CALIFORNIA PRIVACY PROTECTION AGENCY
400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov

Date: October 28, 2025

To: California Privacy Protection Agency Board
(Meeting of November 7, 2025)

From: Maureen Mahoney
Deputy Director, Policy & Legislation

Subject: **Agenda Item 2 - Legislation Update and Agency Proposals**

This memorandum provides for the California Privacy Protection Agency Board's consideration several bill proposals that would amend the California Consumer Privacy Act (CCPA). In staff's view, these proposals meaningfully increase privacy protections for Californians. We recommend multiple proposals because the feedback we have received from the legislature is that offices would appreciate a variety of options to consider when putting together their bill packages for the year.

Staff recommends that the Board approve these proposals and direct staff to present them to members of the California Legislature for possible authoring and Agency support. Because the decision to sponsor a bill depends on several factors, such as the amount of work that the specific bill would require and whether the author has identified other sponsors for the bill, staff recommends that the Board provide directional feedback while leaving it to staff's discretion whether to sponsor the proposals discussed below.

Board approval of these proposals would allow staff to engage in two ways. First, for high-priority proposals, subject to the Board's delegation, staff could determine that the Agency should sponsor the proposed legislation. Sponsorship typically involves working closely with a legislator to draft the bill and engaging with stakeholders to shape the bill as it proceeds through the legislative process, along with communicating the Agency's position to the legislature.

Alternatively, for important but less critical bills, subject to the Board's delegation, staff could determine that the Agency will issue public support for the bill. Support includes providing technical assistance to the author as the bill moves through the legislative process and communicating the Agency's position to the legislature.

Below, we outline the recommended proposals in order of priority for staff.

Establish Comprehensive Whistleblower Protections

- An award program to incentivize whistleblowers,
- A special designation program that enables the Enforcement Division to collaborate with whistleblower attorneys on certain cases and allow whistleblowers to share a portion of an administrative fine, and
- Anti-retaliation provisions to protect whistleblowers and encourage cooperation.

Technology and data-driven business practices are often opaque, making it important for regulators to gather and review business records during investigations. Whether for competitive advantage or protection of proprietary systems, companies design complex algorithms, implement data collection systems, or make policy decisions about privacy behind closed doors. This lack of clear visibility means that potential privacy violations can be time-consuming to identify using traditional investigative tools.

Additionally, data processing and emerging data technologies are highly technical areas that often require inside knowledge. Employees within a business possess this inside knowledge and can quickly identify when companies are failing to comply with privacy laws. Indeed, private tech companies typically have teams of experts in contrast to the lean legal and technical teams of regulators that must perform oversight on entire industries.

Given the hidden and complex nature of the information industry, internal whistleblowers can play a key role in exposing unknown or unknowable violations. Recent examples demonstrate that privacy violations may remain hidden at technology companies while publicly there appears to be compliance. For example, in 2021 Frances Haugen alleged to the Securities and Exchange Commission (SEC), lawmakers, and the media that Facebook had knowledge of potential harm and safety concerns related to teenagers that had been intentionally ignored or hidden.[1] In this case, internal knowledge was critical to exposing potential wrongdoing occurring inside the black box.

Building whistleblower protections into California's technology and privacy laws would be an important step to increase transparency and accountability in the information ecosystem. Indeed, this year the Joint California Policy Working Group on Frontier AI Models recommended whistleblower provisions as critical elements for laws related to artificial intelligence to help increase transparency.[2] Their report highlighted parallels between the tech and tobacco industries, referencing how tobacco companies spent decades concealing evidence of health risks while publicly disputing the dangers of smoking, despite regulatory attempts to address the issue.[3]

---

[1] Ryan Mac & Cecilia Kang, *Whistle-Blower Says Facebook 'Chooses Profits Over Safety,'* The New York Times, October 3, 2021, updated June 23, 2023, https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html.
[2] Joint California Policy Working Group on AI Frontier Models, The California Report on Frontier AI Policy at 4, June 17, 2025, https://www.gov.ca.gov/wp-content/uploads/2025/06/June-17-2025-–-The-California-Report-on-Frontier-AI-Policy.pdf
[3] *Id.* at 15.

Adding whistleblower incentives to the CCPA could enhance the Agency's ability to uphold and enforce consumers' privacy rights. First, a financial awards program would incentivize whistleblowers to come forward with original, valuable information for investigation. A financial incentive would help to even the scales for whistleblowers who worry about the repercussions of speaking out. Additionally, establishing a mechanism for collaboration where whistleblower representatives can work alongside the Agency on selected cases, offering expert support, and allowing whistleblowers to share a portion of an administrative fine would provide added support to both the Agency and the potentially vulnerable whistleblower. The net result of this collaboration would be a higher volume of meritorious cases that the Agency could pursue to hold businesses accountable for violations. Finally, safeguards that protect whistleblowers from retaliation and empower them to seek legal recourse if they face retaliation provide forward-looking protections to whistleblowers.

These types of incentives have precedent in other whistleblower laws. Both the federal and state False Claims Act and the SEC's whistleblower law, for example, offer financial incentives to whistleblowers when they provide certain information or allow whistleblowers and their representatives to bring or collaborate in enforcement actions.[4] The SEC program, for example, operates successfully without any private right of action or other vehicle for whistleblowers to proceed on their own when the agency declines to take up the case.

Other California laws offer protections for whistleblowers. Specifically, laws such as those included in California's Labor Code (1) restrict businesses from limiting an employee's ability to provide disclosures to the government or law enforcement or retaliating against employees for disclosures, and (2) allow whistleblowers to receive a damage award and attorneys' fees in any lawsuit brought based on business retaliation.[5] Additionally, the Transparency in Frontier Artificial Intelligence Act (SB 53), which was recently signed into law, provides this style of anti-retaliation protections and requires AI frontier developers to have internal whistleblower processes that allow employees to alert their employer of potential legal violations.[6]

A comprehensive approach that incorporates both award and collaboration elements along with the protections from retaliation available in the Labor Code would encourage reporting of wrongdoing while also protecting and supporting those who step forward. Offering whistleblowers protections that only kick in if they face retaliation does little to encourage the critical first step of disclosure. Whistleblowers may face significant risks to their livelihood and relying exclusively on the protections in California's Labor Code does not adequately address those risks or incentivize reporting. Financial awards would provide incentives for meaningful reporting, a collaboration scheme would ensure whistleblowers are supported and engaged throughout the investigative process, and

[4] *See,* Cal. Gov. Code § 12652(c)(1); 31 U.S.C. §§ 3729 – 3733; 15 U.S.C. § 78u-6 (2025); 17 C.F.R. § 240.21F-1 (2025).
[5] Cal. Labor Code § 1102.5.
[6] The Transparency in Frontier Artificial Intelligence Act, S.B. 53, California Legislature, 2025-2026 Session (2025), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB53

protections from retaliation would provide a last line of defense if a business were to take action against whistleblowers. Taken together, these provisions would encourage essential insider reporting.

Extend the Right to Delete to All Personal Information Collected About a Consumer

The CCPA grants consumers the right to request that businesses delete any personal information about them that "the business has collected from the consumer."[7] As it is currently crafted, this right does not require a business to delete a consumer's personal information if that information was collected from a third party.

However, businesses today routinely augment consumer records with data purchased from third parties to enhance targeting, personalization, and profiling. For example, a retail company might collect basic information directly from the consumer and then purchase detailed demographic data, purchasing histories, and other behavioral information from data brokers to create a rich profile used for marketing and pricing decisions.[8]

There is precedent in other privacy laws for the deletion right to require the deletion or restrict the processing of all personal information held by a business. For example, the Delete Act requires data brokers to delete all the personal information related to the consumer making the deletion request.[9] Similarly, a significant majority of state consumer privacy laws apply the right of deletion to all personal information concerning an individual.[10] These state laws typically provide that a business may comply with the deletion right for information obtained by third parties by (1) retaining the deletion request and only the minimum amount of data necessary to ensure that the consumer's data remains deleted, or (2) opting the consumer out of any processing of the third party obtained data, though some states, such as Maryland, permit only the first option.[11] Of the approximately twenty states with comprehensive consumer privacy laws, only two other states, Iowa and Utah, apply the deletion right exclusively to information collected from the consumer.[12]

The current right to deletion may create a false sense of protection by failing to address the full scope of data a company may hold and use to make decisions about individuals. Additionally, it may make businesses more vulnerable to security incidents like data

[7] Cal. Civ. Code § 1798.105.
[8] *See*, US Senate Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* at 21, December 18, 2013, https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577 (Describing how one product that data brokers provide is additional information on consumers that their customers use to supplement the data they already have on a given consumer).
[9] Cal. Civ. Code § 1798.99.86(c).
[10] *See*, Colo. Rev. Stat. § 6-1-1306(1)(d); The following states provide a right to delete that requires deletion of all personal information related to a consumer: CO, CT, DE, IN, KY, MD, MT, NE, NH, OR, RI, TN, TX, and VA.
[11] *See, e.g.*, Va. Code § 59.1-577(B)(5), which allows either option; Md. Code, Com. Law § 14-4605(E)(7), which allows only the first option.
[12] Iowa Code § 715D.3(1)(b); Utah Code § 13-61-201(2).

breaches even after a consumer has taken steps to protect the privacy and security of their information. Extending the right to delete to all personal information held about an individual would provide more meaningful privacy protections.

Require Alternative Methods for Submitting Consumer Privacy Requests

Privacy rights that are functional and accessible are critical for effective consumer privacy. Under the CCPA, online-only businesses that have a direct relationship with the consumer are only required to provide an email address for consumers to submit most privacy requests, such as requests for access, deletion, or correction.[13] In contrast, brick-and-mortar stores are required to provide two or more methods to submit those requests, including a toll-free number. This single-method requirement for certain businesses creates barriers for consumers because it offers minimal support or guidance.

Requiring additional alternative methods for privacy requests would improve usability and accessibility. For example, many state privacy laws require businesses to have one or more methods of submitting requests and require that the methods "take into account the ways in which consumers interact with the controller."[14] Providing only an email address for privacy requests is not consumer-friendly because it requires individuals to draft free-form requests that may not capture all the needed information. Alternative methods, like webforms, can provide consumers with structure and guidance on what to include in their requests. A streamlined form or portal would also ensure that businesses receive all necessary information in the first communication, limiting labor required to follow-up and clarify consumer requests.

Amending the CCPA to require that online-only businesses provide different methods for consumer privacy requests would better ensure that the rights of access, deletion, and correction are easily exercisable. This would ensure there is an accessible mechanism in place for Californians to make privacy requests.

Recommendation

Staff recommends that the Board approve the proposals included in this memo and direct staff to present them to members of the California legislature for possible authoring and Agency support. Because the decision to sponsor a bill depends on several factors, such as the amount of work that the specific bill would require and whether the author has identified other sponsors for the bill, staff recommends leaving it to staff's discretion whether to sponsor the proposals discussed above.

[13] Cal. Civ. Code § 1798.130(a)(1). Requests to opt-out of the sale or sharing of personal information or to limit the use of sensitive personal information are subject to different notification and request procedures. *See*, Cal. Civ. Code § 1798.135.
[14] *See*, *e.g.*, § Minn. Stat. 325M.15(4)(b).