention in particular depends on this limited retention: third-party signals such as alerts about compromised credentials, suspicious account activity, or identity-verification checks are often what allow a business to detect and stop fraud targeting the very consumer who requested deletion.

The June 11, 2026, amendments recognize the need to hold on to data for exempted needs but do not fix this critical issue. The author added *findings and declarations* restating the Legislature's policy objective, but findings and declarations are not operative statutory language. They do not create a safe harbor, establish a compliance standard, or tell a business whether retaining a suppression record or opting a consumer out of further processing actually satisfies a deletion request under Civil Code Section 1798.105. Businesses are governed by the statute's operative text, not uncodified findings

² DE, IN, MD and NJ. Technically, NJ provides a dual-compliance safe harbor, but a different one than the 16 states above. Specifically NJ provides for a *retain or delete* option as opposed to *retain or opt out*.

³ It is also worth noting that from a practical standpoint, given the liability exposure created by data breaches, a business has no incentive to hold on to any PI other than the information it can use for limited exempted purposes when it cannot otherwise process the consumer's PI for any non-exempt purpose.

— and these provisions still leave them guessing whether honoring their fraud-prevention and security obligations will later be read as a violation of the deletion mandate.

SB 923's Email-Only Mandate Creates Unnecessary Cybersecurity Risk

SB 923 would require businesses that operate exclusively online to publish both an email address and a separate online method — such as a web form or portal — for submitting CCPA rights requests. Requiring a publicly listed email address as a mandatory channel exposes businesses, and by extension their customers, to unnecessary risk: such addresses are routinely harvested by cybercriminals and used as vectors for phishing attacks, a risk substantially heightened by the rise of AI-generated attacks capable of producing highly convincing, targeted phishing communications at scale. This is precisely why many businesses have already moved toward secure, authenticated webforms and portals as their primary channel for consumer requests.

We provided a simple amendment to achieve the same outcome for consumers with far less exposure to fraud and data breaches: businesses should be permitted to offer a secure webform or online portal in lieu of — rather than in addition to — a publicly listed email address, but the author, again, repeatedly declined this request.

Conclusion

SB 923 is modeled on an out-of-state framework but omits the very provision that makes that framework workable in the vast majority of states, while simultaneously imposing a cybersecurity-negative mandate that runs counter to the state's own interest in protecting consumers from phishing and fraud.

We raised both concerns at first policy committee and in every subsequent stage of this bill's consideration, and neither was addressed in the version now before you. For these reasons, we respectfully request your veto of **SB 923**.

Thank you for your consideration.

Sincerely,



Ronak Daylami

Vice President for Advocacy | Privacy, Cybersecurity & Emerging Technologies
California Chamber of Commerce

on behalf of:

American Car Rental Association
Association of National Advertisers
California Bankers Association
California Chamber of Commerce

California Restaurant Association
Civil Justice Association of California
Computer & Communications Industry Association
Insights Association
Silicon Valley Leadership Group
Software Information Industry Association
TechCA
TechNet