

**Grenda, Rianna@CPPA**

---

**From:** Ian Moloney <ian@Fintechcouncil.org>  
**Sent:** Tuesday, June 10, 2025 4:17 AM  
**To:** Regulations@CPPA  
**Subject:** "Public Comment on Accessible Deletion Mechanism: American Fintech Council  
**Attachments:** American Fintech Council Letter on California Accessible Deletion Mechanism Proposed Rule.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To whom it may concern,

On behalf of the American Fintech Council (AFC), I am submitting the attached comment letter in response to the California Privacy Protection Agency's proposed rulemaking on the Accessible Deletion Mechanism. Please feel free to reach out if you have any questions. Thank you for your consideration of our comments.

Sincerely,

Ian P. Moloney

**Ian P. Moloney** | SVP, Head of Policy and Regulatory Affairs  
**American Fintech Council**  
853 New Jersey Ave SE Ste 200, Washington DC 20003  
T: (586) 718-6736 | [fintechcouncil.org](https://fintechcouncil.org)

**AFC** American Fintech Council



Media Partner  
**PUNCHBOWL NEWS**  
A THOMSON COMPANY

**Policy Summit**  
**November 18, 2025**  
The Westin Washington, D.C. City Center



**2025**

*HUMAN NOTICE: Getting this email out of working hours? We work at a digitally-enable relentless pace, which can disrupt our ability to sleep enough, eat right, exercise, and spend time with the people that matter most. I am sending you this email at a time that works for me. I only expect you to respond to it when convenient to you.*



June 10, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

Re: American Fintech Council Public Comment on Accessible Deletion Mechanism

To whom it may concern,

On behalf of The American Fintech Council (AFC),<sup>1</sup> I am submitting this comment letter in response to the California Privacy Protection Agency's (CPPA or Agency) Notice of Proposed Rulemaking on the Accessible Deletion Mechanism Regulations (Proposed Rule).<sup>2</sup>

AFC is the premier trade association representing the largest financial technology (Fintech) companies. Our mission is to promote a transparent, inclusive, and customer-centric financial system by supporting responsible innovation in financial services and encouraging sound public policy. Our members are also improving access to financial services and increasing overall competition in the financial services industry by lowering the cost of financial transactions, allowing them to help meet demand for high-quality, affordable financial products.

AFC respects the CPPA's efforts to implement important consumer data rights by developing the accessible deletion mechanism—referred to as the Delete Request and Opt-Out Platform (DROP). However, as written, we believe that the Proposed Rule contains provisions that contradict existing California laws and may actually harm consumers. To that end, we respectfully request that the CPPA carefully considers the analysis and recommendations detailed below.

AFC consistently advocates for pragmatic regulation that recognizes the nuances of the financial products and services, as well as the existing requirements providers must adhere to under federal and state law. We also consistently work to ensure that regulations do not inadvertently create consumer harm. As written, the Proposed Rule establishes new requirements for covered

---

<sup>1</sup> American Fintech Council's (AFC) membership spans EWA providers, lenders, banks, payments providers, loan servicers, credit bureaus, and personal financial management companies.

<sup>2</sup> California Privacy Protection Agency, "California Privacy Protection Agency Proposed Text (Express Terms): Title 11. Law Division 6. California Privacy Protection Agency Chapter 3. Data Broker Registration and Accessible Deletion Mechanism", (Apr. 25, 2025), available at [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_text.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_text.pdf).

entities that are incongruent or contradict existing California State laws, as well as their underlying legislative intent, and leaves out crucial requirements that could ensure consumers are served in a safe and sound manner.

Specifically, the Proposed Rule establishes a definition of “direct relationship” that would categorize entities that sell personal information about consumers with whom they have a direct, first-party relationship with the consumers as “data brokers”. Within the Proposed Rule’s text, it states that “[a] business does not have a “direct relationship” with a consumer simply because it collects personal information directly from the consumer; the consumer must intend to interact with the business”.<sup>3</sup> The Proposed Rule further clarifies that businesses are still data brokers and does not have a direct relationship with the consumer “as to the personal information it sells about the consumer that it collected outside of a “first party” interaction with the consumer”.<sup>4</sup>

This expansion of what constitutes a direct relationship, and therefore which entities are considered data brokers, far exceeds the legislative intent of the California State Assembly for the statute underlying the Proposed Rule.<sup>5</sup> Based on the text of the statute, it is clear that the California State Assembly intended to limit registration and other attendant requirements to businesses that do not directly interface with consumers, not categorize those entities that have existing relationships with consumers as data brokers in a wholesale manner predicated upon certain activities. Therefore, AFC respectfully requests that the CPPA review its definition of direct relationship to ensure that it does not inadvertently expand which entities constitute “data brokers” in a manner that was not intended by existing statute and remains faithful to the California State Assembly’s legislative intent on the issue.

AFC believes that, as written, the Proposed Rule lacks important verification guardrails needed to ensure that consumers are not inadvertently harmed by the execution of deletion requests for consumers who did not actually submit the requests. Unfortunately, as written, the Proposed Rule is largely devoid of requirements for verifying authorized agents and consumer requests. As noted above, the lack of provisions related to verification processes directly conflicts with existing requirements under the CCPA.<sup>6</sup>

The lack of provisions associated with the important verification processes may have been intended to allow consumers requesting deletion a more streamlined process. However, without these verification safeguards, covered entities will not have the much-needed processes in place to ensure that only the consumers actually requesting deletion of their data are actually deleted from their systems. In turn, responsible covered entities may delete information of individuals who did not make the deletion request in order to comply with the Proposed Rule’s requirements, causing significant consumer harm.

---

<sup>3</sup> Ibid, § 7601(d).

<sup>4</sup> Ibid.

<sup>5</sup> California General Assembly, Senate Bill 362, *available at* [https://leginfo.ca.gov/faces/billNavClient.xhtml?bill\\_id=202320240SB362](https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362).

<sup>6</sup> Cal. Code Regs, Tit. 11, Div. 6, Art. 5. Particularly, § 7060 and § 7063.

Specifically, the Proposed Rule requires data brokers to execute deletion requests through the DROP if more than 50 percent of the unique identifiers in a consumer deletion list match with the same consumer record maintained by the data broker.<sup>7</sup> This provision in the Proposed Rule are incongruent with existing requirements under the CCPA—promulgated in the Agency’s regulations—which state “[a] business’s compliance with a request to delete or a request to correct may require that the business verify the identity of the consumer to a **reasonable or reasonably high degree of certainty** depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction” [emphasis added].<sup>8</sup>

Simply put, the 50 percent requirement within the Proposed Regulation does not meet the threshold of a “reasonably high degree of certainty” needed to warrant the deletion of all personal information associated with that consumer. Operationally, relying on the 50 percent requirement within the Proposed Regulation will result in required deletion practices that are overly inclusive and will lead to deletion requests being actioned for consumers who did not submit requests. It is important to note that mistakenly deleting all consumer information creates significant harms to consumers who rely on their data flowing through the covered entities in order to access products and services that they need. Also, mistakenly deleting consumers’ data could result in significant legal and regulatory harm to covered entities by potentially leaving them open to consumer complaints and lawsuits related to Unfair, Deceptive, Acts or Practices (UDAP) claims.

To avoid the significant consumer and business harms associated with mistakenly deleting consumers’ information who did not make the deletion request, CPPA should ensure that it increases its deletion requirement in a manner that is commensurate with the impacts discussed above and develops prudent verification processes within the Proposed Rule.

Lastly, the Proposed Rule would require covered entities to reformat their data in a standardized manner that removes all capital letters, extraneous, and special characters.<sup>9</sup> While likely intended to streamline operations for covered entities and improve operational efficiencies, this requirement could create data security issues by mandating all databases to use certain standardization methods and may also run afoul of the First Amendment. In addition, names and spellings can hold significant cultural importance. By requiring that covered entities remove all special characters, the Agency is essentially dismissing the cultural importance of the individual consumer in a manner that is improper given the historical context associated with naming and immigration in the United States. Thus, AFC respectfully recommends that the CPPA avoids pursuing provisions related to the reformatting of covered entities’ data in a standardized manner that removes all capital letters, extraneous, and special characters.

---

<sup>7</sup> Proposed Rule, § 7613(a)(2).

<sup>8</sup> Cal. Code Regs, Tit. 11, Div. 6, Art. 5 § 7062(d).

<sup>9</sup> Proposed Rule, § 7613(a)(1)(A).

We appreciate the opportunity provide comment on CPPA's Notice of Proposed Rulemaking on the Accessible Deletion Mechanism Regulations and we thank you for your consideration of our views on the Proposed Rule. We look forward to continuing to find opportunities to collaborate on the pragmatic regulation of responsible innovations in a manner that ultimately serves consumers best.

Sincerely,



Ian P. Moloney  
SVP, Head of Policy and Regulatory Affairs  
American Fintech Council

**Grenda, Rianna@CPPA**

---

**From:** Travis Frazier <tfrazier@ana.net>  
**Sent:** Tuesday, June 10, 2025 6:59 AM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** Joint Ad Trade Comments - Public Comment on Accessible Deletion Mechanism (June 2025).pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear California Privacy Protection Agency Board:

Please find attached comments from the following advertising trade associations in response to the CPPA's request for public comment on the proposed regulations regarding an accessible deletion mechanism: the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, the Interactive Advertising Bureau, and the Digital Advertising Alliance. We appreciate your consideration of these comments.

If you have any questions about these comments, please feel free to reach out to Chris Oswald at [coswald@ana.net](mailto:coswald@ana.net).

Best Regards,  
Travis Frazier

**Travis Frazier**

Senior Manager, Government Relations | **Association of National Advertisers (ANA)**

P: 202.296.2097 | [ana.net](http://ana.net) | [LinkedIn](#)

2020 K Street, NW, Suite 660, Washington, DC 20006

**The ANA drives growth for you, your brand, our industry, and humanity. Learn how at [ana.net/membership](http://ana.net/membership).**



June 10, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

**RE: Public Comment on Accessible Deletion Mechanism**

Dear California Privacy Protection Agency:

On behalf of the advertising industry, we provide the following comments in response to the California Privacy Protection Agency’s (“CPPA” or “Agency”) request for comment on its proposed regulations regarding an accessible deletion mechanism and the Delete Request and Opt-Out Platform (“DROP”).<sup>1</sup> We and the companies we represent, many of whom do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We provide the following comments to inform the CPPA of potential unintended effects of the proposed regulations, illustrate key areas of ambiguity in the proposal, and request clarifications related to requirements for processing deletion requests made through the DROP. We thank you for the opportunity to participate in this regulatory process.

Below we provide comments on several areas the CPPA should address as it develops these rules, including: (1) the breadth of the “direct relationship” definition; (2) verification of requests submitted through authorized agents; (3) over-inclusivity of the proposed 50% match rate rule and conflicts with existing California Consumer Privacy Act (“CCPA”) regulations; (4) issues related to “standardizing” database architecture; and (5) potential data security concerns associated with the DROP. We suggest key changes to the proposed regulations to enhance their clarity, improve their operational workability, reduce security risks within the DROP, and help ensure the CPPA is acting within the bounds of the legal authority conferred upon it by the California legislature. If the CPPA finalizes the proposed regulations in their current form without making revisions to address these concerns, the regulations would raise significant constitutional and statutory issues.

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of responsible companies across the country that make up and support the digital economy. These companies range from small businesses to household brands, advertising agencies, publishers, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet and the digital economy, which accounted for 18 percent of total U.S. gross domestic product (“GDP”) in 2024.<sup>2</sup> By one estimate, over 1.8

---

<sup>1</sup> See *Notice of Proposed Rulemaking – Accessible Deletion Mechanism*, CALIFORNIA PRIVACY PROTECTION AGENCY BOARD (May 31, 2024), located [here](#). See also California Delete Act, SB 362 (Reg. Sess. 2023), located [here](#).

<sup>2</sup> John Deighton and Leora Kornfeld, *Measuring the Digital Economy*, INTERACTIVE ADVERTISING BUREAU, 8 (April, 2025), located at [https://www.iab.com/wp-content/uploads/2025/04/Measuring-the-Digital-Economy\\_April\\_29.pdf](https://www.iab.com/wp-content/uploads/2025/04/Measuring-the-Digital-Economy_April_29.pdf).



million jobs in California are related to the ad-subsidized Internet.<sup>3</sup> Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the CPPA further on the non-exhaustive list of issues with the proposed regulations that we discuss in these comments.

**I. The proposed definition of direct relationship would unreasonably broaden the scope of data brokers under the law, contrary to the statutory definition and clear legislative intent.**

The proposed regulations' definition of "direct relationship" is exceedingly broad.<sup>4</sup> As drafted, the definition could be read to require nearly all entities doing business in California to register as data brokers. Such a result would diminish the utility of the data broker registry to Californians, as the registry would no longer clearly identify "data brokers" with whom a consumer does not intentionally interact. The registry would instead amount to a list of practically *all companies* that do business in California. This outcome would conflict with the Delete Act's statutory definition of "data broker" and also run counter to legislative intent: California's data broker registration law was passed with the clear goal of requiring only those companies who do not directly interface with consumers to register. The CPPA should revise the proposed "direct relationship" definition so that the Delete Act's "data broker" definition does not capture entities that have direct, first-party relationships with consumers. As currently drafted, the proposed regulations are inconsistent with the Delete Act and exceed the scope of the CPPA's statutory authority.

Contrary to California's data broker registration law, as amended by the Delete Act, the proposed "direct relationship" definition states that even if a business has a first party relationship with a consumer, "a business is... *still* a data broker *and does not have a direct relationship* with a consumer as to personal information it sells about the consumer that it collected outside of a "first party" interaction with the consumer[.]"<sup>5</sup> Because "sell" is broadly defined to include transfers of personal information in exchange for consideration, any transfer of data that a business did not collect directly from a consumer could be considered a "sale" under California law, requiring data broker registration.<sup>6</sup> It is extraordinarily common for businesses that maintain direct, first-party relationships with consumers to augment the data they collect through first-party consumer interactions with data from third-party sources to enhance their ability to advertise and reach consumers with relevant messaging at scale. These processes include data hygiene, address standardization and updates, sales and return on investment analyses, as well as basic marketing functions. The proposed "direct relationship" definition could render all companies that do business

---

<sup>3</sup> *Id.* at 130-132.

<sup>4</sup> Cal. Code Regs. tit. 11, § 7601(d) (proposed), located [here](#).

<sup>5</sup> *Id.* (emphasis added). *See also* California AB 1202 (Reg. Sess. 2019); California Delete Act, SB 362 (Reg. Sess. 2023).

<sup>6</sup> *See* Cal. Civ. Code § 1798.140(ad).



and engage in digital advertising in California—including consumer-facing brands that directly interact and interface with consumers—to be “data brokers” in the state.

This broad definition, drawing many more entities into the scope of the term “data broker,” would be inconsistent with the Delete Act’s text and would subvert the California legislature’s intent in standing up the data broker registry and passing the Delete Act.<sup>7</sup> The Delete Act defines a “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*.”<sup>8</sup> But the CPPA’s proposed definition of “direct relationship” would broaden the meaning of “data broker” to include, in many circumstances, *even those companies that actually have direct relationships with consumers*. Specifically, those companies would be data brokers if they “sell” personal information they did not collect directly from the consumer, or, even more broadly, “sell” personal information they collected outside of a “first party” interaction with the consumer. When deliberating California’s data broker registration law, moreover, the legislature made clear that it did not intend for the CPPA to define “direct relationship” so broadly that the statutory term “data broker” would cover entities consumers transact and interact with directly. In fact, the legislative record draws a clear line between data brokers, on the one hand, and businesses with whom consumers deal directly, on the other:

[T]here are important differences between data brokers and businesses with whom consumers have a direct relationship. Consumers who have a direct relationship with businesses... may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business’ products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement.<sup>9</sup>

By reaching a broad swath of first-party businesses, the proposed regulations would be inconsistent with the Delete Act’s statutory text and exceed the authority that the California legislature granted to the CPPA under the authorizing statute.<sup>10</sup> Consumers already have visibility into these first-party businesses’ practices, where data collection from sources other than the consumer, or outside of a first party interaction, would be described in the first parties’ privacy notices, and consumers are able to exercise their privacy rights with those businesses by interacting with them and submitting consumer rights requests to them directly. Such rights requests, made directly to first parties, are effective on all non-exempt personal information those businesses

---

<sup>7</sup> See California AB 1202 (Reg. Sess. 2019), Sec. 1(g); California Delete Act, SB 362 (Reg. Sess. 2023).

<sup>8</sup> Cal. Civ. Code § 1798.99.80(c) (emphasis added).

<sup>9</sup> California AB 1202 (Reg. Sess. 2019), Sec. 1(g) (declaring legislative intent and providing legislative findings).

<sup>10</sup> *Assoc. Gen. Contractors of Ca., Inc. v. Dep’t of Indus. Rels.*, 108 Cal. App. 5th 243, 263 (2025) (regulations must be “consistent with the governing law”); Cal. Gov. Code § 11349 (“consistency” means “being in harmony with, and not in conflict with or contradictory to, existing statutes, court decisions, or other provisions of law”); see also *Assoc. Gen. Contractors*, 108 Cal. App. 5th at 264 (regulations must “be ‘within the scope of authority conferred’ on the agency by the enabling statute” (quoting Cal. Gov. Code §§ 11342.1, 11349(b))).

maintain about the consumer—including both personal information the business collected via its first-party relationship *and* personal information the business collected from other sources or outside of first party interactions with the consumer. The California legislature did not intend for first-party businesses to be required to register as data brokers and observe an accessible deletion mechanism, because consumers already have a direct touchpoint with those businesses to interact with them and submit rights requests.

The CPPA should update the proposed rules to amend the proposed definition of “direct relationship” so it does not unreasonably broaden the construct of a “data broker” beyond the scope and intent of California law. Alternatively, the CPPA should exempt businesses from registration requirements to the extent a business’s sale of personal information that it collected from a source other than the consumer to whom the information pertains is limited to advertising and marketing activities and/or sharing. This approach would reduce the confusion created when consumer-facing first parties are required to register as data brokers while still enabling consumers to directly learn about such businesses’ data practices and exercise rights.

## **II. The CPPA should ensure proper authentication of agents’ authority to assist consumers in submitting deletion requests through the DROP to avoid violating the First Amendment’s Free Speech Clause.**

The proposed regulations set forth virtually no processes or requirements for verifying agents’ authority to submit requests through the DROP on behalf of consumers.<sup>11</sup> The rules cursorily note that agents may “aid in a consumer’s deletion request” and require agents that assist consumers to provide certain contact information about themselves in the consumer’s DROP account. But the regulations do not set forth any processes or safeguards to ensure that agents have the authority to act on behalf of consumers. Absent such protections, the proposed regulations’ requirements would not help ensure that consumers have given valid authorization to agents to act on their behalf, deter fraudulent agent requests, or reduce anticompetitive intermediary interference by agents in the DROP process. The proposed regulations should be updated to require agents to observe the same verification steps as they are required to under CCPA.

Pursuant to existing CCPA regulations, if a consumer uses an agent to submit a deletion request, the business may: (1) require the agent to provide signed proof that the consumer gave the agent permission to submit the request *and* (2) ask the consumer directly to confirm their identity with the business or confirm that they granted the agent permission to make the request.<sup>12</sup> The proposed accessible deletion mechanism regulations, in contrast, do not include similar safeguards for requests submitted via the DROP. By not including these consumer rights safeguards, the proposed regulations would create a loophole that would allow entities without proper authorization to make rights requests via the Agency that otherwise would have been thwarted via verification. The proposed rules, for example, could allow an entity self-certifying itself as an authorized agent

---

<sup>11</sup> Cal. Code Regs. tit. 11, §§ 7620(b), 7621 (proposed).

<sup>12</sup> See Cal. Code Regs. tit. 11 § 7063(a).

to upload the entirety of the California White Pages directory to the DROP under the guise of being an agent for 40 million people. Compounding the concern, the proposed DROP regulations directly conflict with the CCPA regulations by explicitly stating that data brokers may not contact consumers to verify their deletion requests submitted through the DROP.<sup>13</sup>

In addition to running counter to CCPA requirements, banning data brokers from verifying consumers' intent to delete personal information through agents could allow agents to fraudulently claim they have authority to act on behalf of consumers or use coercive methods, manipulative processes, dark patterns, or other tactics to persuade consumers to give them authority to act. It could also allow entities who compete with data brokers to act as agents or work with agents to use the DROP as a means to instigate mass data deletion from data brokers to gain a competitive advantage. The proposed regulations must provide for reasonable verification of agents' authority to act on consumers' behalf to protect consumers from unauthorized data deletion and the economy from gamesmanship. The CPPA should prohibit agents from self-certifying such authority, require agents to obtain informed consent from consumers to submit requests through the DROP on their behalf, and allow for reasonable verification of this authority. The regulations to implement the DROP should be harmonized with the CCPA's authorized agent verification procedures to avoid agents using dark patterns or other gamesmanship in the DROP process. By including these measures in any final rules, the CPPA can enhance consumer protection, foster interoperability and consistency across its regulatory regimes, and help ensure agents are authorized and are acting in the interests of the consumers they say they represent.

In addition, the regulations state the CPPA "may" verify consumers' California residency prior to submitting a deletion request through the DROP.<sup>14</sup> The Agency should be required to verify consumers' residency to ensure the Delete Act is not applied beyond its scope and state borders. This residency verification requirement should be mandatory rather than discretionary to foster consistent, cohesive, and legally appropriate effectuation of deletion requests through the DROP.

The proposed regulations' lack of verification safeguards also underscores a broader issue with the Delete Act and the proposed regulations: they raise significant constitutional concerns. The Delete Act and the proposed regulations may violate the First Amendment's Free Speech Clause.<sup>15</sup> The data brokers' sale, use, and disclosure of consumer personal information is protected expression under settled Supreme Court caselaw.<sup>16</sup> Because the proposed regulations are content-

---

<sup>13</sup> Cal. Code Regs. tit. 11, § 7616(c) (proposed).

<sup>14</sup> *Id.* at § 7620(a) (proposed).

<sup>15</sup> The Delete Act and the proposed regulations, through requiring data brokers to delete data through the DROP and prohibiting the sale or sharing of any new data collected thereafter, may also constitute a regulatory taking in violation of the Takings Clause. Further, the Act and proposed regulations may violate the Contracts Clause, preventing data brokers from fulfilling their contractual obligations to customers to provide the requested data products and services.

<sup>16</sup> *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 558–59 (2011) (holding that a Vermont law unconstitutionally regulated speech where it restricted the sale, disclosure, and use of pharmacy records revealing physicians' prescribing practices when the information was used by pharmacies for drug marketing).

based, they should receive heightened scrutiny, but the regulations would fail any level of scrutiny if finalized in their current form. Among other First Amendment concerns, the regulations’ lack of verification safeguards to prevent unauthorized agents from making consumer requests, when combined with the mass-deletion mechanism, would not pass First-Amendment scrutiny because the regulations are far more extensive than necessary—i.e., they would facilitate mass deletion of data that consumers did not intend by their unauthorized agents.<sup>17</sup>

### **III. The proposed match rate rule conflicts with existing CCPA regulations and will impact the rights and freedoms of others, contravening California privacy law.**

Under the proposed rules, if the consumer deletion list that the data broker is comparing to its own records includes multiple identifiers (“IDs”), the data broker must separately compare each unique category identifier with applicable identifiers in its own records.<sup>18</sup> If more than 50% of unique IDs accessed by a data broker through the DROP match with the same consumer record, the data broker would be required to delete all personal information associated with the record.<sup>19</sup> This proposed regulation is overly broad and is likely to result in application of deletion requests to data about a consumer who did not submit such a request.

For example, the proposed regulations state: “if a data broker compares its records with a consumer deletion list that includes name, date of birth, and zip code, and only finds a match for the name and zip code with a particular consumer record, the data broker must delete that consumer’s associated personal information because approximately sixty-seven percent (67%) of the individual identifiers match with the consumer deletion list.”<sup>20</sup> As a result of this rule, if a person named John Smith living in Los Angeles zip code 90011 submits a deletion request, data brokers would be required to delete data associated with *every John Smith that lives in zip code 90011*. The CCPA explicitly states that one consumer’s deletion request shall not extend to information a business maintains on behalf of another consumer.<sup>21</sup> But the proposed rules create a construct that will result in unreasonably broad application of deletion requests and that will—contrary to the statute—impact the rights and freedoms of other California consumers by resulting in deletion of data they did not wish to remove from the marketplace.

In addition, this proposed rule does not align with the CCPA’s regulations related to data point matching to verify consumer deletion requests. CCPA regulations require businesses to verify consumer deletion requests to a “reasonable or reasonably high degree of certainty depending on the

---

<sup>17</sup> See *Milavetz, Gallop & Milavetz, P.A. v. United States*, 559 U.S. 229, 249 (2010) (laws subject to intermediate scrutiny must “directly advance a substantial government interest and be no more extensive than necessary to serve that interest”).

<sup>18</sup> Cal. Code Regs. tit. 11, § 7613(a)(2)(A) (proposed).

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> See Cal. Civ. Code § 1798.145(k) (“The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request... to delete a consumer’s personal information pursuant to Section 1798.105... shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person.”)

sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion[.]”<sup>22</sup> A “reasonably high degree of certainty” requires matching at least three pieces of personal information provided by the consumer with personal information maintained by the business “that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request.”<sup>23</sup> The DROP regulations, requiring deletion of a consumer record if there is a 50% match of relevant identifiers, directly conflict with this CCPA regulatory provision. The CPPA should update the DROP regulations so they are harmonized with existing verification requirements for data deletion requests in the CCPA regulations. Failure to do so could give rise to a claim under the California Administrative Procedure Act that the final regulations are not “consistent with the governing law.”<sup>24</sup>

#### **IV. Requiring data brokers to “standardize” customer records is an unduly onerous requirement that would impact the integrity of datasets.**

The proposed regulations would require a data broker to “standardize” its own customer records by using all lowercase letters, “removing extraneous or special characters” such as punctuation, math symbols, and other characters, and implementing other standardization methods “to increase the likelihood of a match between its records and the applicable consumer deletion list.”<sup>25</sup> This requirement would be extraordinarily burdensome, particularly for small and mid-sized data brokers.

Special characters and capital letters are commonly used in data elements maintained about consumers, such as email addresses, and data brokers’ customers expect the data they receive to include these characters and capitalization formatting. As a result, the proposed standardization requirement would functionally force data brokers to maintain multiple databases to house the same data in different ways, because otherwise they could no longer effectively deliver the services their customers bargained for. Data brokers of all sizes would, for example, need to maintain one “standardized” database for matching purposes under the DROP and a separate database with the capital letters and special characters that data brokers’ customers expect. This requirement would impose a significant cost on small and mid-sized data brokers to take on the expense of maintaining a separate database to facilitate DROP requests. Smaller and mid-size entities would be placed at a significant disadvantage. The proposed “standardization” requirement would unreasonably interfere with the accuracy and functionality of data brokers’ proprietary datasets and should be removed from the proposed regulations.

Compelling data brokers to “standardize” proprietary internal records in a prescribed format raises additional First Amendment concerns because this requirement affects data brokers’ ability to

---

<sup>22</sup> Cal. Code Regs. tit. 11, § 7062(d).

<sup>23</sup> *Id.* at § 7062(c).

<sup>24</sup> *See Assoc. Gen. Contractors*, 108 Cal. App. 5th at 263.

<sup>25</sup> Cal. Code Regs. tit. 11, § 7613(a)(1)(A)(ii) (proposed).



convey their desired message to customers. This requirement effectively compels data brokers to structure databases in a way that changes how they compile, use, and communicate consumer data.<sup>26</sup> Because the proposed regulations would require data brokers to substantively alter the contents of their databases to “increase the likelihood of a match” between customer records and the identifiers maintained in the DROP, these alterations may have downstream effects on the reports and data compilations that data brokers provide to their customers.<sup>27</sup> That, too, would burden data brokers’ ability to communicate with customers in the manner they choose.

**V. The CPPA should be required to report breaches to data brokers registered through the DROP.**

In the event of a breach of data broker credentials used to access the DROP, the proposed rules would require data brokers to notify the Agency immediately in writing and take certain remedial steps.<sup>28</sup> Similar obligations should be placed on the Agency in the event of a data breach to help ensure data security and protect consumer privacy. Through the DROP, the State of California is creating a database of personal information about California consumers and is enabling connections with data brokers through automated means.<sup>29</sup> As a result, any data breach impacting the DROP has the potential to create security risks for the data brokers that maintain automated connections with the DROP system. At a minimum, the CPPA should be required to report data breaches impacting the DROP to all registered data brokers so data brokers can take any necessary steps to prevent further security incidents impacting their own information systems and databases.

\* \* \*

---

<sup>26</sup> *DoorDash, Inc. v. City of New York*, 750 F. Supp. 3d 285, 298–99 (S.D.N.Y. 2024) (analogizing to *Sorrell* and reasoning that the communication of consumer data is protected speech, and that the challenged New York City law implicated the First Amendment by compelling such speech).

<sup>27</sup> Cal. Code Regs. tit. 11, § 7613(a)(1)(A)(iii) (proposed).

<sup>28</sup> *Id.* at § 7610(a)(1)(C)(ii) (proposed).

<sup>29</sup> *Id.* at §§ 7612(b), 7614(b) (proposed).





Thank you in advance for your consideration of these comments.

Sincerely,

Christopher Oswald  
EVP for Law, Ethics & Govt. Relations  
Association of National Advertisers  
202-296-1883

Alison Pepper  
EVP, Government Relations & Sustainability  
American Association of Advertising Agencies, 4As  
202-355-4564

Michael Hahn  
EVP & General Counsel  
Interactive Advertising Bureau  
212-380-4700

Clark Rector  
Executive VP-Government Affairs  
American Advertising Federation  
202-898-0089

Lou Mastria  
CEO  
Digital Advertising Alliance  
347-770-0322

CC: Mike Signorelli, Venable LLP  
Allie Monticollo, Venable LLP

**Grenda, Rianna@CPPA**

---

**From:** Leder, Leslie <leslie.leder@calchamber.com> on behalf of Daylami, Ronak <ronak.daylami@calchamber.com>  
**Sent:** Tuesday, June 10, 2025 3:40 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on the Accessible Deletion Mechanism  
**Attachments:** CalChamber Comment Letter\_Accessible Deletion Mechanism\_DROP platform (June 10, 2025).pdf  
  
**Importance:** High

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To whom it may concern:

Please see comments from the California Chamber of Commerce on the Accessible Deletion Mechanism, attached.

Best,

**Ronak Daylami**  
Policy Advocate

  
HR Expert & Business Adv  
California Chamber of Commerce  
1215 K Street, 14th Floor  
Sacramento, CA 95814  
C: [REDACTED]

Visit [calchamber.com](https://calchamber.com) for the latest California business legislative news plus products and services to help you do business.

*This email and any attachments may contain material that is confidential, privileged and for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient or have reason to believe you are not the intended recipient, please reply to advise the sender of the error and delete the message, attachments and all copies.*

June 10, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

Submitted electronically to: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

SUBJECT: **“Public Comment on Accessible Deletion Mechanism” (PR 04-2025)**

The California Chamber of Commerce (“CalChamber”) submits these comments in response to the California Privacy Protection Agency (“CPPA” or “Agency”) request for public input on the Accessible Deletion Mechanism,<sup>1</sup> for to the implementation of the Delete Request and Opt-Out Platform (“DROP”) System Requirements. CalChamber’s members reflect a diversity of small, medium, and large businesses across industries and sectors in the state and approximately a quarter of all California private sector jobs.<sup>2</sup>

1. The proposed definition of “direct relationship” would significantly broaden the scope of the data broker definition beyond what the Legislature authorized, or even intended, the Agency to regulate.

The proposed definition of direct relationship **in the Agency’s draft regulations** could make any business a data broker if it sells personal information it did not collect through a first-party interaction with a consumer.<sup>3</sup> Because “sale” is defined broadly to include any transfer of personal information in exchange for monetary or other valuable consideration,<sup>4</sup> many entities—including those with first-party consumer relationships—are likely to fall under this expanded data broker definition. It is extremely common in the marketplace for consumer-facing brands and other companies to augment the first-party data they collect directly from consumers with data from third-party sources to enhance their ability to provide custom offers to existing customers and to reach new customers through advertising. The proposed direct relationship definition could make any business that transfers its data augmented from third-party data sources for an advertising or marketing purpose **in a transaction that meets the “sale” definition** a “data broker” subject to registration and accessible deletion mechanism requirements. That would effectively turn the California data broker registry into a list of virtually all companies that do business in the state.

Expansion of the data broker term through the proposed definition of direct relationship would also conflict with legislative intent and existing California law. While the Agency cites SB 362 (Becker, Chapter 709, Statutes of 2023), also known as the Delete Act, for its authority, the **definition of data broker, and in particular the reference to “direct relationship” takes root from** another piece of legislation altogether: AB 1202 (Chau, Chapter 753, Statutes of 2019), where the

---

<sup>1</sup> CPPA, *Proposed Regulations on Accessible Delete Mechanism – Delete Request and Opt-out Platform (“DROP”) System Requirements* (April 25, 2025), available at: <https://coppa.ca.gov/regulations/drop.html>

<sup>2</sup> See CalChamber, *CalChamber Membership*, <https://www.calchamber.com/calchambermembership#:~:text=CalChamber%20membership%20represents%20one%2Dquarter,thrive%20through%20challenges%20and%20adversity>.

<sup>3</sup> Cal. Code Regs. tit. 11, § 7601(d) (proposed), located [here](#).

<sup>4</sup> See Cal. Civ. Code § 1798.140(ad).

Legislature adopted the Data Broker Registry that SB 362 later modified. AB 1202 was enacted on the heels of the Legislature approving AB 375 (Chau, Chapter 55, Statutes of 2018) by the same author, enacting the California Consumer Privacy Act (CCPA).

The resulting 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.<sup>5</sup> In 2019, when the Legislature initially passed the data broker registration statute, it acknowledged and discussed important differences between data brokers and first-parties, stressing the fact that consumers have the ability to directly contact first-parties and submit rights requests to them.<sup>6</sup> The Legislature has never expressed any intent for the CCPA to broaden the statutory definition of data broker in a manner that would encompass first parties that have direct relationships with consumers. Had it wanted to do that, it could have done so in SB 362, when it **updated the definition of “data broker” among other aspects of the Data Broker Registry Law.**

The impact of such a change almost cannot be overstated. It is as though the Agency were to say a consumer has never interacted with a business that shipped the consumer their order and potentially even handled their return—simply because they placed the order on another **company’s website. Even though the fulfillment partner sent the consumer emails, processed** their personal information, provided customer service, and is a known entity to the consumer—because they do not have a first party relationship, they are to be deemed a total stranger. That is **the effect of this regulation. It regards these businesses as “data brokers” simply because they** were not the first click; even when they are clearly part of the experience. That is obviously not what the lawmakers had in mind when they passed AB 1202. They were thinking of the practical challenges some consumers might face when effectuating their CCPA rights given the potential gap in consumer awareness as to the identity of third-party data brokers they have no reason to know may have come into possession of their information.<sup>7</sup> And it was not what stakeholders understood the law to mean, either under AB 1202 or SB 362. If such a change is to be made, it **must be made by the state’s elected policy makers, not a regulatory body.**

The **Agency’s definition of “direct relationship” in these proposed regulations** thus conflicts with clear legislative intent and inappropriately expands the statutory data broker definition. In doing so, it will create new liability and remove protections from those first parties, as further discussed below. The CCPA should update the proposed definition of direct relationship to ensure it does not capture first party entities that the California legislature intended to exclude from

---

<sup>5</sup> Cal. Civ. Code § 1798.99.80(c).

<sup>6</sup> CA AB 1202 (Reg. Sess. 2019), Sec. 1(g).

<sup>7</sup> See the author’s statement of intent, reflected in the Asm. Privacy & Consumer Protection Com., analysis of AB 1202 (2019-2020 Reg. Session), Mar. 26, 2019, p. 5.

“This bill would better allow privacy conscious consumers to exercise their rights granted under CCPA and develop a more thorough understanding of the data industry’s scope and practices. It will also allow for a modicum of oversight over an industry that has so far been allowed to thrive with little to no obligations to the public or to the individuals whose personal information provides the foundation for their industry. In a world where an individual’s real time location, arrest record, rental history, or court filings are available online, and conveniently aggregated for purchase, people deserve, at a minimum, to know who is collecting information about them, and to have the ability to opt-out of the sale of their personal information. AB 1202 would consolidate data brokers into one easily accessible list so that consumers may exercise their rights.”

*See also* Sen. Floor, analysis of AB 1202 (2019-2020 Reg. Session) Sept. 10, 2019, p.7.) which, at the time that the bill was approved, expressly recognized that “AB 1202 would consolidate data brokers into one easily accessible list so that consumers may exercise their rights.”

classification as a data broker under the law, and also to ensure alignment with the CCPA, given the underlying objective of the law is to assist consumers in exercising their CCPA rights with third party entities.

2. The proposed DROP regulations are inconsistent with existing CCPA regulations, including its requirement for verification of deletion requests.

The CCPA rules require verification of a deletion request to a “reasonable” or “reasonably high degree of certainty,” the latter requiring matching of at least three data points from a consumer to data maintained in a business’s systems.<sup>8</sup> The proposed rules differ from this requirement by mandating that data brokers process DROP deletion requests if at least 50% of identifiers on a deletion list match to a consumer record in the data broker’s systems.<sup>9</sup> When matching to a deletion list containing a name, date of birth, and zip code, for example, the data broker would be required to delete data associated with consumers who matched at least two of the three data points provided.<sup>10</sup> This result directly conflicts with the CCPA regulations, which may require matching of at least three data points depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion.<sup>11</sup> The CCPA should update the proposed regulations to ensure they are consistent with the existing CCPA regulations.

- A. The proposed identity matching requirements provide an insufficient basis for a threshold to delete all personal information.

The proposed DROP regulation’s threshold will lead to over-inclusive deletion of consumer information *of people who did not actually submit requests* as the threshold is too low to ensure that the correct person is identified. Specifically, the threshold used is “[i]f more than fifty percent (50%) of the unique identifiers” in a consumer deletion list “match with the same consumer record in the data broker’s records.” If so, the data broker would be required to delete all personal information associated with that consumer.<sup>12</sup> The problem is easily illustrated by the example provided in the proposed regulations: where the available data fields are name, date of birth, and zip code, as long as there is a match for the name and zip code, that would be sufficient to trigger the deletion of all information relating to that name and zip code, the threshold will have been met. Two fields would account for a 67% match in identifiers and therefore fall above the 50% threshold.

Consider the surname Rodriguez, which is one of most popular family names in the United States, belonging to approximately 298 out of every 100,000 people.<sup>13</sup> And consider the given name Jose, which belongs to approximately 328 out of every 100,000 people.<sup>14</sup> Looking to the California zip code 90001, which a population of approximately 56,000 people and an approximately 91% (52,642) Hispanic population,<sup>15</sup> using the statistical frequency of the name Jose Rodriguez in the U.S., and the demographic composition of zip code 90001, we can infer that there may be as many as 210-315 people in that zip code sharing that name. This is just one singular example used to demonstrate both the ease with which there can be, and the high probability of there being, erroneous “matches” where only name and zip code are used to dictate deletion requests, and common names are not uncommon, particularly where approximately 18-

---

<sup>8</sup> Cal. Code Regs tit. 11, § 7062(c).

<sup>9</sup> Cal. Code Regs. tit. 11, § 7613(a)(2)(A) (proposed).

<sup>10</sup> *Id.*

<sup>11</sup> Cal. Code Regs tit. 11, § 7062(c).

<sup>12</sup> Proposed § 7613(2).

<sup>13</sup> <https://www.mynamestats.com/Last-Names/R/RO/RODRIGUEZ/index.html>

<sup>14</sup> [https://www.mynamestats.com/First-Names/J/JO/JOSE/index.html#google\\_vignette](https://www.mynamestats.com/First-Names/J/JO/JOSE/index.html#google_vignette)

<sup>15</sup> <https://zipatlas.com/us/ca/zip-code-90001.htm>

20% of Americans—totaling nearly 60 million people—live in multigenerational households with cultural, name-preserving traditions where family names are passed down along generations. Using a match of just these two of three identifiers is too low a standard to trigger deletion and highly likely to lead to scenarios where records belonging to multiple people sharing common names would risk improper deletion.

By then requiring a data broker to instead opt out *each associated consumer* out of the sale or sharing of their PI if the data broker associates multiple consumers with a matched identifier from the consumer deletion list (presumably to avoid improper deletion), the low verification threshold risks turning the deletion portal into a mass opt-out system deleting data for consumers who never wanted their data deleted, or to opt-out—taking away consumer choice and the right to control their data privacy from those Californians. In other words, by setting such a low threshold for identity matching, the Agency will in many cases be assuming or inferring consent it does not have to *associated consumers*. Giving Californians control over their own personal data was of course a core principle of both the CCPA that gave rise to the Data Broker Registry in AB 1202, and the Delete Act in SB 362 – not to mention that it violates the text of the Delete Act, *which requires the consumer to request deletion*<sup>16</sup>.

Of concern, however, the proposed DROP regulations require very little verification of consumer requests at all. Indeed, there are virtually no safeguards for ensuring the identity of the consumer making a deletion request. While there appears to be authorization for the Agency to **verify an individual’s residency and guidelines for consumer compliance with such requests**,<sup>17</sup> there is actually no mandate to determine that the individual is a resident of the state. It should go without saying that permitting verification of specific data elements does not provide protection in the same way that requiring it does—one is permissive and can be ignored; the other is mandatory and cannot.<sup>18</sup> This is simply inadequate from as a consumer privacy protection.

We propose that the Agency adopt the approach taken under the CCPA, which requires a business to establish reasonable methods for verifying that the person making a request to delete is the consumer with whom the business has collected information and to consider whether the personal information provided is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.<sup>19</sup> The Agency should incorporate into the proposed regulations the **balancing used in the CCPA’s right of deletion, which requires that the deletion request be balanced against the “risk of harm to the consumer posed by any unauthorized deletion[.]”**<sup>20</sup> **Under that framework, a consumer’s identity must be verified to a “reasonable”**<sup>21</sup> **or “reasonably high degree of certainty”**<sup>22</sup> in conjunction with a request, depending on the sensitivity of the data, with the latter requiring at least three data points to match the consumer before a business must effectuate the request.<sup>23</sup> Such changes would better ensure the effectuation of this particular

---

<sup>16</sup> Cal. Civ. Code § 1798.99.86(2).

<sup>17</sup> See Proposed § 7620(a).

<sup>18</sup> Proposed § 7620(b) provides that “[c]onsumers may add personal information to their deletion requests, including date of birth, email address, phone number, and pseudonymous identifiers, such as a Mobile Ad Identifier (MAID)” and the Agency “may verify such personal information at any time”). Proposed § 7620(b) (emphasis added).

<sup>19</sup> See Cal. Code Regs. tit. 11, § 7060.

<sup>20</sup> Cal. Code Regs. tit. 11, § 7060(c)(3)(B).

<sup>21</sup> “A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.” Cal. Code Regs. tit. 11, § 7062(b).

<sup>22</sup> “A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer[.]” Cal. Code Regs. tit. 11, § 7062(c).

<sup>23</sup> Cal. Code Regs. tit. 11, § 7060(c)(3).



privacy right in a more consumer protective manner that aligns with the core principle of both the CCPA and DELETE Act, which hold that the consumer should determine their own data privacy.

- B. The proposed DROP regulations create a loophole for authorized agents by failing to bind them to the same obligations they must observe when they submit rights requests directly to businesses.

We are very concerned that the proposed regulations also fail to provide guardrails to prevent fraudulent requests from agents purporting to act on behalf of consumers. We caution the Agency to not overlook the fact that very real privacy concerns can arise even when promoting consumer-friendly policies. Take, for example, the right of access to specific pieces of personal information under the CCPA. It quickly became obvious in the passage of AB 375 that the Legislature could inadvertently create one of the biggest threats to privacy at the same time that it passed landmark privacy rights if a person could fraudulently represent that they are the consumer or the **consumer's authorized representative and obtain all of his or her specific pieces of personal information. Which is why the concept of a "verified consumer request" was added to the law.**

Under existing CCPA regulations, an authorized agent must prove a consumer gave signed **permission for the agent to submit the request on the consumer's behalf.**<sup>24</sup> Businesses are also permitted to ask consumers to verify their own identities directly with the business or directly confirm with the business that they gave the agent permission to act on their behalf.<sup>25</sup> By contrast, the DROP rules contain no safeguards to ensure an agent has actual authority to submit a deletion request on behalf of a consumer. The proposed regulations, in fact, explicitly state that data brokers may not contact consumers to verify their choices.<sup>26</sup> Stated another way, it prohibits them from ensuring that they are not deleting the information of the wrong individual, or potentially even received a fraudulent request.

The Delete Act does not provide statutory authority to prevent data brokers from verifying that authorized agents are who they say they are, and in fact mandates that the deletion **mechanism "shall** allow data brokers registered with the California Privacy Protection Agency to determine whether an individual has submitted a verifiable consumer request to delete the **personal information related to that consumer[.]**"<sup>27</sup> In doing so, the Agency has exceeded its statutory authority with these particular provisions and we ask that you revise the draft regulation accordingly, to align with the statute.

Under these proposed rules, the DROP would be ripe for intermediary interference, as agents **alleging authority to act on consumers' behalf would be subject to no meaningful safeguards** to verify that authority. This lack of verification could allow entities that compete with data brokers to use the DROP as a method to request mass data deletion from registered data brokers to gain a competitive advantage and disrupt legitimate commerce. The CPPA should update the proposed regulations to require authorized agents to provide the same proof of authority to act on behalf of Californians, as is required of them under the CCPA regulations, or to allow data brokers to verify such requests directly with consumer.

Stated another way, as it stands, the differing requirements between the proposed regulations and the CCPA regulations creates a loophole: if the proposed DROP is implemented as is, an agent who is unable to provide proof they actually have permission to act on behalf of the consumer can perform an end-**run around the CCPA's verification requirements by using the DROP rather than**

---

<sup>24</sup> Cal. Code Regs. tit. 11 § 7063(a).

<sup>25</sup> *Id.*

<sup>26</sup> Cal. Code Regs. tit. 11, § 7616(c) (proposed).

<sup>27</sup> Cal. Civ. Code § 1798.99.86(b)(3) (emphasis added).

going directly to a business to submit a deletion request under the CCPA. The CPPA should amend this draft to be consistent with the CCPA regulations permitting data brokers to (1) ask authorized agents to submit signed proof of their authority to act on behalf of the consumer when submitting requests through DROP and (2) confirm with consumers directly that they have authorized the agent to act on their behalf.<sup>28</sup>

C. The DROP regulations should ensure consumers receive information necessary to provide informed consent.

The Agency should ensure that the DROP clearly discloses to consumers the scope of a deletion request to enable consumers to make an informed decision before committing to the – irreversible – deletion of their personal information, which has many different implications. Informed consent is a bedrock principle of California privacy law. Under the CCPA, for example, **“consent” is defined as a “freely given, specific, informed, and unambiguous indication of the consumer's wishes[.]”**<sup>29</sup> A consumer cannot make an informed choice to submit a deletion request if they are unaware of the benefits and drawbacks of doing so. For example, the result of submitting a deletion request may include the loss of access to:

- Civic engagement: Nonpartisan organizations use demographic data to provide voter registration information, polling location details, and ballot measure explanations to eligible voters who may otherwise be unaware of these opportunities.
- Educational and scholarship information: Schools use data to identify and reach students who may be eligible for educational programs or grants they may not otherwise hear about.
- Community resources: Local organizations use public data to target food assistance, housing programs, job training, or social services to people who may need them.
- Financial benefits: Businesses routinely offer consumers discounts and information on receiving financial benefits. For example, roofing companies convey information to homeowners after natural disasters on how to navigate the insurance process after a roof repair; entities located people eligible for health insurance exchanges after the passage of the Affordable Care Act to help them enroll.

Consumers have the right to receive speech, commercial and otherwise<sup>30</sup>. Advertising is not just selling products; it also involves providing advice and support. Unless amended, the proposed DROP regulations would leave consumers unaware of important consequences of deleting their information. The Delete Act itself contemplates that consumers may find some information **sharing useful by mandating that DROP “[a]llow a consumer to selectively exclude specific data brokers from a request” to delete.**<sup>31</sup> If consumers do not know the kinds of information they are excluding when they view this list, this mandate is meaningless. The final regulations should account for the need to educate consumers about the consequences of submitting a deletion request that informs consumers of both the benefits and the drawbacks of such requests.

---

<sup>28</sup> The CCPA regulations require authorized agents to “provide proof that the consumer gave the agent signed permission to submit the request.” Cal. Code Regs. tit. 11, § 7063(a). In addition, the business may require the consumer to either (1) verify their own identity directly with the business; or (2) directly confirm with the business that they provided the authorized agent permission to submit the request. Cal. Code Regs. tit. 11, § 7063(a).

<sup>29</sup> Cal. Civ. Code § 1798.140(h) (emphasis added).

<sup>30</sup> See *infra*, section II.a

<sup>31</sup> Cal. Civ. Code § 1798.99.86(a)(3).

3. There should be a delayed enforcement period and a right to cure initially for DROP compliance.

The initial version of the CCPA provided for a 30-day right to cure<sup>32</sup> as well as a delayed enforcement period that allowed covered entities time to make changes to prepare for compliance, as well as respond and address alleged violations before facing an enforcement action. Given the substantial undertaking required of data brokers to adjust their compliance processes to comply **with the DROP and the state's experience with the CCPA's right to cure** successfully helping businesses transition to a new regulatory regime, we ask the Agency to consider similar rights here, with an appropriate sunset date, in the final regulations. At the very minimum, delayed enforcement should be provided to give businesses enough time to assess and implement changes necessary to comply with new requirements, particularly if our concerns regarding verification issues and alignment with the CCPA are not fully addressed.

4. The Agency has not specified how the proposed registration fees are related **to the Agency's reasonable costs.**

The Delete Act authorizes “a registration fee in an amount determined by the [CPPA], not to exceed the reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84 and the reasonable costs of establishing, maintaining, and **providing access to the accessible deletion mechanism described in Section 1798.99.86.**”<sup>33</sup> Under California law, “a fee may be charged by a governmental entity so long as it does not exceed the reasonable costs of providing services necessary to regulate the activity for which the fee is charged” and “may not be imposed for unrelated revenue purposes.”<sup>34</sup>

Excluding payment processing fees, the maximum registration fee under these proposed DROP regulations is \$6,600.<sup>35</sup> The minimum is \$550.<sup>36</sup> Given that there are approximately 528 data brokers in California, the fees generated under the proposed regulations could total around **\$3.5 million. The Agency's Economic and Fiscal Impact Assessment**<sup>37</sup> for the proposed regulations states fiscal costs associated with the regulation were \$2,477,000 in 2025/26 and anticipated to be \$2,340,000 in 2026/27 with future costs to be covered by the data broker registration fees but does not explain how it reached these cost figures or how the registration fees are reasonably related to them as required.<sup>38</sup>

5. Constitutionality concerns

Although we do not address them at length in this comment, CalChamber has concerns regarding the constitutionality of the proposed regulations, including potential infringements on **individuals'** First Amendment rights to free expression and to access information, not only in terms of commercial speech, but also in terms of other forms of speech, press, and political freedom which are distinctly separate concepts from commercial speech and require higher levels

---

<sup>32</sup> Originally codified at Cal. Civ. Code § 1798.155(b), which provided: “A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.” Cal. Civ. Code § 1798.155(b).

<sup>33</sup> Cal. Civ. Code § 1798.99.82(b)(1) (emphasis added).

<sup>34</sup> *Am. Coatings Assn., Inc. v. State Air Res. Bd.*, 62 Cal. App. 5th 1111, 1125, 277 Cal. Rptr. 3d 284, 295 (2021). But “[t]he mere fact a fee exceeds the reasonable costs of providing the service or regulatory activity for which it is charged does not transform the fee into a tax.”

<sup>35</sup> Proposed § 7611(a)(3)(A).

<sup>36</sup> Proposed § 7611(a)(3)(L).

<sup>37</sup> [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_std\\_399.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_std_399.pdf)

<sup>38</sup> [Economic Impact Statement](#), p. 5, item 4.

of scrutiny. These stem primarily from the risk of inadvertent mass opt-outs due to the lax identity matching standards<sup>39</sup> and the inadequate provisions for informed consent<sup>40</sup> will result in the restriction of information to consumers without their consent.<sup>41</sup> A strict scrutiny review would require the state to demonstrate the regulation (1) is narrowly tailored (2) to achieve a compelling governmental interest and (3) that it is the least restrict means of achieving that interest. It is our view that the proposed DROP regulations overlook a number of better-tailored and more-effective alternative approaches, and there are strong arguments that they are not sufficiently drawn to serve the state's interests.


We also believe that in this case, there may be issues of first impression and strong arguments that the proposed regulations should be subjected to higher scrutiny as opposed to intermediate scrutiny that would typically be applied to commercial speech, since we believe these proposed regulations fail that standard under the second prong of the *Central Hudson* test, which requires the state to assert a substantial interest to be achieved by restriction on commercial speech. Here, the courts have been clear that the assertion of privacy as a substantial state interest is insufficient to pass that second prong.<sup>42</sup>

Thirdly, by forcing data providers to alter the nature of their databases by reformatting their language in a way that will undermine the integrity of the connections between data points, we believe the government may be unconstitutionally depriving businesses of their property interests without just compensation, in violation of the Fifth Amendment's Takings Clause, as incorporated against the States by the Fourteenth Amendment, which provides that private property shall not "be taken for public use, without just compensation."<sup>43</sup>

\* \* \*

CalChamber appreciates the CPPA's consideration of these comments, and we look forward to continuing to work with the Agency on these important issues.

Sincerely,



Ronak Daylami  
Policy Advocate  
California Chamber of Commerce

---

<sup>39</sup> See *supra*, section I.b.

<sup>40</sup> See *supra*, section I.c.

<sup>41</sup> "The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers." *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982).

<sup>42</sup> *Central Hudson Gas & Electric Corp. v. Public Service Commission* (1980) 447 U.S. 557. Courts "pay particular attention to attempts by the government to assert privacy as a substantial state interest" due to the "breadth of the concept of privacy", because "the government cannot satisfy the second prong of the *Central Hudson* test by merely asserting a broad interest in privacy ... [but rather] must specify the particular notion of privacy and interest served." See *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234 (10th Cir. 1999).

<sup>43</sup> U.S. Const. amend. V.



**Grenda, Rianna@CPPA**

---

**From:** Jacob Brint <jacob@calretailers.com>  
**Sent:** Monday, June 2, 2025 10:41 AM  
**To:** Regulations@CPPA  
**Cc:** Sarah Pollo  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT and Insurance Regulations  
**Attachments:** Cal Retailers Comments Letter on CPPA Updates, Cyber, Risk, ADMT, and Insurance Regulations\_6.2.25.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Hello,

Attached are the California Retailers Association's comments regarding the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations, based on the May 1st CPPA hearing.

For your reference, our comments from the February meeting are also included at the end of the letter.

Best,

**Jacob Brint**

Legislative and Regulatory Manager

California Retailers Association

1121 L Street, Suite 607

Sacramento, CA 95814

O: (916) 443-1975

C: [REDACTED]

[jacob@calretailers.com](mailto:jacob@calretailers.com)





June 2, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350 Sacramento, CA 95811

VIA Email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

## **Cal Retailers Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

Dear Members of the Committee:

The California Retailers Association (Cal Retailers) is submitting the following concerns we have on the modified regulatory text, which is based on the May 1 CCPA hearing, regarding Automated Decision-making Technology (“ADMT”), risk assessments, and cybersecurity. We have also attached our original letter submitted to the CCPA in February for reference.

### **§ 7001(e) – ADMT Definition:**

#### **Request to revise as follows:**

- On 1(b), revise: “information that is relevant necessary to make . . .” As currently framed, it is unclear what info would be relevant and may be impossible for a human reviewer to consider all such factors. If a business has a protocol on what info is needed to make a decision or exception, then that should be sufficient.
- On (3), remove “provided that they do not replace human decision making,” as it otherwise removes the purpose of the exception. And if a company were to make a decision based solely on a calculator, while perhaps not advisable, it should not be within scope.
- On (3), add “search term software” to exclude when recruiters or employers conduct manual searches using terms to narrow the scope of a recruitment pool.

### **§ 7001(ddd) – Significant Decision:**

#### **Request to revise as follows:**

- Under the Significant Decision definition “employment or independent contracting opportunities or compensation” should be removed.
- Under (4), Cal Retailers requests that employment related decisions be limited to hiring or firing—not decisions related to allocation or assignment of work, compensation, bonuses, etc.

### **§ 7010 (d):**

Cal Retailers seeks the removal of this provision. A persistent option for opt-out through a link, versus a just-in-time option, is not as consumer friendly. Consumers are unlikely to have the context needed to know to access the link. The business should determine the appropriate interaction based on its relationship with the consumer and nature of the processing.



The ideal approach would give business flexibility to determine how to offer opt-out; specifically, where PI is being processed for a significant decision, a business should be able to offer the opt-out as part of the user experience that leads to that decision.

**§ 7150(b):**

Cal Retailers would like the removal of this provision. If this does not prove possible, we have included some feedback along with revisions below.

**Feedback:**

The rules still regulate the use of ADMT to process publicly available information, as a consumer's presence on a college campus or a grocery store with a pharmacy is not private information. The CPRA otherwise regulates the use of data collected from geo-trackers that identify a consumer's precise geolocation, regardless of the location. As sensitive data, a controller must still conduct a risk assessment (per these regs) and provide an opt out. The overbreadth would capture low risk activities such as providing discounts for (i) prescriptions at specific pharmacies based on a consumer's prior use or (ii) college merchandise based on a student's residence at a specific college.

**Potential Revisions:**

- (3) – Seek the below revisions to this provision:
  - Using ADMT for a significant decision concerning a consumer that presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers.
- (4) – Seek removal of this provision.
- (5) – Profiling Sensitive Location – Seek removal of this provision.
- (7) - Seek the creation of a new provision utilizing the below text:
  - A risk assessment completed under another law that is substantially similar to the assessment required under this Article will satisfy the requirements of this Article.

**§ 7152(a)(3) – Risk Assessment Requirements:**

The purpose of the risk assessment is to make sure the business considers and weighs the privacy harms resulting from certain high-risk processing activities. As businesses continue to innovate, the nature of in-scope processing activities will change. Businesses should retain flexibility in how to approach assessments to make sure that they identify and weigh the right factors. However, the approach in the proposed rules under § 7152 is overly prescriptive and may force businesses to view assessments as a check-the-box exercise rather than focusing on the factors that ultimately matter for the assessment.

The cost of this approach to business and innovation outweighs the privacy benefits to consumers. California companies operate nationally and internationally. Under almost all other privacy laws including GDPR, a business will prepare risk assessments tailored to the processing activity rather than follow the CPPA's formulaic approach. Yet since the proposed rules do not permit a business to rely entirely on an assessment prepared to meet the requirements for another jurisdiction, a business will need to prepare a California-specific supplement for the same processing activity. The CPPA has not explained how this approach will provide incremental benefits to consumer privacy. See § 7156 below for more info.

### **§ 7156 Interoperability of Risk Assessments:**

The modified regulatory text continues to require a California risk assessment to include all the specific requirements under this regulation. Instead, it should follow the approach of all other state privacy laws and permit businesses to rely on assessments prepared for other laws that are reasonably similar in scope and effect. For instance, Colorado requires data protection assessments for (1) processing personal data for targeted advertising (defined as equivalent to “*cross-context behavioral advertising*,” not “*behavioral advertising*”) and profiling if the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial or physical injury to consumers; (iii) physical or other intrusion on the solitude, seclusion, or private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury; (2) selling personal data; and (3) processing sensitive data.

Moreover, other state privacy laws that require “*risk assessments*” (i.e. “*data protection assessments*”) for high-risk activity limit the scope of activities requiring such assessments in similar circumstances to (1) the processing of “*sensitive data*,” which could include location information ***but only when such data is precise geolocation information***, and (2) profiling, ***but only when it presents a reasonably foreseeable risk of the following***: unfair or deceptive treatment of (or unlawful disparate impact on) consumers, financial or physical injury, physical or other intrusion on the solitude or seclusion – or private affairs or concerns – of consumers if it would be offensive to a reasonable person (***hardly the case in a publicly available space, where consumers do not have a reasonable expectation of privacy***), or other substantial injury.

As currently written, the draft rules contemplate interoperability only between similar “*risk assessments*” and do not contemplate “*data protection assessments*.” Further, the draft rules are rather stringent in requiring that a company may only forego a risk assessment if (1) the other “*risk assessment*” created for the purpose of complying with another law or regulation “*meets all the requirements of this Article*,” and (2) if it covers a “*comparable set of processing activities*,” defined as processing activities that “*present similar risks to consumers’ privacy*.” Of course, an entity would not know if an activity presented similar risks until it conducts the risk assessment, thereby the purpose of this provision.

(F): This is an example of how the rule leans more toward the prescriptive rather than functional. Section (a)(1) already requires an assessment to identify the processing purpose, and then (a)(3)(F) requiring mapping those purposes to specific third parties. A business should consider in its assessment both processing purposes and sharing, but this mapping will not always be necessary—especially when a business already discloses categories of data sharing in its privacy notice and the purpose of processing in its agreements with service providers.

(G)(1) [limited to significant decisions]: As described below at § 7220(c)(5), research is still ongoing in how to explain the logic of ADMT models. Moreover, the focus on methodology is not tethered to the risk to the consumer—privacy or otherwise. Instead, the risks are related to an adverse impact of a significant decision and whether a data subject can exercise rights. These are sufficiently addressed by other RA provisions.

### **§ 7157 Submission of Risk Assessments to the Agency:**

The draft rules require companies to submit abridged forms of their risk assessments on an annual basis to the CPPA. Routine submission is not only burdensome, but inconsistent with other state privacy laws and may result in reduced privacy protections as businesses may prepare assessments in a way that is legally protective rather than focused on the right risk-benefit balancing.

However, the CPRA statute mandates that the CPPA issue regulations that require submission at a regular cadence. For instance, the statute does not preclude the CPPA from setting separate standards for what processing activities trigger a risk assessment vs what activities are sufficiently risky to trigger a submission. This would allow the CPPA to focus on those assessments that are highest risk, such as those involving the sale of sensitive data.

Further, the rules require companies to submit risk assessments in the employment context to the regulator, but in most instances, any decisions in the employment context are confidential and not available to competitors. We'd likely need an exception to not require the submission of information that is confidential business/trade secret information.

**§ 7157(b):**

It is still unclear what the CPPA plans to do with this information. Per our prior points, consider limiting the requirement to certain processing activities only—e.g., sales of sensitive data. Alternatively, seek to limit the substance to metrics, i.e. the number of assessments, and drop (4). Companies are otherwise required to disclose in their privacy notice the types of personal data that they collect, process, and share. Unclear how adding this to the submissions will produce any greater benefit for the Agency.

**§ 7150(a)(1) – Significant Decision:**

This should be limited in the same manner and for the same reasons above at § 7150(b)(3)(A). § 7200(a)(1) extends application to all uses of ADMTs for decisions regarding provision of, denial of, or access to, employment and employment compensation. Per the regulation, this includes almost all activity within the scope of the employment lifecycle: hiring, promotion/demotion; suspension/termination; and, during employment, allocation/assignment of work; setting of base and incentive compensation; and decisions regarding “other benefits.” This also includes “independent contracting opportunities,” i.e., the same activities in the IC, gig-economy, and other emerging work contexts.

**§ 7150(b)(6) – AI/ADMT Training:**

On limiting AI training assessments for models used for significant decisions, we support the revised scope to exclude language covering models that are “capable” of certain purposes and to instead limit to models where the business “intends to use” for those purposes. However, as defined in revised text, the term “intends to use” also covers “permits others to use, plans to permit others to use” and advertising such uses. This language should be removed, as it conflicts with the “intent” language and will bring in scope a wide-range of general use models that are primarily used for other, low-risk purposes. The proposed rules otherwise cover (i) if a deployer intends to use a model to make a significant decision or (ii) a deployer modifies a model with supplemental training that it then intends to use to make a significant decision.

The rules should not extend risk assessments to processing for training a model that is used for emotion recognition, if it does not otherwise involve identifying a specific person (which is already covered). It should also not expressly call out training for models used for biological identification. Risk assessments already extend to processing of sensitive data (which includes biometric data as defined under CPRA). If a deployer is using such a model for biological identification, then RAs already apply. Same if a developer uses biometric data to train a model. But it should not extend to models that are not trained on biometric data—otherwise the rules remove an incentive for developers to minimize the sensitive data that they use in training.

**§ 7200(a)(1) – Significant Decision:**

See above at 7001(ddd)

The first sentence of 7200(b) should be removed—a business should not have to provide a risk assessment where ADMT was used prior to effective date and is not used on or after the effective date.

**§ 7200(a)(2)(A) - Extensive Profiling (Profiling of Employees):**

This should be limited in scope.

**§ 7200(a)(2)(B) - Extensive Profiling (Publicly Accessible Spaces):**

This should be limited in scope.

**§ 7200(a)(2)(C) - Extensive Profiling (Behavioral Advertising):**

This should be limited in scope.

**§ 7150(a)(3) - AI/ADMT Training:**

This should be limited in scope.

**§ 7220(a) – When Required:**

As a threshold matter, the CPRA does not permit regulations on pre-use notice of ADMT—instead, CPRA § 1798.185 calls for regulations “*governing access and opt-out rights*,” with respect to ADMT. The access right (addressed below) covers the information that a business needs to provide about its ADMT, and so CPPA should not issue separate and overlapping rules on notice.

At minimum, pre-use notice should be limited to where the ADMT processing is otherwise subject to access and opt-out rights. To the extent that one of these customer rights does not apply (e.g., relying on security or fraud prevention exception), then the business should not have an obligation to post this notice. In other words, section 7220(a) should apply subject to the exceptions in § 7221(b) and § 7222(a)(1).

This makes practical sense as forcing a business to make disclosures on how it uses ADMT to perform these functions would undermine the safety and security of consumers and businesses. The notice must provide extensive details about the use of the ADMT, which will be difficult to draft and likely not useful to the consumer, particularly where a business uses ADMT in multiple ways and must provide several notices. Consumers may not be well-equipped to evaluate information about how ADMT works and the logic behind the ADMT.

**Suggested Revision:**

CPPA did not revise the regulations to limit the pre-use notice requirement to only where ADMT processing is otherwise subject to access and opt-out rights. As a result, businesses will be required to provide such notices even if they use ADMT for exempt purposes for which consumers do not have the right to access or opt out. Amend § 7220(a) as follows:

- A business that uses automated decision-making technology as set forth in section § 7200, subsection (a), and subject to the exceptions in section § 7221(b) and section § 7222(a)(1), must provide consumers with a Pre-Use Notice.

**§ 7220(c)(5):**

Our preference is to delete pre-use notice entirely. If pre-use notice is required, it should be limited to manageable information.

**Suggested Revisions:**

- Amend § 7220(c)(5)(A) as follows: The categories of personal information processed by the ADMT.
- Strike § 7220(c)(5)(B)

**§ 7220 – Notices:**

While the updated rules include the appropriate carveouts (§ 7200(d)), it still requires the notice to include a significant amount of information. The most problematic are (A) and (B), which requires disclosing the type of outputs generated and how the output is used to make a significant decision. Per our original concerns, the CPPA should consider whether this helps the consumer and whether risks are better mitigated through an assessment that requires rigorous testing.

On (A), unclear how it relates to 7222(b)(2) re access right, as one requires disclosing how ADMT processes personal info to decide and other the ADMT logic.

**§ 7221(a) – Opt-out of ADMT:**

Our preference is to delete the right to opt-out entirely, as this is administratively difficult to implement without significant consumer benefit unless there is an adverse decision. If the right cannot be deleted, it should only apply as a right to appeal in the event of an adverse decision, like the Colorado AI Act and other similar laws, as per the below.

An exception for cybersecurity uses previously included in the regulations should be re-inserted as this type of safe harbor is critical to allowing businesses to safely protect consumer data from unauthorized uses.

**Suggested Revisions:**

- Amend § 7221(a) to read as follows: In the event of an adverse significant decision having legal or similarly significant effect, a business must provide consumers with the ability to appeal the decision and in that appeal opt-out of the use of ADMT to make a significant decision concerning the consumer, except as set forth in subsection (b).
- Amend § 7221(b) to add the following sections and text:
  - (1) The business's use of that automated decision-making technology is necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below ("security, fraud prevention, and safety exception"):
  - (A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information.
  - (B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
  - (C) To ensure the physical safety of natural persons; or
  - (D) To protect property or rights or defend against legal claims.

**§ 7221(b)(4) & (5) – Employee Exceptions:** Cal Retailers requests that the CPPA remove the limiters "solely" in both exceptions—so long as the ADMT is not used to make another type of significant decision, then the opt out should not apply. As written, it suggests that the exception would not apply to ADMT that is used for both assignment of work and how the business manages its products and services—even though the latter is not a significant decision.

The standard "ensures" sets an unreasonably high bar. Propose revising to say that a business must take reasonable measures to ensure. Also, an ADMT deployer should be able to rely on an assessment or instructions from developer rather than conduct an independent assessment.

### **§ 7221(f)**

#### **Request to Amend entire section to the following text only:**

- A business may require a verifiable consumer request for a request to opt-out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of ADMT.

### **§ 7222 (a) – When Access Right Applies:**

This provision in the modified text still requires that business's responses be specific to the specific consumer making the request (see previous Cal retailers letter attached).

At a minimum, the access right should be limited to an adverse decision. A company should not be required to explain details about when and how it uses technology when no harm is involved, such as where a consumer is pre-approved for credit. This follows the approach of FCRA and the Equal Credit Opportunity Act. We are not aware of any other regulatory regime that requires a company to disclose how it made a non-adverse decision to a consumer. We request the removal of section § 7222 (a)(b)(2).

The same opt-out exceptions for employment uses (under § 7221(b)) should be added here. If the terms ADMT and significant decisions are broadly interpreted to include interim hiring decisions or filtering tools, then it will be impractical to require a business to respond to consumer-specific access requests on how the ADMT was applied to them, regardless of whether it was adverse. This will eliminate the advantages of using automated tools in the first place.

### **§ 7222(b) – Response to Access Request:**

We propose limiting the right to access to situations in which the consumer has actually been subjected to an adverse significant decision. Perhaps including a Pre-Use Notice as a baseline disclosure, and then only upon an adverse decision could a consumer potentially obtain more individualized info.

#### **Suggested Revisions:**

- On (1), per above, this should be limited at minimum to where the ADMT use resulted in an adverse decision.
- On (2), this language should be removed, even if limited to were used for an adverse decision. Other regulatory regimes that require a business to explain an (adverse) decision do not require disclosing methodology (eg, under FCRA, the notice when taking an adverse action based on a consumer report must explain that an adverse action occurred, identify the consumer rights, and provide contact info of consumer reporting agency—but not the methodology of the decision making). It does not relate to any privacy risk to the consumer but instead creates a moral hazard in that the primary benefit to consumers of accessing a methodology is to either copy it for their own business needs or use it to game the system, defeating the purpose of the technology and harming all consumers.
- On (3), this is inconsistent with the definition of ADMT, which is limited to technologies that fully replace or substantially replace human decision-making. As framed, it suggests that this requirement applies to interim automated tools. To the extent the rule is seeking to inform consumers about the purpose of the decision, then that is already covered under (1). Again, the outcome at most should be limited to adverse decisions, per 7222(a) above.



### **§ 7222(k) – Adverse Significant Decisions:**

In the employment context, the rules give companies too little time to effectively provide detailed, and in parts, data specific to each individual decision—a bar too burdensome given the broad applicability. In the case of an “*adverse significant decision*” (suspension, demotion, termination, or reduction in compensation), the business must provide notice of the right to access within 15 days of the adverse decision, and with detailed information within 45 days. Upon request, the business must provide “*a plain language explanations*” — requiring interpretation — of the purpose of the ADMT, and more concerningly, (a) the specific outputs the ADMT produced after processing the individual’s data; (b) the way in which the business used (and plans to use) the ADMT output and human assessment in making decisions regarding that individual; (c) the “*extensive profiling*”, if any, performed by the business using an ADMT; and (d) the precise “*logic*”, “*key parameters*”, and “*range of possible outputs or aggregate output statistics*” of the ADMT, so the individual can understand the workings of the tool and how the specific decision came to be. Little of this information will be helpful to the individual and will require extensive interpretation on behalf of a company to produce this information in “*plain language*” to an individual—often in each specific “*adverse significant decision*.”

### **Behavioral Advertising – Fallback:**

The scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply the access right to this type of ADMT processing.

### **Suggested Revisions:**

See previous comments to strike “*behavioral advertising*.”

We also have concerns with the way § 7123(f) is currently drafted. As written, it is effectively useless as it says another audit can only be used if another audit has all the same requirements as the CCPA audit. No other audit regime looks like the CCPA audit, so businesses will always be required to conduct a separate audit for CCPA. Most businesses already conduct annual audits for ISO certification. We suggest the regulations include common security audit frameworks that will be accepted as compliant with these regulations without requiring businesses to make the determination whether they meet all the requirements the agency requires.

Related to this, the specific controls outlined in § 7123(b) risk becoming outdated quickly. Most current cybersecurity audit standards focus on assessing how organizations achieve security outcomes. For example, NIST recommends controls such as: “The confidentiality, integrity, and availability of data-at-rest are protected.” In contrast, the proposed regulations mandate specific technical controls to achieve these outcomes—for instance, requiring assessment of “Encryption of personal information, at rest.” As an example, § 7123(b)(2)(A) emphasizes multi-factor authentication (MFA) and password requirements, even though many companies are now transitioning to passkeys and other modern authentication methods. We recommend removing subsections (E) and (P), which we believe are overly prescriptive. Additionally, we request that subsection (O) be revised to exclude third parties, as this could result in businesses being required to audit their peers—raising concerns around feasibility and confidentiality.

We also believe the definition of a “security incident” in § 7123(b)(2)(Q) is overly broad. Specifically, including violations of a business’s internal program—rather than focusing on unauthorized access—does not align with industry standards for incidents that may require reporting. This could conflate internal compliance issues with actual security events.

Finally, we recommend the following:

- A limitation on the requirement to submit full audit reports,
- The ability to redact sensitive security and proprietary information, and

- A requirement that the CPPA maintain strict confidentiality and security of submitted reports.

### **Additional Issues:**

In addition to the concerns outlined above, we respectfully raise the following issues with the proposed regulations, which may create unintended consequences or conflict with existing statutory frameworks:

**1. Over-Inclusive Deletion Threshold:**

The proposed regulations would require data brokers to honor deletion requests submitted through the DROP if more than 50% of the unique identifiers provided match a single consumer record. This threshold is overly broad and could result in the deletion of personal information for individuals who did not actually submit a request. Additionally, this approach conflicts with existing CCPA regulations, which require verification of deletion requests to a “reasonable” or “reasonably high degree of certainty,” depending on the sensitivity of the data. For more sensitive information, verification typically requires at least three matching data points before a business is obligated to act.

**2. Lack of Verification for Authorized Agents:**

The proposed DROP regulations lack sufficient safeguards to verify that authorized agents are legitimately acting on behalf of consumers. This omission conflicts with existing CCPA regulations, which require agents to provide signed authorization from the consumer and allow businesses to verify the consumer’s identity directly or confirm the authorization. Without similar verification requirements in the DROP process, a significant loophole is created that could be exploited by unauthorized agents.

**3. Insufficient Consumer Verification Requirements:**

The proposed regulations do not mandate adequate verification to confirm that a deletion request is being made by the actual consumer. While there are limited guidelines for verifying residency, there is no requirement to confirm that the individual is a California resident. Moreover, although the regulations allow for verification of specific data elements, they do not require it. This is inconsistent with existing CCPA rules, which obligate businesses to establish reasonable methods for verifying the identity of the requestor and to assess whether the personal information provided is robust enough to prevent fraudulent or spoofed requests.

**4. Mandated Data Standardization Raises Concerns:**

The proposed rules would require all registered data brokers to reformat their databases to conform to a standardized format prescribed by the CPPA—such as removing capital letters, extraneous characters, and special symbols. This requirement could introduce data security risks by enforcing uniform formatting across systems and may also raise First Amendment concerns by compelling how business’s structure and maintain their data.

**5. Improper Expansion of the “Data Broker” Definition:**

The proposed expansion of the “data broker” definition through the revised interpretation of “direct relationship” exceeds the CPPA’s regulatory authority. By including entities that have a first-party relationship with consumers—such as those that sell personal information but also directly interact with consumers—the CPPA is contradicting legislative intent. The California Legislature clearly intended to limit data broker registration and compliance obligations to entities that do not have a direct relationship with consumers.

Again, we appreciate the opportunity to provide comments on the modified regulatory text but continue to urge a thoughtful reconsideration of these regulations to ensure they protect consumers without

unduly burdening businesses or stifling innovation. California's position as a global leader in AI research and development is at stake, and a balanced, well-deliberated approach is crucial for maintaining our competitive edge while safeguarding consumer interests.

If you have any questions or need additional information on our comments included in this letter, please do not hesitate to contact me directly.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Brint'.

Jacob Brint  
Policy Advocate

Original Cal Retailers letter included on following pages.



February 19, 2025

California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

VIA Email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov).

## **Cal Retailers Comments on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

Dear Members of the Committee:

The California Retailers Association respectfully urges reconsideration of the proposed regulations regarding Automated Decision-making Technology (“ADMT”), risk assessments, and cybersecurity, as they may inadvertently hinder California's economic growth and innovation while potentially falling short of their intended consumer protection goals. We believe a more balanced approach is necessary to safeguard both consumer privacy and the state's economic vitality.

The Standardized Impact Assessment (SRIA) reveals concerning projections: over 52,000 California businesses could face compliance costs, resulting in a \$3.5 billion economic impact. This burden may disproportionately affect small businesses, forcing them to divert resources from growth and innovation to legal and compliance needs. The SRIA also forecasts significant job losses, peaking at 126,000 in 2030, and state revenue losses of up to \$2.8 billion annually by 2028.

We appreciate the importance of consumer privacy but believe the proposed regulations may exceed the scope of the California Consumer Privacy Act (CCPA). Even Alastair Mactaggart, author of the California Privacy Rights Act, has expressed concerns about the rules' scope. We suggest that AI regulations be developed through a more inclusive process led by the Legislature and the Newsom Administration, ensuring a thorough evaluation of costs, benefits, and budget impacts.

The proposed regulations, particularly those concerning Automated Decision-Making Technology (ADMT), may unintentionally impede online transactions and research. Multiple pop-up notifications could frustrate consumers and hinder their online experiences, potentially harming small and local businesses that rely heavily on e-commerce. We recommend simplifying notice requirements to focus on high-risk activities, benefiting both consumer privacy and business efficiency. Furthermore, the regulations may inadvertently discourage the use of AI technologies that could enhance efficiency, productivity, and growth across various sectors. By treating low-risk AI applications similarly to high-stakes decisions, we risk losing valuable opportunities for innovation and economic advancement.

We respectfully suggest that the California Privacy Protection Agency (CPPA) collaborate closely with Governor Newsom and the Legislature to develop a risk-based approach that addresses genuine consumer risks while fostering innovation. This approach would align with the Governor's Executive Order on AI, which aims to harness AI's benefits for Californians while avoiding a patchwork of conflicting regulations.

We would also like to share very specific examples within the proposed regulations to illustrate why we encourage the board to take time to collaborate with the Governor and the Legislature on this important issue.

**EXAMPLE #1 - The draft regulations inappropriately attempt to limit first party advertising:** The draft regulations are overly broad and exceed the California Privacy Protection Agency's (CPPA) authority to regulate beyond what was expressly included in the California Consumer Protection Act (CCPA) and the amendments voters approved in the California Privacy Rights Act (CPRA). CCPA clearly exempted information a business acquires through its own interaction with consumers while CPRA amended CCPA to restrict **cross-contextual behavioral advertising** by requiring a business to obtain a consumer's consent before it could share the consumer's personal information with **third parties**. Instead of providing businesses with implementation guidance, the draft regulations inappropriately attempt to broaden the scope of the CPPA's authority by granting consumers a right to opt-out of ADMT and restrict businesses' use of **first party data**. Many consumers expect businesses to provide relevant product recommendations and personalized ads that correspond to items they have previously purchased or considered purchasing to be able to take advantage of special offers and competitive pricing of goods and services. Many businesses also provide customers with opportunities to restrict how a business can use personal information it has collected about them if they choose. The draft regulations inappropriately violate the First Amendment by restricting businesses' free speech right to advertise their products and services without government interference. The draft regulations provide no compelling state interest for restricting speech, and they do not set forth a narrowly tailored solution to achieve their desired outcome.

**EXAMPLE #2: The draft regulations inappropriately attempt to regulate Automated Decision-Making Technologies (ADMT):** It is inappropriate for CPPA to use its authority to regulate data privacy as justification for regulating ADMTs and apply a data privacy protection framework when this type of technology was not clearly contemplated by CCPA or CPRA. Last year, the California Legislature considered, but did not pass legislation to regulate ADMTs. The Legislature and Governor continue to consider the appropriate restrictions on AI technology. The Governor signed AB 2013 imposing training data transparency requirements, but vetoed other bills attempting to regulate AI. The Governor has noted the importance of striking the appropriate balance between providing industry incentives to innovate without enacting arbitrary restrictions on technology that will stifle competition and has invited continued conversation on this topic with the Legislature. CPPA is encroaching upon the power of the Legislature to legislate with its attempt to usurp authority to regulate ADMTs.

**EXAMPLE #3: The draft regulations do not appropriately distinguish between significant decisions and non-significant decisions:** Effective AI laws regulate conduct, not the technology itself; otherwise, continued technological advancement renders them obsolete. For example, Colorado's AI law distinguishes between consequential and non-consequential uses of generative AI and grants consumers the right to appeal consequential decisions to ensure that human review is part of any decision pertaining to a consumer's access to education, employment, financial services, housing, health care, or legal services. Individuals are afforded analogous protection under the EU AI Act. The CPPA's draft regulations do not recognize or describe what would be considered a "significant harm" under existing California law, nor do they refer to any examples that would point to these areas of existing law. As a result, the draft regulations do not provide enough clarity on what would be considered a "significant decision" for businesses to meaningfully rely upon to ensure their compliance with California law.

**EXAMPLE #4: The draft regulations interfere with regular business operations under existing law:** The draft regulations' requirements for cybersecurity audits force a business' board of directors to perform managerial tasks instead of delegating those tasks to business leaders who are better qualified to execute them. For example, the draft regulations require a board member to sign a written statement they have reviewed stating they understand the findings of the cybersecurity audit. This is not an appropriate requirement given the role of a board of directors is to provide strategic planning, leadership,



and guidance, not to weigh in on day-to-day business decisions for which the board member may or may not have the appropriate level of experience or expertise to meaningfully evaluate.

**EXAMPLE #5: The draft regulations impose burdensome compliance requirements without**

**appropriate justification:** The purpose of cybersecurity audits is to ensure that businesses who process significant amounts of sensitive personal information have appropriate safeguards in place to protect consumers from the risk of harm of this information becoming public. The draft regulations provide no threshold to evaluate the significance of the risk of harm to consumers before imposing additional costly and burdensome cybersecurity requirements upon the organization. As directed in CCPA and as amended by CPRA, the draft regulations should have provided a methodology to consider the complexity of the business and the type of information it processes before imposing additional cybersecurity requirements.

**EXAMPLE #6: The draft rules include several concerning provisions that may mandate businesses to compromise their proprietary info and IP (e.g., how the logic operates and the key parameters that affect the output).** The rules should clarify that no provision shall be construed to require the disclosure of trade secrets or confidential or proprietary information about the design or use of an automated system. Also, per § 1798.185(a)(3), the CPPA must issue rules to clarify that companies are not required to disclose trade secrets or proprietary information.

We also have concerns with specific sections of the proposed regulations.

**§ 7001(f) – ADMT Definition** - The definition of ADMT is overbroad. Including technology that “*substantially facilitates human decision making*” (i.e., “*using the output of the technology as a key factor in a human’s decision making*”, as when “*a human reviewer uses [an output] as a primary factor to make a significant decision about them*”) will require an impossible line-drawing exercise (what is a “key/primary factor”? when are other factors considered by the reviewing human “key/primary” when they produce the same result recommended by the ADMT?), and will chill use of innovative technologies in California. An ADMT should not “*substantially facilitate human decision-making*” when it (i) performs a narrow procedural task, (ii) improves the result of a previously completed human activity, (iii) detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review, or (iv) performs a preparatory task to an assessment relevant to a significant decision.

**§ 7150(b)(3)(A) – Significant Decision** - In every other US State law that defines “*profiling*,” such profiling is tied to a legal or similarly significant decision. And in those states, a decision that produces legal or similarly significant effects is a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services or basic necessities, such as food and water. Providing consumers with the right to opt-out of profiling (and any other associated rights) is not an easy feat. As such, to the extent California will provide consumers with the right to opt-out of profiling (and other similar rights), those rights should be available only when they will significantly impact consumers.

**Suggested Revision:** Revise as follows – “For purposes of this Article, “*significant decision*” means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions I-(g), or 1798.146, subdivisions (a)(1), (4), and (5), ~~that results in access to, or~~ the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment ~~or independent contracting opportunities or compensation~~, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).”



**§ 7150(b)(3)(B)(i) – Extensive Profiling (Profiling of Employees)** - It is not clear what the “*extensive profiling*” concept accomplishes that would not be addressed by the privacy risk assessment requirement for “significant decisions” concerning a consumer, which include decisions about provision or denial of educational or employment opportunities. The statute defines **profiling** as automated processing “*to evaluate certain personal aspects concerning that natural person,*” and therefore, it seems extensive “*profiling*” would be encompassed by the privacy risk assessment requirement for significant decisions. The CCPA should avoid duplicative requirements that are likely to confuse California businesses and consumers.

**Suggested Revision:** Strike § 7150(b)(3)(B), or at minimum, subpart (i).

**§ 7150(b)(3)(B)(ii) – Extensive Profiling (Publicly Accessible Spaces)** - The requirement to undertake risk assessments for extensive profiling is fundamentally in tension with the statutory text, which explicitly exempts “*publicly available information*” (i.e., information made available to the consumer to the public or from widely distributed media or if the consumer has not restricted the information to a specific audience). When a consumer is in public spaces, they have made a deliberate decision not to restrict the information to a specific audience, and moreover, have no reasonable expectation of privacy.

Accordingly, the CCPA makes clear that requirements for businesses, processors, and contractors, including the creation of risk assessments, do not apply to publicly available information, which includes information collected and processed in public spaces.

The definition of publicly available spaces is also unworkably broad and suggests that it encompasses not only parks and sidewalks, but also shopping areas, stadiums, and other places of congregation. The breadth of this definition would be extremely onerous for California businesses, especially small businesses, without a countervailing benefit to consumers.

**Suggested Revision:** Strike § 7150(b)(3)(B). If any part of this subpart (ii) remains, it would be helpful to clarify that “*publicly accessible place*” excludes the “*internet*” (similar to the EU AI Act), by clarifying that it refers to a **physical** place that is open to or serves the public.

**§ 7150(b)(3)(B)(iii) – Extensive Profiling (Behavioral Advertising)** - While other state privacy laws require a risk assessment for “*targeted ads*,” the draft rules significantly expand and alter what would be required—(i) it would extend to all behavioral ads rather than only CCBA (the focus of the statute) and (ii) impose detailed requirements that are not calibrated to the potential risk, since no consumer data is being shared with third parties or combined with other third-party data.

**Suggested Revision:** Strike § 7150(b)(3)(B), or at minimum, subpart (iii).

**§ 7150(b)(4) – AI/ADMT Training** - ADMT/model training should not be a category subject to heightened obligations (risk assessments, notice, opt out).

(1) Training a model is not “*automated decision-making*” in its core—because the “*training*” does not involve a decision that has an impact on a specific consumer—and so should be out of scope for these rules. The rules aim to cover certain high-risk AI/ADMT applications, such as when used to make a significant decision. But here, the rules would also cover developing tools that could provide lots of low-risk processing, but would still be in scope because they could one day be used for a higher risk application.

The actual use of ADMT/AI systems for these higher-risk applications would still be covered under these rules, and so extending obligations to the training of such tools is both misplaced and unnecessary. In other words, this training category expands the type of technologies that are subject to these obligations because many if not all models “*could*” be used to make a significant decision.

This "*theoretical*" approach is inconsistent with other risk-based frameworks focused on automated decision-making used to make a significant decision. This is a different issue because training a model on personal data is different from making a decision about that person (or otherwise creating any risk for them).

(2) This also exceeds the subject matter of what the CCPA contemplates, i.e., the privacy risk that may result from the processing of personal data. The statute and rules already provide ways for consumers to control how their data is used for training—they can opt out of ADMT that results in legal or similarly significant effects, access the data that a business processes about them, correct their data, and delete their data. The CPPA should not use this rulemaking to impose risk assessments that regulate AI training more broadly, when untethered to the privacy risk.

(3) The CPPA significantly departs from the approach taken in other state privacy frameworks, which neither mention nor provide heightened requirements for the use of personal information for model training. It also differs from the one other AI law (CO), where model training is not considered a high-risk decision. Also, California passed AB 2013 this year, which already imposes disclosure requirements on training data.

**Suggested Revision:** Strike §7150(b)(4)

**§ 7154(a) – Prohibition of Certain Activities:** The draft rules will prohibit processing of personal info for any covered activity if the risks outweigh the benefits. This is an extreme prohibition, and goes far beyond other AI regulations (e.g., the EU AI Act bans very limited categories of uses). It will also discourage innovation since the balance between benefits and risks is highly subjective and may be close depending on what perspective is applied (e.g., what qualifies as a risk or benefit varies wildly among experts). As an alternative, consider formulation used for unfairness under other legal regimes is the processing likely to cause substantial harm to consumers that is not reasonably avoidable (e.g., an opt out after reasonable notice and option for human review), and the injury is not outweighed by the benefit to consumers. This formulation limits the restriction to only processing that causes “substantial harm” rather than where there is only a non-material impact, and acknowledges that through the opt out, consumers can make their own choice about whether to permit the activity (rather than regulators making the choice for them).

**Suggested Edit:** Strike § 7154(a).

**§ 7156 Interoperability of Risk Assessments:** The rules governing “*risk assessments*” should align and be interoperable with the requirements for data protection assessments in other states. For instance, Colorado requires data protection assessments for (1) processing personal data for **targeted advertising** (defined as equivalent to “*cross-context behavioral advertising*,” not “*behavioral advertising*”) and **profiling** if the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial or physical injury to consumers; (iii) physical or other intrusion on the solitude, seclusion, or private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury; (2) **selling** personal data; and (3) processing **sensitive data**.

Moreover, other state privacy laws that require “*risk assessments*” (i.e. “*data protection assessments*”) for high-risk activity limit the scope of activities requiring such assessments in similar circumstances to (1) the processing of “*sensitive data*,” which could include location information **but only when such data is precise geolocation information**, and (2) profiling, **but only when it presents a reasonably foreseeable risk of the following:** unfair or deceptive treatment of (or unlawful disparate impact on) consumers, financial or physical injury, physical or other intrusion on the solitude or seclusion – or private affairs or concerns – of consumers if it would be offensive to a reasonable person (**hardly the case in a publicly available space, where consumers do not have a reasonable expectation of**

**privacy**), or other substantial injury.

As currently written, the draft rules contemplate interoperability only between similar “*risk assessments*” and do not contemplate “*data protection assessments*.” Further, the draft rules are rather stringent in requiring that a company may only forego a risk assessment if (1) the other “*risk assessment*” created for the purpose of complying with another law or regulation “*meets all the requirements of this Article,*” and (2) if it covers a “*comparable set of processing activities,*” defined as processing activities that “*present similar risks to consumers’ privacy.*” Of course, an entity would not know if an activity presented similar risks until it conducts the risk assessment, thereby the purpose of this provision.

**§ 7157 Submission of Risk Assessments to the Agency:** The draft rules require companies to submit abridged forms of their risk assessments on an annual basis to the CPPA. Routine submission is not only burdensome, but inconsistent with other state privacy laws and may result in reduced privacy protections as businesses may prepare assessments in a way that is legally protective rather than focused on the right risk-benefit balancing.

However, the CPRA statute mandates that the CPPA issue regulations that require submission at a regular cadence. For instance, the statute does not preclude the CPPA from setting separate standards for what processing activities trigger a risk assessment vs what activities are sufficiently risky to trigger a submission. This would allow the CPPA to focus on those assessments that are highest risk, such as those involving the sale of sensitive data.

Further, the rules require companies to submit risk assessments in the employment context to the regulator, but in most instances, any decisions in the employment context are confidential and not available to competitors. We’d likely need an exception to not require the submission of information that is confidential business/trade secret information.

**§ 7150(a)(1) – Significant Decision:** This should be limited in the same manner and for the same reasons above at § 7150(b)(3)(A). § 7200(a)(1) extends application to all uses of ADMTs for decisions regarding provision of, denial of, or access to, employment and employment compensation. Per the regulation, this includes almost all activity within the scope of the employment lifecycle: hiring, promotion/demotion; suspension/termination; and, during employment, allocation/assignment of work; setting of base and incentive compensation; and decisions regarding “other benefits.” This also includes “independent contracting opportunities,” i.e., the same activities in the IC, gig-economy, and other emerging work contexts.

**§ 7200(a)(2)(A) - Extensive Profiling (Profiling of Employees):** This should be limited in scope.

**§ 7200(a)(2)(B) - Extensive Profiling (Publicly Accessible Spaces):** This should be limited in scope.

**§ 7200(a)(2)(C) - Extensive Profiling (Behavioral Advertising):** This should be limited in scope.

**§ 7150(a)(3) - AI/ADMT Training:** This should be limited in scope.

**§ 7220(a) – When Required:** As a threshold matter, the CPRA does not permit regulations on pre-use notice of ADMT—instead, CPRA § 1798.185 calls for regulations “*governing access and opt-out rights,*” with respect to ADMT. The access right (addressed below) covers the information that a business needs to provide about its ADMT, and so CPPA should not issue separate and overlapping rules on notice.

At minimum, pre-use notice should be limited to where the ADMT processing is otherwise subject to access and opt-out rights. To the extent that one of these customer rights does not apply (e.g., relying on

security or fraud prevention exception), then the business should not have an obligation to post this notice. In other words, section 7220(a) should apply subject to the exceptions in § 7221(b) and § 7222(a)(1).

This makes practical sense as forcing a business to make disclosures on how it uses ADMT to perform these functions would undermine the safety and security of consumers and businesses.

**Suggested Revision:** Amend § 7220(a) as follows: *A business that uses automated decision-making technology as set forth in section § 7200, subsection (a), and subject to the exceptions in section § 7221(b) and section § 7222(a)(1), must provide consumers with a Pre-Use Notice.*

**§ 7220(c)(5) – Explainability:** The draft requires businesses to explain, in plain language, the logic used in the automated decision-making technology, including the key parameters that affect the output of the automated decision-making technology. We recommend deletion of this provision as it is effectively an explainability requirement. Research in the field of explainable ADMT is progressing rapidly, but many complex AI models (which tend to be the most useful ones) are not yet fully explainable. Indeed, requiring an explanation now could result in consumer confusion. CCPA should therefore consider whether it would benefit California to impose this requirement, or whether there are other better methods to mitigate risk such as human review and rigorous testing.

The draft rules are also in tension with the statute's explicit recognition that the CCPA's requirements do not require the business to disclose trade secrets (Cal. Civ. Code 1798.100(f)). The exception under § 7220(c)(5)(C) is too narrow. This is particularly important in the HR context, because HR deals with not only employee confidential data, but also beta and pilots for products that should be excluded as confidential business/trade secret information.

**Suggested Revision:** Strike § 7220(c)(5).

**Behavioral Advertising – Fallback:** For reasons stated above, the scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If that is not excluded, then any notice requirements should be tailored to the reduced risk and different circumstances of advertising. For instance, as drafted, the rules would impose more detailed disclosures than required for higher-risk cross-context behavioral ads under § 7013.

**AI/ADMT Training – Fallback:** For reasons stated above, the scope of covered ADMT under § 7200 should not include the use of ADMT for training. If that is not excluded, then at minimum such processing should not trigger pre-use notice. It will contribute to notice fatigue without reducing risk as consumers will struggle to understand this notice. Instead, the draft rules already require AI/ADMT deployers (i.e., “users”) to conduct risk assessments and companies may invest in accuracy/testing safeguards that better demonstrate trustworthiness.

**§ 7221(b) – Exceptions General:** Expand the set of exceptions under § 7221(b) to include conducting internal research, fixing technical errors, effectuating product recalls, and performing internal operations consistent with the consumer’s expectations (like other privacy laws).

**§ 7221(b)(1) - Security and Fraud Prevention:** The fraud and security exception should be unencumbered by whether ADMT is “necessary” for the purposes of security, fraud prevention, or safety. Businesses should be free to choose the most effective and reasonable method of security, fraud prevention, or safety without regard for whether a particular method is “necessary.”

**Suggested Revision:** Amend § 7221(b)(1) as follows: (b)(1) The business’s uses of that automated decision-making technology ~~is necessary solely~~ to achieve, ~~and is used solely for~~, the security, fraud prevention, or safety purposes listed below...

**§ 7221(i) – Single ADMT Opt Out:** The draft rules would require a business to offer a single option to opt-out of all covered ADMT, although businesses may present consumers with a choice to allow specific uses. Consumers will struggle to comprehend the impact of a general opt out in the abstract or to analyze a vast range of potential use cases (e.g., behavioral advertising vs screening for health risks). This will likely result in consumers making opt-out elections to avoid certain high-risk use cases, and then losing out on significant beneficial opportunities that would likely approve when presented with the specific use case. Instead, business should be required to surface an opt out that is targeted to the specific use case so the consumer can decide in real time and in context rather than in the abstract. Also, mandating a single opt out presumes that the use of ADMT is generally harmful to consumers or lacks benefits, and is antithetical to California’s support for innovation, efficiency, and tools that reduce human error and bias.

**Suggested Revision:** Amend § 7221(i) as follows: In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decision-making technology ~~as long as the business also offers a single option to opt-out of all of the business’s use of automated decision-making technology set forth in subsection (a).~~

**§ 7221(b)(4) & (5) – Employee Exceptions:** The draft rules provide some exceptions to the ADMT Opt-Out for “*allocation/assignment of work and compensation decisions*” and “*work or educational profiling*.” However, these exceptions require companies to conduct “*an evaluation*” and implement expensive and burdensome “*accuracy and nondiscrimination safeguards*.” Employers generally are allowed flexibility to ensure employees are working and productive. This would stifle employers’ ability to ensure employees are properly working or the company is properly staffed. It can also affect customer service where companies look at these tools to identify when to route calls to employees to ensure 1) they are working and 2) ensure they are not overwhelmed with the volume of calls. Moreover, it is not clear what “*work or educational profiling*” means. The proposed rules refer to “*extensive profiling*,” not “*work or educational profiling*.”

**Behavioral Advertising – Fallback:** The scope of covered ADMT, under § 7200, should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply an opt-out right to all behavioral ads as it conflicts with the statutory opt-out framework that is limited to CCBA. As a final fallback, the rules should be clear that any opt out that applies to behavioral ads is limited to targeting ads based on inference preferences from consumers based on their personal data. The draft rules potentially sweep in contextual ads since the definition of behavioral ads is not limited to activity “*over time*.”

Additionally, the proviso in the “*behavioral advertising*” definition makes it seem like measurement (e.g., attribution) could be covered as well. It unhelpfully copies some CPRA language, but without the additional context from the CPRA that clarifies that measurement is not in scope.

**AI/ADMT Training – Fallback:** § 7221(b) provides a limited set of exceptions to the opt-out right, but does not extend them to AI/ADMT training. For reasons stated above, the scope of covered ADMT under § 7200 should exclude ADMT training uses. If that is not excluded, then the exceptions should apply to this use, in particular, the fraud and security exception under (b)(1) and the evaluation exception under (b)(3), (4), and (5). Businesses should be encouraged to evaluate whether the ADMT is discriminatory or working as intended and the best way to do that is to train on representative samples of data.

If AI/ADMT training is not excluded entirely from Article 11, then another fallback should exclude or limit the right to opt out. Generally, model training (especially for the largest models trained on internet-scale data) personal data included in the training corpus is incidental. Requiring implementation of an opt out process runs counter to data minimization best practices, as it may require individual identification.



**Suggested Revisions:** The preferred option would be to strike § 7150(b)(4) – AI/ADMT Training altogether. If not, amend § 7221(b) by striking (b)(6).

**§ 7222 Requests to Access ADMT:** General concerns - CPRA § 1798.185 instructs the CPPA to issue regulations on access rights with respect to a business’s use of ADMT, and requiring responses to include “*meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.*” It does not call for separate notice. Based on these statutory requirements, the CPPA should consider a single set of rules about how businesses need to provide meaningful information about their use of ADMT.

Businesses should have the option to provide this information in a notice (rather than a response to a specific request). The rules should not require businesses to provide consumer-specific responses, as this (i) is not required under the statute, (ii) is not practical or feasible in many cases, and (iii) would be difficult to comply without disclosing confidential information or allowing consumers to game the process, which would have dangerous implications where the ADMT is used to make a significant decision. Consumers already have separate access rights under the CPRA, and so can obtain any personal information processed by the company, including ADMT inputs and outputs containing their personal information.

**§ 7222 (a) – When Access Right Applies:** The draft rules create a right to access ADMT when a business uses ADMT for significant decisions (§ 7200(a)(1)) or extensive profiling (§ 7200(a)(2)). It does not apply to AI/ADMT training. This right should be limited to where ADMT is used to make a significant decision. The access right serves to allow consumers to understand whether they want to exercise their opt-out right, and to allow them to correct any inaccurate input concerning their personal information. This may assist consumers when presented with an ADMT offering that will assist in making a significant decision, but does not apply to “extensive profiling” such as profiling for behavioral advertising. For those uses, the consumer can decide whether to opt out regardless of how technology works. Businesses should not be required to publicly disclose confidential information about their technological processes absent any direct consumer benefit.

**Suggested Revisions:** Amend § 7222(a) as follows: *Consumers have a right to access ADMT when a business uses automated decision-making technology as set forth in § 7200, subsections (a)(1)-(2) ....* Strike § 7222(b)(3)(B).

**§ 7222(b) – Response to Access Request:** Per above, the responses should not be tailored to specific consumers. At minimum:

(b)(2) should be modified so that the business must provide only the range of potential outputs and not the specific output as it relates to the consumer. If the output itself contains personal information related to the consumer, then it would be subject to the separate, broader access right under the CPRA.

(b)(4) should be clarified to not require the business to explain how the ADMT operated with respect to a specific consumer.

**§ 7222(k) – Adverse Significant Decisions:** In the employment context, the rules give companies too little time to effectively provide detailed, and in parts, data specific to each individual decision—a bar too burdensome given the broad applicability. In the case of an “*adverse significant decision*” (suspension, demotion, termination, or reduction in compensation), the business must provide notice of the right to access within 15 days of the adverse decision, and with detailed information within 45 days. Upon request, the business must provide “*a plain language explanations*” — requiring interpretation — of the purpose of the ADMT, and more concerning, (a) the specific outputs the ADMT produced after processing the individual’s data; (b) the way in which the business used (and plans to use) the ADMT output and human assessment in making decisions regarding that individual; (c) the “*extensive profiling*”,



if any, performed by the business using an ADMT; and (d) the precise “logic”, “key parameters”, and “range of possible outputs or aggregate output statistics” of the ADMT, so the individual can understand the workings of the tool and how the specific decision came to be. Little of this information will be helpful to the individual and will require extensive interpretation on behalf of a company to produce this information in “plain language” to an individual—often in each specific “adverse significant decision.”

**Behavioral Advertising – Fallback:** The scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply the access right to this type of ADMT processing.

**Suggested Revisions:** See previous comments to strike “behavioral advertising.”

We also have concerns with the way § 7123(f) is currently drafted. As written, it is effectively useless as it says another audit can only be used if another audit has all the same requirements as the CCPA audit. No other audit regime looks like the CCPA audit, so businesses will always be required to conduct a separate audit for CCPA. Most businesses already conduct annual audits for ISO certification. We suggest the regulations include common security audit frameworks that will be accepted as compliant with these regulations without requiring businesses to make the determination whether they meet all the requirements the agency requires.

Related to this, the specific controls in § 7123(b) run the risk of quickly becoming outdated. Most existing cybersecurity audit standards call for the assessment of how organizations achieve outcomes (e.g., NIST recommends as a security control, “The confidentiality, integrity, and availability of data-at-rest are protected.”). The proposed regulations instead require specific security controls to achieve certain outcomes (e.g., requiring assessment of “Encryption of personal information, at rest”). For example, (b)(2)(A) focuses on MFA and passwords when most companies are increasingly moving to passkeys.

Finally, we suggest a limitation on the submission of full audits, allowance for redaction of sensitive security information and other information, and a requirement that the CPPA keep the reports secure and confidential.


#### **General Comments and Concerns on AI/Privacy Regulations Impact on Emergencies**

Weave in how these regulations will negatively impact the supply chain or small business recovery for those who are trying to rebuild after emergencies like the recent wildfires in Los Angeles County.

Again, we appreciate the opportunity to provide comments on the proposed regulations, but urge a thoughtful reconsideration of these regulations to ensure they protect consumers without unduly burdening businesses or stifling innovation. California's position as a global leader in AI research and development is at stake, and a balanced, well-deliberated approach is crucial for maintaining our competitive edge while safeguarding consumer interests.

If you have any questions or need additional information on our comments included in this letter, please do not hesitate to contact me directly.

Sincerely,



Sarah Pollo Moo  
Policy Advocate

**Grenda, Rianna@CPPA**

---

**From:** Kris Quigley <kquigley@cdiaonline.org>  
**Sent:** Tuesday, June 10, 2025 12:52 PM  
**To:** Regulations@CPPA  
**Subject:** "Public Comment on Accessible Deletion Mechanism"  
**Attachments:** Final DROP COMMENTS June 10.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

**Kris Quigley**  
*Director, Government Relations*  
[kquigley@cdiaonline.org](mailto:kquigley@cdiaonline.org)  
c: [REDACTED]





Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905  
P 202 371 0910 [CDIAONLINE.ORG](http://CDIAONLINE.ORG)

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

RE: Public Comment on Accessible Deletion Mechanism

The Consumer Data Industry Association (CDIA) appreciates the opportunity to comment on the rulemaking for the Delete Request Opt-Out Platform (DROP) through the California Privacy Protection Agency (CPPA).

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk.

Through data and analytics, CDIA members empower economic opportunities all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumer access to financial and other products suited to their unique requirements. They help people meet their credit needs; they ease the mortgage and employment processes; they help prevent fraud; they help people acquire homes, jobs, and cars with quiet efficiency. CDIA members locate crime victims and fugitives; they reunite consumers with lost financial assets; they keep workplaces and apartment buildings safe. CDIA member products are used in more than nine billion transactions each year.

#### **Data Matching Thresholds Increase Risk of Incorrect Deletions**

Data brokers are required to process deletion requests through the DROP if more than 50% of the unique identifiers provided match a single consumer record. Under this rule, if a majority of the identifiers in a consumer deletion list correspond to one consumer profile maintained by the broker, all personal information associated with that profile must be deleted. This approach is overbroad and risks deleting data for individuals who did not submit a request. Moreover, it conflicts with existing CPPA regulations, which mandate verifying a deletion request to a “reasonable” or “reasonably high degree of certainty,” depending on the sensitivity of the data—standards that may require at least three matching data points before a business must act on the request.



Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905  
P 202 371 0910 [CDIAONLINE.ORG](http://CDIAONLINE.ORG)

Further, data brokers may not organize data sets by identifiers such as phone numbers, emails, etc. but instead may organize data at the consumer level and then associate the identifiers to that consumer with deletion requests being processed at the consumer level as opposed to the identifier level. As such, the verification, deletion, and reporting should not be about the various identifier lists but instead about the unique individual. This is in line with the requirements of the CCPA which provide that data may be deleted following a “verifiable consumer request” which identifies the consumer, not a verification or reporting of unique data points which could potentially belong to multiple consumers, some of whom have not made a deletion request.

### **Exemptions to Deletion**

The regulations contemplate that if there is an exemption to deletion that the data broker should inform the agency that the data was not deleted due to the exemption. However, it may be the case that the same data point is in different databases, some that include data that is exempt and others that include data that is not exempt and would have been deleted. The regulations and reporting requirements back to the agency should take into account how to report to the agency that a data point has been deleted in some databases but not in others where there is an applicable exemption with the same data broker.

### **Lack of Agent Verification Standards Leave System Vulnerable to Abuse**

The proposed regulations lack essential safeguards for verifying authorized agents. Specifically, the proposed framework provides virtually no mechanisms to confirm that agents are legitimately acting on behalf of consumers. This stands in direct contrast to existing CCPA regulations, which require agents to present proof of signed authorization from the consumer and permit businesses to either (1) verify the consumer’s identity directly or (2) obtain direct confirmation from the consumer that they authorized the agent’s request. By omitting these requirements, the proposed DROP regulations create a significant loophole, allowing agents to bypass established verification procedures simply by submitting requests through the DROP instead of directly to a business.

### **Encryption Enables More Reliable Consumer Identification Than Hashing**

Encryption would be the preferred method to provide information to data brokers for processing through the DROP as opposed to hashing. If a data broker is only provided a hash, then it may be more difficult for the data broker to identify and match the consumer to the records in their databases and products. If a hash is utilized, then the hash will have to match exactly for the request to be processed. There will be no ability to match identifiers that may be similar but not exact. Processing hashed transactions also makes it more difficult to investigate any issues that may be present in the processing, such as determining whether there is a mismatch due to similar names.

### **Consumer Residency and Identity Verification Requirements Lack Sufficient Guidance**

Virtually no safeguards are included to verify that a deletion request is being made by the specific consumer to whom the data pertains. While the regulations offer limited guidance on verifying an individual's residency, they do not require confirmation that the individual is in fact a California resident. Moreover, the regulations permit, but do not require, verification of specific data elements. This stands in contrast to existing CCPA regulations, which require businesses to implement reasonable methods to verify that the individual

### **Strict Data Standardization Rules Could Compromise Accuracy**

All registered data brokers would be required to reformat their data to conform to a "standardized" system prescribed by the CPPA. For example, the rules would mandate the removal of capital letters, extraneous spaces, and special characters from databases. Imposing uniform standardization requirements on all data brokers could introduce data security risks by reducing variability in data structures and creating uniform attack surfaces. Additionally, mandating specific data formatting practices may raise First Amendment concerns, particularly where the formatting affects how information is stored, categorized, or expressed.

### **Registration Requirements Create Operational Inefficiencies and Consumer Confusion**

Each business entity meeting the definition of a data broker, including subsidiaries within a single corporate structure, would be required to create and manage a distinct DROP account at the entity level. For some companies, this could necessitate registering and maintaining multiple DROP accounts, despite operating a centralized privacy request system that provides consumers with a single, unified interface through which privacy requests are fulfilled across all affiliated entities. We are concerned that the current proposal may have unintended consequences, including:

- **Consumer confusion**, as multiple, seemingly unrelated DROP entry points may appear for what is effectively a single company.
- **Fragmentation of request processing**, complicating the efficient and timely fulfillment of consumer rights.
- **Duplicative administrative and technical burdens**, which do not enhance consumer privacy but increase operational complexity.



Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905  
P 202 371 0910 [CDIAONLINE.ORG](http://CDIAONLINE.ORG)

To mitigate these concerns, we respectfully urge the CPPA to permit a single, parent-level DROP registration for affiliated business groups that operate under a unified privacy program. This parent entity would assume accountability for routing and fulfilling all consumer requests across its registered subsidiaries in compliance with applicable legal obligations.

We acknowledge and support the requirement to register, and pay the applicable fee, for each legal entity that qualifies as a data broker. Our request pertains solely to the management and presentation of DROP accounts in a manner that is both consumer-friendly and operationally efficient.

### **Identity Assurance Standards Must Be Reflected in DROP Regulations**

With respect to both consumers and authorized agents, our members are subject to federal obligations that require adherence to identity assurance standards before processing deletion requests. In order to interact with and act upon data from the DROP system, members require an attestation from the CPPA that the DROP meets minimum security standards contained in NIST 800-63-3 for Identity Assurance Level (IAL) 2 for any entity submitting requests. The regulations need to reflect these requirements and contemplate a process for attestation.

### **Insufficient Timeline for Effective Implementation**

The proposed compliance timeline does not provide sufficient time for businesses to evaluate technical impacts, design or reconfigure internal workflows, train relevant personnel, and thoroughly test and validate system integrations with the DROP platform. To ensure effective and accurate compliance, we respectfully recommend that the CPPA adopt an implementation window of *at least 18 months* from the date the DROP platform is fully operational and accompanied by complete, final technical documentation. A rushed implementation timeline could increase the risk of system failures, processing errors, or consumer confusion and undermine the goals of the regulations. A phased or adequately delayed rollout will better serve both consumers and regulated businesses by promoting smoother adoption and more reliable long-term outcomes.

Thank you for your time and consideration. Should you have questions please contact me at [kquigley@cdiaonline.org](mailto:kquigley@cdiaonline.org).

Sincerely,



Kris Quigley  
Director, Government Relations



**From:** Justin Brookman <justin.brookman@consumer.org>  
**Sent:** Tuesday, June 10, 2025 1:43 PM  
**To:** Regulations@CPPA  
**Cc:** Matt Schwartz; Sara Geoghegan  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** FINAL - CR-EPIC Comments - Notice of Proposed Rulemaking on Accessible Delete Mechanism – Delete Request and Opt-out Platform (“DROP”) System Requirement.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

I am submitting the attached comments from Consumer Reports and the Electronic Privacy Information Center.

\*\*\*

This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

\*\*\*

Comments of Consumer Reports and the Electronic Privacy Information Center  
In Response to the  
California Privacy Protection Agency's  
Notice of Proposed Rulemaking on  
Accessible Delete Mechanism – Delete Request and Opt-out Platform ("DROP") System  
Requirements

By

Matt Schwartz, Policy Analyst, Consumer Reports  
Justin Brookman, Director of Technology Policy, Consumer Reports  
Sara Geoghegan, Senior Counsel, Electronic Privacy Information Center

June 10, 2025



Consumer Reports<sup>1</sup> and the Electronic Privacy Information Center appreciate the opportunity to provide feedback on the California Privacy Protection Agency's (CPPA) Notice of Proposed Rulemaking on Accessible Delete Mechanism – Delete Request and Opt-out Platform (“DROP”) System Requirements. We thank the CPPA for moving forward with this rulemaking package and for its other initiatives to protect consumer privacy. We are supportive of the vast majority of proposals in this rulemaking package and believe that they will advance the Agency's efforts to create a robust and user-friendly mechanism for consumers to delete their personal information held by data brokers, as required under the Delete Act.

We offer suggestions related to a few of the Agency's proposed regulations below.

## **I. Section 7601 (Definitions)**

### *“Direct Relationship”*

CPPA proposes various amendments to the definition of “direct relationship,” which governs when a business that is selling the personal information of consumers to third-parties is considered a data broker for purposes of the Delete Act.<sup>2</sup> For instance, the Agency is considering removing the time limitations in the current rules, so that a business would have a direct relationship with a consumer if the consumer had *ever* accessed, purchased, used, requested, or obtained information about the business' products or services. The previous definition stated that a direct relationship did not exist if the consumer had not interacted with the business in the previous three years.

We urge the CPPA to restore the previous language. In our view, the term “direct relationship” implies a continuous interaction between the consumer and business. If a business is selling the personal information of a consumer it collected five years ago, with no other meaningful interaction since then, the business is acting as a data broker. Consumers have their information collected and shared by an astoundingly large number of businesses. Last year, Consumer Reports found that, on average, consumers' personal information was shared to

---

<sup>1</sup> Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

<sup>2</sup> Proposed Rules, Section 7601(d),  
[https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_text.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_text.pdf)

Facebook alone by 2,230 different companies.<sup>3</sup> While consumers certainly interact with many businesses on a continual basis, many others gather and share data derived from ephemeral interactions, potentially even from a single visit to a website. This is the exact type of relationship where a consumer ought to be able to leverage the DROP to exercise a universal deletion request. Consumers should not be expected to remember every website or business with which they once interacted if they want to delete their personal information, especially after several years have passed. Even if they did, the sheer number of individual deletion requests would be impractical.<sup>4</sup> Three years strikes us as a fair balance; companies can leverage consumer information for a reasonable period of time after an interaction without becoming a data broker, but cannot do so indefinitely.

On the other hand we appreciate that the Agency is proposing to clarify that a business does not have a direct relationship with a consumer “as to the personal information it sells about the consumer it collected outside of a ‘first party interaction’ with the consumer.”<sup>5</sup> This resolves an issue we flagged in previous comments,<sup>6</sup> whereby an entity that sometimes acts as a data broker and other times acts as a consumer-facing business would’ve been required to delete *all* personal information, including data collected via a first-party relationship, about a consumer in response to a DROP request. This could have led to unintended consequences, such as a consumer accidentally deleting their account or other personal information shared directly with a social media company when they expected to simply delete information collected through that social media company’s tracking technologies embedded on third-party websites (e.g. the Facebook pixel). The proposed change also ensures that data brokers aren’t incentivized to create superficial “direct relationships” with consumers (such as through non-commonly branded apps or websites)<sup>7</sup> to evade compliance with the law.

## **II. Section 7610 (Delete Request and Opt-out Platform Account Creation)**

### *Selection of Deletion Lists*

Proposed Section 7610(a)(3)(A) states that data brokers must select all consumer deletion lists (lists containing consumer identifiers submitted through the DROP) that will match personal

---

<sup>3</sup> Don Marti et al., Consumer Reports, “Who Shares Your Information with Facebook,” (January 2024), [https://innovation.consumerreports.org/wp-content/uploads/2024/01/CR\\_Who-Shares-Your-Information-With-Facebook.pdf](https://innovation.consumerreports.org/wp-content/uploads/2024/01/CR_Who-Shares-Your-Information-With-Facebook.pdf)

<sup>4</sup> See, e.g., Maureen Mahoney, Consumer Reports, CCPA: Are Consumers’ Digital Rights Protected, Medium, (finding that consumers had significant difficulty opting out from just a handful of data brokers), (October 1, 2020), [https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR\\_CCPA-Are-Consumers-Digital-Rights-Protected\\_092020\\_vf2.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf)

<sup>5</sup> Proposed Rules, Section 7601(d)

<sup>6</sup> Comments of Consumer Reports In Response to the California Privacy Protection Agency’s Invitation for Comments On Proposed Data Broker Regulations, (August 20, 2024), <https://advocacy.consumerreports.org/wp-content/uploads/2024/08/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agency’s-Invitation-for-Comments-On-Proposed-Data-Broker-Regulations-FINAL.pdf>

<sup>7</sup> See, e.g., X-Mode Social, Inc., Complaint, In the Matter of X-Mode Social, Inc., FTC File No. 202-3038 (2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/X-Mode-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf)

information about consumers in their records. On the other hand, proposed Section 7610(a)(3)(B) provides that a data broker may select fewer lists if “consumer identifiers used across multiple lists will result in matches to a completely duplicative list of consumers within the data broker’s records.” This however could allow data brokers to select lists that they know will result in a fewer number of successful deletion requests. For instance, even if a data broker collects email addresses and phone numbers for every consumer in its database, it might know that the quality of phone numbers it collects is less reliable and therefore less likely to result in a match than the email addresses it collects. In order to increase the chances of successful deletion requests, CCPA should simply delete proposed Section 7610(a)(3)(B) and require data brokers to select all consumer deletion lists that will match personal information about consumers in their records.

### **III. Section 7613 (Processing Deletion Requests)**

#### *Limiting Data Leakage From Sharing Hashed Identifiers*

Under Section 7613(a)(1)(B), a data broker is given access to a hashed list of identifiers, against which they compare their own list of identifiers hashed using the same algorithm. For each match, they must then delete the matched identifier along with any other linked personal information.

However, giving data brokers access to large numbers of hashed identifiers presents substantial privacy risks. Hashing data does not render it anonymous, as the recipient of such data can use the hashing algorithm to pregenerate tables of likely identifiers; this tactic is especially effective for identifiers like phone numbers that have a precisely defined universe of possible values.<sup>8</sup> As a result, data brokers may get access not just to new identifiers but also to potential linkages among those identifiers. While the proposed rule forbids recipients from using these identifiers for any purpose other than processing current or future deletion requests,<sup>9</sup> bad actors may ignore this policy prohibition and use a list of hashed identifiers to augment their databases.<sup>10</sup>

The Agency should explore technical mechanisms to redress the problem of data leakage from sharing hashed identifiers. One potential solution is private set intersection, a cryptographic protocol that allows two parties to compare data sets, but only generating a result that shows shared records — records not appearing in both databases are not observable to a party that

---

<sup>8</sup> Staff in the Office of Technology, Federal Trade Commission, No, hashing still doesn't make your data anonymous, (July 24, 2024), [https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous#ftn\\_3](https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous#ftn_3).

<sup>9</sup> Proposed Rules, Section 7616(a).

<sup>10</sup> Using data received as part of a privacy rights request to augment marketing databases is not unprecedented. A Consumer Reports investigation into the effectiveness of CCPA opt-out laws demonstrated that in at least one case, a consumer who submitted personal information to effectuate an opt-out request had their data added to an email marketing list. Maureen Mahoney, Consumer Reports, California Consumer Privacy Act: Are Consumers’ Digital Rights Protected, (October 2020), [https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR\\_CCPA-Are-Consumers-Digital-Rights-Protected\\_092020\\_vf2.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf).

did not possess the record before. Another potential approach would be to match records in a separate trusted execution environment, only revealing to the data broker the identity of the records it should suppress. These approaches could have costs — data brokers would not be able to retain identifiers to be suppressed in the future — but those costs could be outweighed by the privacy benefits from reduced data leakage.

### *Threshold for Deleting Data*

In Section 7613(a)(2)(A), the Agency proposes a standard whereby a data broker must delete personal information associated with multi-part identifiers (e.g. a combination of name, date of birth, and zipcode) if more than 50 percent of the identifiers match (e.g. name and zipcode). In general, we're supportive of this proposal, as it will result in more successful deletion requests. However, in Section 7613(a)(2)(B), the Agency states that if a data broker associates *multiple* consumers with a matched identifier from the deletion list, they must process the request as an opt out for each matched consumer. It is likely that there will be many consumers that share certain parts of a multi-part identifier (for instance, there are likely to be many people with the same birthday in a given zipcode), and it is unclear what a data broker is required to do when there are multiple combinations of matching identifiers (e.g. many people with the same birthdate and zipcode, a few people with the same name and zipcode, and only one person with all three matching identifiers). CCPA should clarify that in this example, the data broker is required to delete the data of the person with all three matching identifiers. Otherwise, data brokers may unfairly thwart the deletion request of the best matching consumer in favor of opting more consumers out, but retaining the underlying data.

### *Deleting Matching Identifiers*

We appreciate that CCPA's proposed definition of "personal information associated with a matched identifier," states that the term includes inferences made personal information subject to applicable exemptions.<sup>11</sup>

Section 7613(b) states that data brokers must delete all personal information associated with a matched identifier, including inferences "based in whole or part on personal information collected from third parties or from consumers in a non-'first party' capacity", but that data brokers are not required to delete personal information exempted under the Delete Act or the cross-referenced exemptions in the CCPA. The Agency's clarification that inferences derived in whole or in part from exempted information are not exempt themselves will prevent data brokers from evading coverage. It also comports with CCPA's definition of "infer or inference," which implies that inferences are entirely new pieces of information derived from existing sources of information.<sup>12</sup>

As the Agency is aware, data brokers often aggregate records from many independent sources of information, and dozens of data brokers in the California registry, including some of the

---

<sup>11</sup> Proposed Rules, Section 7601(i)

<sup>12</sup> CCPA, Section 1798.140(r), [https://ccpa.ca.gov/regulations/pdf/ccpa\\_statute.pdf](https://ccpa.ca.gov/regulations/pdf/ccpa_statute.pdf)



nation's largest, currently claim one or more of the available exemptions.<sup>13</sup> This makes it possible for them to combine exempted and nonexempted information to make novel inferences about consumers. For example, a data broker may place a consumer into a marketing category labeled "wealthy and not healthy," on the basis of inferences derived from a consumer's exempted financial records and a consumer's non-exempted grocery store shopping history.<sup>14</sup> That inference certainly should *not* be considered exempt from a consumer's deletion request under the Delete Act. In many cases, a major risk that data brokers create for consumers is in the inferences they make about consumers, which are often inaccurate<sup>15</sup> but can be used to make significant decisions about their lives.<sup>16</sup> Consumers should be able to delete these inferences, regardless of the inputs data brokers used to generate them.

#### **IV. Section 7614 (Reporting Status of Deletion Requests)**

##### *Exempted Data*

Under proposed Section 7614(b)(2), data brokers are required during each access session to report to the DROP the status of deletion requests with one of the following response codes: record deleted, record opted out of sale, record exempted, and record not found. For cases of exempted records, we suggest that CPPA require data brokers to provide information about which of the available exemptions data brokers are claiming in a given instance. This will incentivize additional accountability for data brokers, help consumers better understand why their deletion request was not honored, and allow the Agency to provide more oversight over data brokers' compliance with the law.

#### **V. Section 7616 (Additional Data Broker Requirements)**

##### *Prohibition on Data Broker Verification*

We support Section 7616's explicit prohibition on data brokers from contacting consumers to verify deletion requests submitted through the DROP. Consumers benefit most from universal

---

<sup>13</sup> California Privacy Protection Agency, 2025 Data Broker Registry, [https://cppa.ca.gov/data\\_broker\\_registry/](https://cppa.ca.gov/data_broker_registry/)

<sup>14</sup> See, e.g., Stephanie T. Nguyen, Federal Trade Commission, FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket, (March 4, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket>

<sup>15</sup> Nico Neumann, Catherine E. Tucker, and Timothy Whitfield, "Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies," Marketing Science, Vol. 38, No. 6, (October 2, 2019), <https://pubsonline.informs.org/doi/10.1287/mksc.2019.1188>

<sup>16</sup> See, e.g., Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," at 47-48, (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>; Joanne Kim, Duke Sanford Cyber Policy Program, Data Brokers & the Sale of Americans' Mental Health Data, (February 2023), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf>

controls when they are simple and easy to use. As we wrote in previous comments to the Agency,<sup>17</sup> a consumer's initial DROP request should mark the beginning and end of their involvement, unless they wish to return to check on the status of their request or append their request with more information. Allowing data brokers to directly contact consumers will likely only undermine the efficiency of the DROP and circumvent consumer expectations.

## **VI. Section 7620 (Consumer Deletion Requests)**

### *Verification of Residency*

Proposed Section 7620(a) states that consumers "may" be required to have their California residency verified by the Agency. In order to ease the burden on consumers making DROP requests, we urge the Agency to choose the least invasive method to determine California residency. In our view, estimating residency based on IP address should be generally sufficient for determining residency and legitimacy, unless the Agency has a good faith basis to determine that a particular device is not associated with a California resident or is otherwise illegitimate. Companies generally comply with state and national privacy laws in a similar manner.<sup>18</sup> More burdensome forms of residency verification may dissuade privacy-conscious users, would introduce more data security risk for the Agency, and could decrease overall takeup.

## **VII. Section 7621 (Authorized Agents)**

While we are happy to see that authorized agents have a role in DROP, the proposed regulations do not provide clarity on how authorized agents would submit requests on behalf of users. As written in Section 7621(b), it seems that authorized agents would have to log into a user's account and then submit requests for them from within the user's account.

Such a process is not feasible for authorized agents as they would have to either receive the user's account credentials (which would not alleviate the burden of creating the account for the user and introduce a security risk) or have access to the user's email address to create an account on their behalf (which is much more access than should be required to be an authorized agent).

We urge the CPPA to think through how authorized agents may submit requests on behalf of users in a more frictionless way. One way, for example, would be for the portal to support "authorized agent" accounts from which agents could submit requests on behalf of many users at once.

\*\*\*\*\*

---

<sup>17</sup> Comments of Consumer Reports In Response to the California Privacy Protection Agency's Invitation for Comments On Proposed Data Broker Regulations, (August 20, 2024), <https://advocacy.consumerreports.org/wp-content/uploads/2024/08/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agency's-Invitation-for-Comments-On-Proposed-Data-Broker-Regulations.pdf>

<sup>18</sup> See, e.g., OneTrust, Configuring Geolocation Rules, (April 2, 2025), [https://my.onetrust.com/s/article/UUID-2229ff55-895a-11da-1b5f-79e1785b6e02?language=en\\_US](https://my.onetrust.com/s/article/UUID-2229ff55-895a-11da-1b5f-79e1785b6e02?language=en_US)

We thank the California Privacy Protection Agency for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz ([matt.schwartz@consumer.org](mailto:matt.schwartz@consumer.org)), Justin Brookman ([justin.brookman@consumer.org](mailto:justin.brookman@consumer.org)), or Sara Geoghegan ([geoghegan@epic.org](mailto:geoghegan@epic.org)) for more information.

**Grenda, Rianna@CPPA**

---

**From:** Richard Varn <cspra@cspra.org>  
**Sent:** Monday, June 9, 2025 9:47 AM  
**To:** Regulations@CPPA  
**Cc:** Bailey-Crimmins, Liana@CIO; Cheung, Edmond@CIO  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** CA Drop Rules Comments Final 6-9-2025.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Date: June 9, 2025  
To: California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811  
Re: **Public Comment on Accessible Deletion Mechanism and the Proposed Rules for Implementing the Delete Request and Opt-Out Platform (“DROP”)**

Please find our comments in the attached PDF file. If you need them in any other format, please advise.

Thank you.

Regards,

***Richard J. Varn***  
**Executive Director**  
**Coalition for Sensible Public Records Access**  
San Antonio, TX  
Email: [cspra@cspra.org](mailto:cspra@cspra.org)  
Cell : [REDACTED]

*A non-profit organization dedicated to promoting the principle of open public records access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, commercial, and societal benefit.*

CC:  
Liana Bailey-Crimmins  
State CIO and Director  
California Department of Technology

Edmond Cheung  
Deputy Director of Legislation  
California Department of Technology



---

## COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

Date: June 9, 2025  
To: California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811  
Re: **Public Comment on Accessible Deletion Mechanism and the Proposed Rules for Implementing the Delete Request and Opt-Out Platform (“DROP”)**

### Who We Are

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit organization dedicated to promoting the principle of open public record access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, governmental, commercial, and societal benefit. Members of CSPRA are just a few of the many entities that comprise a vital link in the flow of information for these purposes and provide services that are widely used by constituents in your state. Collectively, CSPRA members alone employ over 75,000 persons across the U.S. and all CSPRA members do business in California.

### Summary of Comments

Our comments are below and incorporate by reference and inclusion the memo appended to this letter and which we requested from the law firm of **Hudson Cook, LLP**. Our comments in the main body of this letter will only summarize the law firm’s findings and suggestions in the memo but we are submitting both documents as our comments. We also offer some additional observations and suggestions not contained in the legal memo. Our concerns are as follows:

- The regulations contain inconsistent and insufficient identity matching requirements
- There are no verification safeguards for authorized agents as to their identity, the validity of a DROP request, and the confirmation that it was submitted by the consumer
- The lack of adequate security opens the door for abuses by commercial interests, hackers, and malevolent actors
- There are insufficient informed consent requirements
- The data standardization requirement is extremely intrusive, burdensome, exceeds any statutory authority, and may constitute a taking of property without just compensation prohibited under the 5<sup>th</sup> and 14<sup>th</sup> Amendments to the Constitution
- The proposed fees are excessive and exceed the projected cost and the statutory authority for their imposition
- The rules lack a safe harbor for a limited time to accommodate good faith efforts at adoption as have been provided with other privacy laws and similar regulatory schemes



**The regulations contain inconsistent and insufficient identity matching requirements.**

The legal memo addresses this issue pointing out the insufficiencies with the 50% match requirement, the conflict with other California law, and the implications of the failure adequately and accurately identify the consumer. We further note that the lack of a reliable method to affirmatively identify the subject of a record is compounded by the rule not validating third-party agents nor verifying that the request came from the subject of the record. This trio of failings opens the door to a host of issues including denial of services and opportunities without consent, social engineering and hacktivism by unscrupulous actors, and fraudulent submissions we discuss further below. Furthermore, consumers wrongly deleted have a right to receive the speech that will be cut off because of the deletion and the entities wishing to communicate have a right to speak. Removing the wrong person or in any way deleting someone who has not consented to a deletion violates the speech rights of the both the senders and recipients of protected speech. The Agency needs to require more protections against this happening.

**The proposed regulations are devoid of needed guardrails around verification of authorized agents.**

The legal memo addresses this issue. In summary, the proposed DROP regulations contain virtually no safeguards for verifying agents' ability to act on behalf of consumers. This conflicts with the regulations to implement the CCPA, which require agents to provide proof that the consumer gave the agent signed permission to submit the request and allow the business to require the consumer to either (1) verify their own identity directly with the business; or (2) directly confirm with the business that they provided the authorized agent permission to submit the request. This creates a loophole for agent verification in instances where agents use the DROP rather than going directly to a business to submit a deletion request.

**The lack of needed guardrails around verification of authorized agents and consumers opens the door for abuses by commercial interests, hacktivists, and malevolent actors.**

The risks from this lack of security and regulation of agents are many. Bad actors could submit false requests for a variety of questionable and illegal purposes. A low-security DROP system could be used to remove voters inclined to certain opinions from databases so that they cannot be part of a get out the vote or persuasion effort in an election. It could be used to preserve markets for incumbent players who do not want their existing customers to switch to a competitor. It could be used by hacktivist or foreign governments to just remove persons from databases to hurt the economy. Authorized agents could use high-pressure and deceptive techniques to push high volumes of people into DROP requests without proper and informed consent. Even if the likelihood of such risks is low, the countermeasures are both low-cost and already required by the CCPA, so we see no reason to leave them out of the rules. We do not want to see a law intended to protect consumers to be used to deceive consumers and harm their interests and the California economy in general. The rules should include a process by which consumers can report suspicious or fraudulent activity by authorized agents to the agency.

**As noted in legal memo, the rules do not adequately address informed consent by the consumer.**

We find it sadly ironic that a purported privacy enhancing platform fails to ensure what is so often advocated by privacy advocates: informed consent. In short, a consumer should know what the gain and lose if they drop out. We have no doubt that advocates and third-party agents

will tout what they see as the benefits of dropping out. We are reasonably skeptical that they also will fairly and fully explain the potential costs and negative effects of doing so such that the decision is indeed an informed one. The rules should require them to do so. Consumers should know that there are many benefits to receiving commercial and civic speech that comes from being in databases that accrue to them as individuals, those they care for, and the society and economy. If a consumer opts out and loses out on something they value, they will be rightly upset when they realize what they lost if they are not informed up front. They may even wish to reverse their request. But the rules provide no clear informed consent requirements nor any safe harbor to allow for data broker to keep any data in a non-operational database for any period that will allow the consumer to restore their data to these systems if they change their minds or for the data broker to restore the data of a consumer was mistakenly deleted. Once the data is deleted, it cannot be restored or recreated and the loss to the consumer will be permanent.

**The proposed regulations would require all registered data brokers to reformat data in their systems to a “standardized” system prescribed by the CPPA.**

As further detailed in the legal memo, the proposed rules would require “standardization” of all data brokers’ databases to, for example, remove all capital letters, extraneous, and special characters. This requirement could create data security issues by mandating all databases to use certain standardization methods, may also run afoul of the First Amendment, and may constitute a taking under the 5<sup>th</sup> and 14<sup>th</sup> Amendments. This kind of micromanaging of data formats in private databases for this kind of purpose is, to our knowledge, without precedent in any US jurisdiction. The failure of California and the US to have a reliable system of identity proofing and cryptographically protected assertions and confirmation of identity is a government problem. This problem cannot be shoved onto the private sector to address with a piecemeal and technologically non-sensical solution that does not have a scrap of statutory authority behind it.

**The proposed fees are excessive and exceed the projected cost and the statutory authority.**

As discussed in the memo, the Delete Act’s authorization is limited to a registration fee that must be in line with the reasonable costs of establishing and maintaining a DROP website. The rules would jack up the data broker registration fee up to 1,500% (from \$400 to \$6,600 with a \$550 minimum) and bring in up to \$3.6 million. This would exceed the estimated cost by over a \$1 million. The agency needs to explain and justify how the estimated cost, and the fees are reasonably related.

**The rules lack a safe harbor for a limited time to accommodate good faith efforts at adoption as have been provided with other privacy laws and similar regulatory schemes.**

The initial version of the CCPA provided for a 30-day right to cure that allowed covered entities time to respond and address alleged violations before facing an enforcement action. Given the substantial undertaking required of data brokers to adjust their compliance processes to comply with the DROP and the state’s experience with the CCPA’s right to cure successfully helping businesses transition to a new regulatory regime, the Agency should provide a similar right to cure for DROP compliance, with an appropriate sunset date, in the final regulations. Consideration should also be given to a safe harbor that allows a consumer option for rescission and to correct mistaken deletions.

Thank you for your consideration of our input.

**Richard J. Varn**  
**Executive Director**  
**Coalition for Sensible Public Records Access**

San Antonio, TX

Email: [cspra@cspra.org](mailto:cspra@cspra.org)

Cell : [REDACTED]

*A non-profit organization dedicated to promoting the principle of open public records access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, commercial, and societal benefit.*

CC:

Liana Bailey-Crimmins  
State CIO and Director  
California Department of Technology

Edmond Cheung  
Deputy Director of Legislation  
California Department of Technology

---

**HUDSON**  
**COOK**

**Hudson Cook, LLP • Attorneys at Law • [www.hudco.com](http://www.hudco.com)**

---

1020 19th Street NW | 7th Floor | Washington, DC 20036  
Direct: 202.715.2007 • Main: 202.223.6930  
Email: [ekosa@hudco.com](mailto:ekosa@hudco.com)

## **MEMORANDUM**

**To:** Coalition for Sensible Public Records Access (“CSPRA”)  
**From:** Erik Kosa, *Admitted in the District of Columbia and Virginia*  
Rob Tilley, *Admitted in the District of Columbia and New York*  
**Date:** June 8, 2025  
**Subject:** California Privacy Protection Agency Proposed Regulations on Accessible Delete Mechanism – Delete Request and Opt-out Platform (“DROP”) System Requirements (published April 26, 2025) (“Proposed Regulations”)

---

This memorandum analyzes the proposed rulemaking under Senate Bill 362 (the “Delete Act”)<sup>1</sup> to establish the Delete Request and Opt-Out Platform (“DROP”) as it relates to CSPRA’s members and mission.

---

<sup>1</sup> Cal. Civ. Code §§ 1798.99.90 -89.

In 2023, the California Legislature passed the Delete Act, which requires data brokers to register<sup>2</sup> with the California Privacy Protection Agency (“CPPA” or “Agency”) and honor requests by California residents to delete their personal information held by registered data brokers,<sup>3</sup> subject to certain exemptions.<sup>4</sup> To effectuate the right to delete, the Delete Act requires the CPPA to establish an accessible deletion mechanism that allows consumers to request from registered data brokers the deletion of all non-exempt personal information related to the consumer through a single deletion request made to the Agency.<sup>5</sup> The Agency voted to commence formal rulemaking to establish the DROP on March 7, 2025 and published proposed regulations on April 25, 2025.<sup>6</sup>

The Proposed Regulations are structured such that, once effective, data brokers must pay a first-time access fee,<sup>7</sup> access DROP every 45 days,<sup>8</sup> and process deletion requests accessed through DROP according to certain criteria set forth in the Proposed Regulations.<sup>9</sup>

We outline several issues with the Proposed Regulations below, first assessing the text of the Proposed Regulations for practical and legal considerations and second, outlining potential constitutional concerns with the type of regulation at issue here.

## **I. Analysis of Proposed Regulations.**

### **a. *The DROP contains insufficient identity-matching requirements.***

The Delete Act requires the accessible deletion mechanism to “allow data brokers registered with the California Privacy Protection Agency to determine whether an individual has submitted a verifiable consumer request to delete the personal information related to that consumer[.]”<sup>10</sup> Under the Proposed Regulations, “[i]f more than fifty percent (50%) of the unique identifiers” in a consumer deletion list “match with the same consumer record in the data broker’s records,” the data broker would be required to delete all personal information associated with that consumer.<sup>11</sup> This threshold is too weak, and will lead to over-inclusive deletion of consumer information for people who did not submit requests. The example given in the Proposed Regulations illustrates why.

The Proposed Regulations state that where the available data fields are name, date of birth, and zip code, and there is a match for the name and zip code (accounting for a

---

<sup>2</sup> Cal. Civ. Code § 1798.99.82.

<sup>3</sup> Cal. Civ. Code § 1798.99.86

<sup>4</sup> Cal. Civ. Code § 1798.99.80(c).

<sup>5</sup> Cal. Civ. Code § 1798.99.86(b).

<sup>6</sup> See <https://cppa.ca.gov/regulations/drop.html>

<sup>7</sup> Proposed § 7611(a)(3).

<sup>8</sup> Proposed §§ 7611(a)(2); 7612(a).

<sup>9</sup> Proposed § 7613.

<sup>10</sup> Cal. Civ. Code § 1798.99.86(b)(3).

<sup>11</sup> Proposed § 7613(2).

67% match in identifiers and therefore over the 50% threshold), this is sufficient to trigger the deletion of all information relating to that name and zip code. This low threshold is highly likely to lead to scenarios where records belonging to multiple people sharing common names are improperly deleted and could potentially lead to discriminatory outcomes. For example, the surname Rodriguez is one of most popular family names in the United States, belonging to approximately 298 out of every 100,000 people.<sup>12</sup> The given name Jose belongs to approximately 328 out of every 100,000 people.<sup>13</sup> The California zip code 90001 has a population of approximately 56,000 people, of whom approximately 91%—or 52,642—are Hispanic.<sup>14</sup> While there are no publicly available data assessing name collision rates by zip code, we can infer from the frequency of that name and the demographic composition of zip code 90001 that there may be as many as 210-315 people in that zip code sharing that name. In addition, approximately 18-20% of Americans—totaling nearly 60 million people—live in multigenerational households, with higher rates among Asian, Black, and Hispanic populations.<sup>15</sup> Combined with cultural name-preserving traditions where family names are passed down along generations (with e.g., a Jr. and Sr. in the same home), there is a high probability of collisions where only name and zip code are used to match deletion requests, especially with common names. This comports with studies showing that geographic and demographic clustering generally affect name collision rates.<sup>16</sup>

The low verification threshold in the Proposed Regulations risks turning the deletion portal into a mass opt-out system deleting data for consumers who do not want it deleted. By setting such a low threshold for identity matching, the Agency will in many cases be inferring consent it does not have. This would violate both the text of the Delete Act—which requires a consumer to “request” deletion<sup>17</sup>—and its core principle: that consumers should have control over their personal data. The Agency should incorporate into the Proposed Regulations the standard set forth in the California Consumer Privacy Act regulations relating to the exercise of the consumer’s right to delete, which requires balancing the deletion request against the “risk of harm to the consumer posed by any unauthorized deletion[.]”<sup>18</sup> Under that framework, in conjunction with a deletion request, a consumer’s

---

<sup>12</sup> <https://www.mynamstats.com/Last-Names/R/RO/RODRIGUEZ/index.html>

<sup>13</sup> [https://www.mynamstats.com/First-Names/J/JO/JOSE/index.html#google\\_vignette](https://www.mynamstats.com/First-Names/J/JO/JOSE/index.html#google_vignette)

<sup>14</sup> <https://zipatlas.com/us/ca/zip-code-90001.htm>

<sup>15</sup> D’Vera Cohn, et al., “The demographics of multigenerational households,” Pew Research Center (March 24, 2022), available at: <https://www.pewresearch.org/social-trends/2022/03/24/the-demographics-of-multigenerational-households/>

<sup>16</sup> Arthur Charpentier, Baptiste Coulmont, “We are not alone! (At least, most of us aren’t),” First published: February 2018, Significant, Vol. 15, Issue 1, Pages 23-28, available at: <https://doi.org/10.1111/j.1740-9713.2018.01108.x>

<sup>17</sup> Cal. Civ. Code § 1798.99.86(2).

<sup>18</sup> Cal. Code Regs. tit. 11, § 7060(c)(3)(B).



identity must be verified to a “reasonable”<sup>19</sup> or “reasonably high degree of certainty”<sup>20</sup> depending on the sensitivity of the data, with the latter requiring at least three data points to match the consumer before a business must effectuate the request.<sup>21</sup>

More generally, the Proposed Regulations require very little verification of consumer requests at all. There are virtually no safeguards for ensuring the identity of the consumer making a deletion request. The Proposed Regulations provide limited guidelines where the Agency may verify an individual’s residency,<sup>22</sup> but no mandate to determine that the individual is a resident of the state. Further, the Proposed Regulations allow for verification of specific data elements but do not require it. Proposed § 7620(b) provides that “[c]onsumers may add personal information to their deletion requests, including date of birth, email address, phone number, and pseudonymous identifiers, such as a Mobile Ad Identifier (MAID)” and the Agency “may verify such personal information at any time”.<sup>23</sup>

In some cases, the Proposed Regulations even prohibit verification. Proposed § 7616(c) states: “A data broker shall not contact consumers to verify their deletion requests submitted through the DROP.”<sup>24</sup> The Delete Act does not provide statutory authority to prevent data brokers from verifying that authorized agents are who they say they are, and in fact mandates that the deletion mechanism “shall allow data brokers registered with the California Privacy Protection Agency to determine whether an individual has submitted a verifiable consumer request to delete the personal information related to that consumer[.]”<sup>25</sup> In these instances, the Proposed Regulations exceed the limits of the relevant statutory authority.

The final rule should adopt the approach mandated by the CCPA, which requires a business to establish reasonable methods for verifying that the person making a request to delete is the consumer with whom the business has collected information and to consider whether the personal information provided is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.<sup>26</sup>

#### ***b. There are no verification safeguards for authorized agents.***

---

<sup>19</sup> “A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.” Cal. Code Regs. tit. 11, § 7062(b).

<sup>20</sup> “A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer[.]” Cal. Code Regs. tit. 11, § 7062(c).

<sup>21</sup> Cal. Code Regs. tit. 11, § 7060(c)(3).

<sup>22</sup> See Proposed § 7620(a).

<sup>23</sup> Proposed § 7620(b) (emphasis added).

<sup>24</sup> Proposed § 7616(c).

<sup>25</sup> Cal. Civ. Code § 1798.99.86(b)(3) (emphasis added).

<sup>26</sup> See Cal. Code Regs. tit. 11, § 7060.

The Delete Act defines “authorized agent” to have the same meaning it does under the CCPA regulations,<sup>27</sup> which is “a natural person or a business entity that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.”<sup>28</sup> While the Proposed Regulations contemplate that “[a]n authorized agent may aid in a consumer’s deletion request,”<sup>29</sup> they contain no verification requirements for ensuring the agent is actually “authorized.” Specifically, the Proposed Regulations leave open the following questions:

- (1) What measures will be taken to verify the identity of the agent purporting to act on behalf of a consumer to submit a deletion request?
- (2) What measures will be taken to verify that a person claiming to act as an authorized agent for a consumer has actually been given authority to act as an agent for the consumer?
- (3) What measures will be taken to verify the identity of the consumer making the request, to ensure that the requesting party is the consumer they claim to be?

During the California Legislature’s consideration of SB 1076, which would have added much needed security protections for deletion requests, the Privacy Rights Clearinghouse and the Electronic Frontier Foundation correctly observed that “security and fraud considerations are built into the Delete Act and required in the design of the accessible deletion mechanism.”<sup>30</sup> The first requirement of the accessible deletion mechanism<sup>31</sup> is that it “[i]mplements and maintains reasonable security procedures and practices” that “protect[s] consumers’ personal information from unauthorized use, disclosure, access, destruction, or modification” which “is further reinforced in 1798.99.86(b)(3) and 1798.99.86(c)(3).”<sup>32</sup> They also noted that “the Delete Act permits a data broker to refuse to delete a consumer’s information if it is reasonably necessary to fulfill any purpose outlined in the CCPA’s Section 1798.105(d) (which limits the Right to Delete)” including a scenario where “the information is reasonably necessary and limited to help ensure security and integrity, a defined term under the CCPA.”<sup>33</sup> The Proposed Regulations conflict with the Delete Act’s security requirements.

As it stands, the differing requirements between the Proposed Regulations and the CCPA regulations creates a loophole: If the proposed DROP is implemented as is, an agent who is unable to provide proof they actually have permission to act on behalf of the consumer can perform an end-run around the CCPA’s verification requirements by using the DROP rather than going directly to a business to submit a deletion request under the CCPA. The CPPA should amend the Proposed Regulations to be consistent with the CCPA

---

<sup>27</sup> Cal. Civ. Code § 1798.99.80(b)

<sup>28</sup> Cal. Code Regs. tit. 11, § 7001(d) (emphasis added).

<sup>29</sup> Proposed § 7621(a).

<sup>30</sup> SB 1076, Senate Judiciary Committee Report at 13.

<sup>31</sup> Cal. Civ. Code § 1798.99.86(a)(1),

<sup>32</sup> *Id.* at 13-14.

<sup>33</sup> SB 1076, Senate Judiciary Committee Report at 14.

regulations permitting data brokers to **(1)** ask authorized agents to submit signed proof of their authority to act on behalf of the consumer when submitting requests through DROP and **(2)** confirm with consumers directly that they have authorized the agent to act on their behalf.<sup>34</sup>

**c. The DROP should provide for stronger informed consent.**

The DROP should clearly disclose to consumers the scope of a deletion request so they can make an informed decision before committing to the deletion of their personal information. Informed consent is a bedrock principle of California privacy law. Under the CCPA, for example, “consent” is defined as a “freely given, specific, informed, and unambiguous indication of the consumer's wishes[.]”<sup>35</sup> A consumer cannot make an informed choice to submit a deletion request if they are unaware of the benefits and drawbacks of doing so. For example, the result of submitting a deletion request may include the loss of access to:

- **Public health safety notifications:** Data providers help government agencies and health organizations reach specific demographics during health emergencies or safety recalls. For example, notifying people who have young children about toy recalls, or homeowners about home appliance safety recalls.
- **Civic engagement:** Nonpartisan organizations use demographic data to provide voter registration information, polling location details, and ballot measure explanations to eligible voters who may otherwise be unaware of these opportunities.
- **Educational and scholarship information:** Schools use data to identify and reach students who may be eligible for educational programs or grants they may not otherwise hear about.
- **Community resources:** Local organizations use public data to target food assistance, housing programs, job training, or social services to people who may need them.
- **Financial benefits:** Businesses routinely offer consumers discounts and information on receiving financial benefits. For example, roofing companies convey information to homeowners after natural disasters on how to navigate the insurance process after a roof repair; entities located people eligible for health insurance exchanges after the passage of the Affordable Care Act to help them enroll.

Consumers have the right to receive commercial speech<sup>36</sup>. Advertising is not just selling products; it also involves providing advice and support. Left unamended, the DROP would

---

<sup>34</sup> The CCPA regulations require authorized agents to “provide proof that the consumer gave the agent signed permission to submit the request.” Cal. Code Regs. tit. 11, § 7063(a). In addition, the business may require the consumer to either (1) verify their own identity directly with the business; or (2) directly confirm with the business that they provided the authorized agent permission to submit the request. Cal. Code Regs. tit. 11, § 7063(a).

<sup>35</sup> Cal. Civ. Code § 1798.140(h) (emphasis added).

<sup>36</sup> See *infra*, section II.a

leave consumers unaware of important consequences of deleting their information. The Delete Act itself contemplates that consumers may find some information sharing useful by mandating that DROP “[a]llow a consumer to selectively exclude specific data brokers from a request” to delete.<sup>37</sup> If consumers do not know the kinds of information they are excluding when they view this list, this mandate is meaningless. The final regulations should account for the need to educate consumers about the consequences of submitting a deletion request that informs consumers of both the benefits and the drawbacks of such requests.

**d. *The Agency has not specified how the proposed registration fees are related to the Agency’s reasonable costs.***

The Delete Act authorizes “a registration fee in an amount determined by the California Privacy Protection Agency, not to exceed the reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84 and the reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in Section 1798.99.86.”<sup>38</sup> Under California law, “a fee may be charged by a governmental entity so long as it does not exceed the reasonable costs of providing services necessary to regulate the activity for which the fee is charged” and “may not be imposed for unrelated revenue purposes.”<sup>39</sup>

Excluding payment processing fees, the maximum registration fee under the Proposed Regulations is \$6,600.<sup>40</sup> The minimum is \$550.<sup>41</sup> Given that there are approximately 528 data brokers in California, the fees generated under the Proposed Regulations could total up to \$3.6 million. The Agency’s Economic and Fiscal Impact Assessment<sup>42</sup> for the Proposed Regulations states fiscal costs associated with the regulation were \$2,477,000 in 2025/26 and anticipated to be \$2,340,000 in 2026/27 with future costs to be covered by the data broker registration fees, but does not explain how it reached these cost figures or how the registration fees are reasonably related to them.

**e. *The data standardization requirement is overly burdensome.***

Proposed § 7613(a)(1)(A) would require data brokers to alter their databases so the data follows a format prescribed by the Agency, specifically to: “(i) Use all lowercase letters, including changing names to lowercase; (ii) Remove extraneous or special characters; and (iii) Implement any other standardization that the data broker knows will increase the likelihood of a match between its records and the applicable consumer

---

<sup>37</sup> Cal. Civ. Code § 1798.99.86(a)(3).

<sup>38</sup> Cal. Civ. Code § 1798.99.82(b)(1) (emphasis added).

<sup>39</sup> *Am. Coatings Assn., Inc. v. State Air Res. Bd.*, 62 Cal. App. 5th 1111, 1125 (2021).

<sup>40</sup> Proposed § 7611(a)(3)(A).

<sup>41</sup> Proposed § 7611(a)(3)(L).

<sup>42</sup> [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_std\\_399.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_std_399.pdf)

deletion list.”<sup>43</sup> This section imposes arbitrary requirements that go beyond the Delete Act’s core purpose and does not appear to bear any relationship to the Act’s requirements.

The Delete Act provides statutory authority for implementing the deletion mechanism itself,<sup>44</sup> not to mandate how data brokers are to organize their own proprietary databases. The statutory authority for standing up the deletion mechanism mandates that the mechanism shall have appropriate security safeguards, sets forth standards for the user experience, mandates that the Delete Act’s rights be effectuated through one request, and sets forth certain accessibility standards.<sup>45</sup> It does not grant the Agency authority to require data brokers to reformat their preexisting databases, which could be prohibitively expensive for smaller data brokers, technically incompatible with existing legitimate business operations, and unnecessary for achieving the Delete Act’s goals. The overly prescriptive nature of this section does not reflect industry standards. For example, if the requirement to remove special characters is implemented, the address 123 ½ Main Street would be transformed—inaccurately—to 12312 Main Street. People whose names contain special characters or characters from non-Latin alphabets would be listed inaccurately, with potentially discriminatory consequences. For example, many Hispanic surnames are hyphenated. Moreover, requiring all data brokers to maintain uniform systems will increase their vulnerability to cyber threat actors, who would then have a more accurate roadmap of any systems they intend to exploit.

**f. *There should be a safe harbor period for DROP compliance.***

The initial version of the CCPA provided for a 30-day right to cure<sup>46</sup> that allowed covered entities time to respond and address alleged violations before facing an enforcement action. Given the substantial undertaking required of data brokers to adjust their compliance processes to comply with the DROP and the state’s experience with the CCPA’s right to cure successfully helping businesses transition to a new regulatory regime, the Agency should provide a similar right to cure for DROP compliance, with an appropriate sunset date, in the final regulations.

**II. Potential Constitutional Issues.**

**a. *First Amendment.***

The Proposed Regulations present some constitutional issues of first impression. However, there are strong arguments that a court would be bound by Supreme Court and Ninth Circuit precedent to evaluate the provisions under the strict scrutiny standard of review. “Content-based laws—those that target speech based on its communicative

---

<sup>43</sup> Proposed § 7613(a)(1)(A).

<sup>44</sup> Cal. Civ. Code § 1798.99.87(a) (The Agency “may adopt regulations pursuant to the Administrative Procedure Act . . . to implement and administer this title”) (emphasis added).

<sup>45</sup> Cal. Civ. Code § 1798.99.86.

<sup>46</sup> Originally codified at Cal. Civ. Code § 1798.155(b), which provided: “A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.”



content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests . . . Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed.”<sup>47</sup> The Proposed Regulations allow consumers to demand that particular companies delete particular information—*i.e.*, particular content—from their records. These provisions necessarily mean that the relevant companies will no longer be able to (1) disclose that information to others, or (2) send targeted communications to those consumers. The Proposed Regulations are therefore speaker and content-based limitations on speech and subject to strict scrutiny. “In the ordinary case it is all but dispositive to conclude that a law is content based and, in practice, viewpoint discriminatory.”<sup>48</sup>

If forced to defend the constitutionality of these provisions, the state will almost certainly argue that the Proposed Regulations affect only commercial speech and therefore should be evaluated under intermediate scrutiny. However, speech is commercial, and subject to lesser scrutiny, only when it does “no more than propose a commercial transaction.”<sup>49</sup> In the Ninth Circuit, courts consider three factors to determine if speech is commercial: whether it is an advertisement, whether it refers to a particular product, and whether the speaker has an economic motivation.”<sup>50</sup> Although data brokers have an economic motivation, the other factors do not apply to the storage of consumer information, nor does that relevant data propose a commercial transaction. Indeed, courts routinely hold that dissemination of addresses and phone numbers, even by for-profit businesses, constitutes non-commercial speech.<sup>51</sup>

However, even if the Court were to apply intermediate scrutiny, the Proposed Regulations will fail if they are not sufficiently “drawn to serve the State’s asserted interest,” as required under the test for commercial speech.<sup>52</sup> In conducting this analysis, courts must “pay particular attention to attempts by the government to assert privacy as a substantial state interest,” due to the “breadth of the concept of privacy,” because “the government cannot satisfy the second prong of the **Central Hudson** test by merely asserting a broad interest in privacy . . . [but rather] must specify the particular notion of privacy and interest served.”<sup>53</sup>

Complicating matters further for the state, “the right to receive ideas is a necessary predicate to the *recipient’s* meaningful exercise of his own rights of speech, press, and

---

<sup>47</sup> *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).

<sup>48</sup> See *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 564, 571 (2011).

<sup>49</sup> See, e.g., *NetChoice, LLC v. Bonta*, 113 F.4th 1101, 1119 (9th Cir. 2024).

<sup>50</sup> *Id.*

<sup>51</sup> See, e.g., *Dex Media West, Inc. v. City of Seattle*, 696 F.3d 952, 962 (9th Cir. 2012) (phone numbers and community information in telephone directory); cf. *IMDb.com v. Becerra*, 962 F.3d 1111, 1122 (9th Cir. 2020) (online database containing ages and dates of birth).

<sup>52</sup> See *Sorrell*, 564 U.S. at 571-72 (citing *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 566 (1980)).

<sup>53</sup> See *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234 (10th Cir. 1999).

political freedom.”<sup>54</sup> “[T]he State may not, consistent[] with the spirit of the First Amendment, contract the spectrum of available knowledge.”<sup>55</sup> The risk of inadvertent mass opt-outs due to the lax identity matching standards which would infer requests rather than verify them,<sup>56</sup> the lack of verification procedures for authorized agents,<sup>57</sup> and the inadequate provisions for informed consent<sup>58</sup> will result in the restriction of information to consumers without their consent.<sup>59</sup>

As explained above, the Proposed Regulations overlook a number of better-tailored and more-effective alternative approaches, and there are strong arguments that they are not sufficiently drawn to serve the state’s interests.

### **b. Takings Clause.**

Databases represent valuable property interests developed through substantial investment, innovation, and creativity by data providers in collecting, organizing, and maintaining the data. The Takings Clause of the Fifth Amendment, as incorporated against the States by the Fourteenth Amendment, provides that private property shall not “be taken for public use, without just compensation.”<sup>60</sup> By forcing data providers to alter the nature of their databases by reformatting their language in a way that will undermine the integrity of the connections between data points, the government may be unconstitutionally depriving them of their property interests without just compensation. “The Fifth Amendment’s guarantee that private property shall not be taken for a public use without just compensation was designed to bar Government from forcing some people alone to bear public burdens which, in all fairness and justice, should be borne by the public as a whole.”<sup>61</sup> The formatting requirements in the Proposed Regulations<sup>62</sup> do not go to the core of the government’s interest in facilitating its citizens’ right to delete. They appear to exist for some unquantified benefit to the Agency in standing up a new database while significantly hampering the functionality of preexisting databases.

There is no set formula to determine where a regulation ends, and a taking begins. The Supreme Court has set forth three factors to be considered in evaluating regulatory takings claims: (1) the economic impact of the regulation; (2) the extent of its interference

---

<sup>54</sup> *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982) (emphasis in original).

<sup>55</sup> *Id.* at 866-69.

<sup>56</sup> See *supra*, section I.a.

<sup>57</sup> See *supra*, section I.b.

<sup>58</sup> See *supra*, section I.c.

<sup>59</sup> “The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers.” *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982).

<sup>60</sup> U.S. Const. amend. V.

<sup>61</sup> *Armstrong v. United States*, 364 U.S. 40, 48-49 (1960) (holding government acquisition of property for which materialmen had liens was unconstitutional taking where it “destroyed the value of the liens”).

<sup>62</sup> Proposed § 7613(a)(1)(A).

with investment-backed expectations, and (3) the character of the government action.<sup>63</sup> Many cases turn on the nature of the property right itself.

In ***Ruckelshaus v. Monsanto Co.***,<sup>64</sup> the Supreme Court recognized that intangible information such as databases and collections of information can be property protected by the Takings Clause where “the action interferes with reasonable investment-backed expectations.”<sup>65</sup> There, Monsanto was required under the Federal Insecticide, Fungicide, and Rodenticide Act (“FIFRA”) to submit extensive data on its pesticide development to the EPA as part of a registration application.<sup>66</sup> The FIFRA authorized the EPA to use the data in evaluating other applications, and to publicly disclose some of the data.<sup>67</sup> Monsanto sued the EPA, arguing that FIFRA’s provisions allowing the EPA to use its trade secret data for evaluating other applicants were an unconstitutional taking of property without just compensation under the Fifth Amendment.<sup>68</sup> The Supreme Court held that to the extent Monsanto had a property interest in this data under state law—which the parties stipulated it did—that data was protected by the Takings Clause.<sup>69</sup> While the Court held that data submitted to the EPA after FIFRA was amended to give the EPA greater discretion in how to use submitted data was not a taking, it held that data submitted prior to those amendments—when FIFRA allowed applicants to designate their data as confidential trade secrets—and subsequently reused or disclosed by the EPA would be an unconstitutional taking because it “would frustrate Monsanto’s reasonable investment-backed expectation with respect to its control over the use and dissemination of the data it had submitted.”<sup>70</sup> Similarly, CSPRA members have invested significantly in creating databases that do not just store information, but connect it. Their creations allow inferences to be drawn in novel ways, such that the connections built between data points have made the databases more than the sum of their parts.

While the next two cases do not involve the Takings Clause, they provide useful guidance on how courts view the intersection of data and property rights. Where the compilation methodology or structural design of the database itself—reflecting the investment expectations, creative selection, or arrangement of information by the creator—provides independent value, the creator has the right to exclude others.

In ***Assessment Technologies of WI, LLC v. WIREdata, Inc.***,<sup>71</sup> the Seventh Circuit evaluated whether a property data provider’s database of public property information warranted copyright protection. While not involving the Takings Clause, this case

---

<sup>63</sup> *Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 124 (1978).

<sup>64</sup> 467 U.S. 986 (1984) (holding to extent applicant for registration of pesticides had an interest in its health, safety, and environmental data cognizable as a trade-secret property right under state law, that property right was protected by takings clause of the Fifth Amendment).

<sup>65</sup> *Id.* at 987.

<sup>66</sup> *Id.* at 998.

<sup>67</sup> *Id.* at 995-96.

<sup>68</sup> *Id.* at 998.

<sup>69</sup> *Id.* at 1003.

<sup>70</sup> *Id.* at 1011.

<sup>71</sup> 350 F.3d 640 (7th Cir. 2003).

addressed the extent to which databases containing public information constitute property. Assessment Technologies developed software called “Market Drive” that municipalities in Wisconsin used to compile property tax assessment data.<sup>72</sup> The underlying data came from municipal tax assessors visiting the properties and collecting information directly at the site to assess the value of properties for property tax purposes.<sup>73</sup> Once input into the system, the Market Drive program automatically allocated collected data across 456 fields grouped into larger categories, allowing municipal tax officials to use various queries to view the data in different ways.<sup>74</sup> WIREdata, owned by Multiple Listing Services, Inc., wished to obtain the underlying property data in that system for use by real estate brokers.<sup>75</sup> Assessment Technologies sued to stop WIREdata from collecting this information, claiming that the data could not be extracted from its system without infringing its copyright.<sup>76</sup>

While it did allow WIREdata to access the raw data in Market Drive, the Seventh Circuit recognized that Assessment Technologies’ software was subject to copyright protection because no other real estate assessment program arranged the data as it did and “this structure is not so obvious or inevitable as to lack the minimal originality required, as it would if the compilation program simply listed data in alphabetical or numerical order.”<sup>77</sup> The court stressed that data compilations are property from which the owner may exclude others to the extent they take the form of unique arrangements of the data allowing distinctive investment-backed functions, similar to how *Ruckselshaus v. Monsanto* recognized trade secrets as property.

This contrasts with cases where databases involved only the rote copying of information. In *Feist Publications, Inc. v. Rural Telephone Company, Inc.*,<sup>78</sup> for example, a telephone cooperative was required to compile and distribute a “white pages” phone directory to its customers free of charge as a condition of its government-sanctioned monopoly on telephone services in the area.<sup>79</sup> Feist Publications published a telephone directory covering a wider geographic area and sought to obtain the information in Rural’s directory. When Rural refused to license its white pages listings to Feist, Feist “extracted the listings it needed from Rural’s directory without Rural’s consent” and Rural sued for copyright infringement.<sup>80</sup> Unlike Assessment Technology’s database, Rural’s white pages were not entitled to copyright protection because “selection, coordination, and arrangement of Rural’s white pages do not satisfy the minimum constitutional standards for copyright protection” as Rural simply took the raw data provided by its subscribers and

---

<sup>72</sup> *Id.* at 642.

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

<sup>77</sup> *Id.* at 643.

<sup>78</sup> 499 U.S. 340 (1991).

<sup>79</sup> *Id.* at 343-44.

<sup>80</sup> *Id.*

listed it alphabetically by surname.<sup>81</sup> The Court noted that factual compilations *can* possess the originality required to create a property right sufficient to receive copyright protection where the compiler “chooses which facts to include, in what order to place them, and how to arrange the collected data so that they may be used effectively by readers.”<sup>82</sup>

These cases stand for the proposition that the software used to arrange databases is a protected property interest where the compilation methodology or structural design of the database itself enables independent insights.

### **c. Dormant Commerce Clause.**

States may not regulate in a way that discriminates against or excessively burdens interstate commerce.<sup>83</sup> Relevant here, the Delete Act applies to businesses located outside of California if they handle the data of California residents, forcing out-of-state businesses to comply with California’s regulatory scheme even if they have no physical presence there. In addition, the mandatory deletion requirement imposes significant compliance costs for out-of-state data brokers, who must develop a separate process and data systems—and potentially restructure their entire business—to comply with California law. Finally, the mandatory deletion requirements conflict with different state regulations of data brokers, creating a patchwork of laws with varying requirements to the extent that the regulatory inconsistency impermissibly burdens interstate commerce.

While states clearly have authority to regulate the safety of products that come into their boundaries even if it affects business operations outside the state, requiring companies to act outside the state as a prerequisite to doing business in the state may be more susceptible to a constitutional challenge. Moreover, a state law requiring the alteration of records in a database may impinge on data flows which are fundamentally interstate in nature, in violation of the Dormant Commerce Clause.

There is precedent supporting a Dormant Commerce Clause challenge to regulations of interstate data flows. In ***American Libraries Association v. Pataki***,<sup>84</sup> the U.S. District Court for the Southern District of New York struck down a state law making it a crime to use a computer to disseminate obscene visual material which was harmful to minors on the basis it violated the Dormant Commerce Clause.<sup>85</sup> Noting that “the Commerce Clause precludes a state from enacting legislation that has the practical effect of exporting that state’s domestic policies,”<sup>86</sup> the court reasoned that the internet is inherently trans-geographic in nature, “makes it impossible to restrict the effects of the New York Act to conduct occurring within New York” and thus “conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus

---

<sup>81</sup> *Id.* at 362-64.

<sup>82</sup> *Id.* at 348.

<sup>83</sup> *Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970).

<sup>84</sup> 969 F. Supp. 160 (S.D.N.Y. 1997).

<sup>85</sup> *Id.* at 161, 177.

<sup>86</sup> *Id.* at 173-74 (citing *In Edgar v. MITE*, 457 U.S. 624 (1982)).



subordinate the user's home state's policy—perhaps favoring freedom of expression over a more protective stance—to New York's local concerns.”<sup>87</sup> While finding that the protection of children against obscene materials was a legitimate state objective, the court found the statute’s benefits did not outweigh the burdens on interstate commerce because “certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level” and “[t]he Internet represents one of those areas.”<sup>88</sup>

While modern courts have recognized that modern technology’s ability to parse consumers by location may complicate the analysis, these cases are distinguishable. In ***Greater L.A. Agency on Deafness, Inc. v. CNN***, the Ninth Circuit upheld California’s requirement that CNN provide closed captioning on programs accessed on the Internet in California because modern technology allows companies to identify where users are and comply with state law for just residents of one state.<sup>89</sup> In ***Rousso v. Washington State***,<sup>90</sup> the Washington Supreme Court rejected a Dormant Commerce Clause challenge to Washington state’s online gambling laws, reasoning that there was minimal burden to interstate commerce because the ban did not prevent internet gambling businesses from operating outside Washington state, as “those businesses can easily exclude Washingtonians.”<sup>91</sup> We note that the regulations at issue in these cases involved technological requirements—specifically, geolocation technology—that were both common and simple to implement. They did not involve standing up wholly separate databases using different logic to attempt to recreate the carefully constructed connections between vast quantities of data categories, and did not alter the fundamental operations of the business.

\* \* \* \* \*

We hope the foregoing is appropriately responsive to your request. Please contact us if you have any questions about this memo.

---

<sup>87</sup> *Id.* at 177.

<sup>88</sup> *Id.* at 181.

<sup>89</sup> 742 F.3d 414, 433 (9th Cir. 2014).

<sup>90</sup> 170 Wash. 2d 70, 82 (2010).

<sup>91</sup> *Id.*

**Grenda, Rianna@CPPA**

---

**From:** Hancock, Jeremy <Jeremy.Hancock@experian.com>  
**Sent:** Tuesday, June 10, 2025 4:50 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** Experian Comments in Response to CPPA RFC on Proposed Accessible Deletion Mechanism (DROP) Regulations.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please find the attached comments on behalf of Experian.



555 12<sup>th</sup> St NW, Suite 504  
Washington, DC 20004  
[www.experian.com](http://www.experian.com)

June 10, 2025

Via electronic filing

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

Re: Public Comment on Accessible Deletion Mechanism

California Privacy Protection Agency:

On behalf of Experian, we submit these comments in response to the California Privacy Protection Agency's ("CPPA") or ("Agency") invitation for comment dated April 25, 2025 on the proposed regulations to stand up the accessible deletion mechanism (*i.e.*, the "DROP") under the California Delete Act.<sup>1</sup>

Respecting consumer privacy is central to Experian's corporate principles and operational values. Our products and services provide significant benefits to consumers and businesses. For example, Experian's offerings provide value by, among other matters: protecting families from identity theft and fraud; enabling small businesses to find audiences for their offerings; informing consumers about products and services that are relevant to them; and helping to notify consumers of new vehicle safety recalls. All of these offerings, which benefit consumers and the economy, rely on data to function. Consumer trust and effective stewardship of information are vital to our company's continued success.

We provide the following comments to help improve the proposed regulations so they support authentic data deletion choices made by California consumers and align with the California Consumer Privacy Act ("CCPA"). Specifically, below we discuss: (1) the need for consumer and authorized agent verification procedures within the DROP; (2) the over-inclusivity of the proposed match-rate rule, which is likely to result in data deletion Californians did not authorize; and (3) conflicts between the CCPA and the proposed rules related to the requirement for data brokers to report the status of deletion requests made through the DROP. We appreciate the opportunity to respond to the Agency's request for comment.

---

<sup>1</sup> California Privacy Protection Agency, Notice of Proposed Rulemaking (Apr. 25, 2025), located [here](#); see also California Privacy Protection Agency, *Proposed Text of Accessible Deletion Mechanism Regulations* (Apr. 25, 2025), located [here](#).

**I. The DROP regulations should require consumer and agent verification consistent with the CCPA.**

The DROP regulations should be updated to explicitly require reasonable consumer and agent verification to harmonize the proposed rules with CCPA verification requirements. Without changes to ensure proper verification, deletion requests through the DROP will adversely affect the rights and freedoms of other consumers and intermediaries will be empowered to submit deletion requests without proper authorization. As presently drafted, the DROP regulations would harm consumers and raise constitutional and statutory issues, as described in more detail below.

**A. The DROP should permit reasonable consumer verification.**

The proposed regulations to implement the DROP do not require verification that a consumer deletion request is associated with a California resident or provide the same verification mandates that are required under existing CCPA regulations.<sup>2</sup> In particular, the proposed regulations contain virtually no safeguards to help ensure that a data broker actions a deletion request on personal information associated with the specific consumer permitted under the CCPA to make a request. For example, the proposed rules state that the CPPA “may” verify an individual’s residency and other data elements about a consumer, but do not require the Agency to do so.<sup>3</sup> They also explicitly prohibit data brokers from contacting consumers directly to verify their deletion requests submitted through the DROP.<sup>4</sup> The lack of verification processes in the DROP would result in a CCPA loophole, whereby individuals who submit deletion requests directly to businesses must be verified by a business but individuals who submit deletion requests through the DROP are not similarly verified. The ultimate result of this inconsistency will be that personal information of California and non-California residents will be deleted or opted out from sale without the consumer actually sending the deletion request, thereby adversely impacting the rights and freedoms of that consumer—a result the CCPA itself specifically forbids.<sup>5</sup>

The proposed DROP regulations thus conflict with the CCPA as well as the CCPA’s implementing regulations, which require a business to establish reasonable methods for verifying that the person making a request to delete is the consumer about whom the business has collected information and to consider whether the personal

---

<sup>2</sup> Compare Cal. Civ. Code §§ 1798.105(c), 140(ak), 145(k) and Cal. Code Regs. tit. 11, §§ 7060 – 7062 with Cal. Code Regs. tit. 11, §§ 7601 – 7622 (proposed).

<sup>3</sup> Cal. Code Regs. tit. 11, §§ 7620(a), (b) (proposed).

<sup>4</sup> *Id.* at § 7616(c) (proposed).

<sup>5</sup> See Cal. Civ. Code § 1798.140(k) (“A verifiable consumer request... to delete a consumer’s personal information... shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person.”)

information provided to verify them is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.<sup>6</sup>

Considering the range of data broker services provided—from identity theft protection to emergency notices and alert services and more—consumers who do not wish to delete personal information may suffer real harms if a fraudulent deletion request is submitted on their behalf. The proposed DROP rules should be updated to require consumer verification similar to the verification that required of deletion requests under the CCPA.

**B. The DROP should permit reasonable verification of agents’ authority to act on behalf of consumers.**

The proposed DROP rules similarly do not provide for any reasonable authorized agent verification, directly conflicting with the CCPA regulations. The proposed rules require disclosure of an agent’s name and contact information but otherwise contain no procedures to verify an agent’s authority to submit a request on behalf of a consumer.<sup>7</sup> By contrast, the CCPA regulations permit businesses to require agents to provide proof of authority in the form of a signed permission from the consumer.<sup>8</sup> They also permit the business to require the consumer to verify their own identity directly with the business or directly confirm with the business that they provided the authorized agent permission to submit a request.<sup>9</sup> By including no reasonable authorized agent verification provisions, the proposed DROP rules conflict with the CCPA regulations.

Without reasonable agent verification, unscrupulous intermediaries may use the DROP system as a method for competitive interference. Entities with business models that compete with data brokers may act as agents and submit bulk data deletion requests to gain a marketplace advantage against their data broker competitors. In addition, purported “agents” may submit deletion requests for consumers who did not permission them to do so. To avoid gamesmanship and manipulation of the DROP system, the proposed rules should require agent verification consistent with the standards in the CCPA regulations.

Failure to resolve the conflict between the DROP rules and the CCPA regulations on verification would raise concerns under the California Administrative Procedure Act (“APA”) that the DROP rules are inconsistent with other provisions of law.<sup>10</sup> It would

---

<sup>6</sup> See, e.g., Cal. Code Regs. tit. 11, § 7060(c)(3) (noting that when electing a verification method, a business must consider “[t]he risk of harm to the consumer posed by unauthorized deletion” and “[t]he likelihood that fraudulent or malicious actors would seek the personal information.”)

<sup>7</sup> Cal. Code Regs. tit. 11, § 7621 (proposed).

<sup>8</sup> Cal. Code Regs. tit. 11, § 7063(a).

<sup>9</sup> *Id.*

<sup>10</sup> Cal. Gov. Code §§ 11342.1, 11342.2, 11349(b), (d) (each regulation must be within the scope of authority conferred by the statute, in accordance with standards prescribed by other provisions of law, and consistent with other provisions of law).

also create potential constitutional issues. The Supreme Court has affirmed that the processing and disclosure of personal information is protected expression under the First Amendment's Free Speech Clause.<sup>11</sup> As presently drafted, the proposed rules would not withstand any level of First Amendment scrutiny.<sup>12</sup>

## **II. The proposed match-rate rule would result in unauthorized deletion and conflict with data matching requirements under the CCPA.**

The proposed regulations would require data brokers to delete consumer records if more than 50% of the unique IDs in a deletion list match with a consumer in the data broker's records.<sup>13</sup> The proposed rules explicitly state that a data broker considering a deletion list containing a consumer name, date of birth, and zip code would be required to delete records with data elements matching at least two of the three data elements because the match rate would be over 50%.<sup>14</sup> As a result, if Mary Smith, born on January 1, 1985, living in zip code 94203 submits a deletion request, a data broker would be required to delete records associated with every Mary Smith living in zip code 94203, as well as every person born on January 1, 1985 living in zip code 94203. This result is over-inclusive and is significantly likely to result in deletion of data associated with consumers who do not wish to have data about them deleted.

The proposed match rate rule also directly conflicts with data matching requirements for deletion requests under the CCPA. This conflict would create significant operational challenges and could also run afoul of the California APA.<sup>15</sup> Deletion requests under the CCPA must be verified to a high or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion.<sup>16</sup> A reasonably high degree of certainty requires matching at least three pieces of personal information provided by the consumer with personal information maintained by the business.<sup>17</sup> The DROP rules are not harmonized with this requirement, as data deletion would be mandated if fewer data elements are matched so long as the match rate is 50%. The proposed DROP rules should be updated so they are interoperable with the CPPA verification requirements.

## **III. The proposed data standardization requirements would unreasonably interfere with data brokers' databases.**

The proposed regulations would require data brokers to implement measures to structure their internal databases in specific ways to increase the likelihood that an identifier in a deletion list will match to a consumer record in the data broker's systems.

---

<sup>11</sup> *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 558–59 (2011).

<sup>12</sup> The Delete Act and the DROP rules also raise concerns under the Takings Clause and Contracts Clause.

<sup>13</sup> Cal. Code Regs. tit. 11, § 7613(a)(2)(A) (proposed).

<sup>14</sup> *Id.*

<sup>15</sup> Cal. Gov. Code §§ 11342.1, 11342.2, 11349(b), (d).

<sup>16</sup> Cal. Code Regs. tit. 11, § 7062(c).

<sup>17</sup> *Id.* at § 7062(b).



The proposed rules would specifically require data brokers to remove extraneous or special characters from databases, use only lowercase letters, and implement any other standardization method that might increase the likelihood of a match.<sup>18</sup> These proposed mandates are overly burdensome, would interfere with data brokers' proprietary datasets, and could negatively impact the quality and accuracy of data maintained in systems. In addition, the requirement creates First Amendment concerns because it impacts data brokers' ability to engage in protected speech and provide the customized data products and services their customers desire and expect. The proposed rule should be struck from the proposed regulations.


**IV. The proposed DROP request status reporting requirements should be harmonized with consumer rights request timelines under CCPA.**

The time period associated with the proposed requirement for data brokers to report the status of deletion requests received through the DROP is shorter than the time period the CCPA allows businesses to execute such requests. The proposed DROP rules should be harmonized with the CCPA's consumer request effectuation timelines. Under the proposed DROP rules, each time a data broker accesses the DROP (which must be at least once every 45 days), the data broker would be required to report the status of the deletion requests it received during its previous access session by providing response codes indicating whether individual records were deleted, opted out of sale, exempted, or not found in the data broker's records.<sup>19</sup> As a result, data brokers under the proposed DROP rules would be required to effectuate deletion requests received through the DROP within a 45-day period, at most. The CCPA provides businesses up to 90 days to complete a deletion request if a business requests an extension in line with CCPA requirements.<sup>20</sup> The timeline for reporting the status of DROP requests should be aligned with the CCPA by requiring data brokers to submit these responses every 90 days instead of every 45 days.

\* \* \*

Thank you for this opportunity to provide input into this rulemaking under the California Delete Act. We look forward to continuing to work with the Agency on these important matters.

Regards,



Jeremy Hancock  
Vice President, Government Affairs

<sup>18</sup> Cal. Code Regs. tit. 11, § 7613(a)(1)(A)(ii) (proposed).

<sup>19</sup> *Id.* at §§ 7612(a), 7614 (proposed).

<sup>20</sup> Cal. Civ. Code § 1798.130(a)(2)(A).

**From:** Jake Boggan <jake@forgetmenaut.com>  
**Sent:** Tuesday, June 10, 2025 3:12 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Accessible Deletion Mechanism

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

My name is Jake Boggan and I am the founder of Forgetmenaut, a software platform for automating data privacy compliance. I am writing to express my strong support for the new regulations enabling the DROP platform. This will strengthen the privacy interests of Californians, automate and clarify the compliance process for existing data brokers, and will serve as a model for other state efforts in regulation.

The current text is well thought out and anticipates several wrinkles in implementation. I do however have several suggestions that would reduce false negatives for deletion requests and improve the overall utility of the platform:

**Re: Section 7613.a.1.A :**

**" Prior to comparing consumer identifier information between a consumer deletion list and a data broker's records, a data broker must standardize the applicable personal information from the data broker's records as follows:"**

- More specification should be given as to the exact ISO format the DROP platform will be using for birth dates, as slight changes to this would be easily interpreted by humans but would result in wildly different values when hashed. I would suggest ISO 8601 YYYY-MM-DD format, '2025-06-10' for example.
- Zip code formatting should also be formalized since the 5 digit and 5+4 digit formats commonly used hash to different values. I recommend just using the 5 digit format since this is sufficient with name and birthdate for identification, and is present in any dataset where California zip codes are recorded. '90210' for example.
- Phone formatting should be formalized with no special characters or country code, since the scope of this platform is restricted to Californians. The 10 digit subscriber number as a single string should be the format, '2135555555' for example. Though not as easily readable as other common formats this avoids all changes to the final hashed value based on whitespace, special characters, and optional country code that many phone formats could differ by. All datasets used by data brokers can reduce to this format for comparison without losing any specificity.

**Re: Section 7613.a.1.B:**

**"After completing the standardization described in subparagraph (A), a data broker must use the same hashing algorithm provided in the consumer deletion list to hash the consumer personal information within the data broker's records that is the same category of identifier as in the consumer deletion list."**

- I recommend using the SHA-256 hashing algorithm for all use cases in the DROP platform as it is ubiquitous and easily accessible in a variety of free implementations for the data brokers to use.

**Re: Section 7612.b:**

**"A data broker may access the DROP manually or through automated means in formats supported by the DROP. If a data broker is unable to timely download its selected consumer deletions list(s) in compliance with subsection (a) through automated means for any reason, the data broker must manually download its consumer deletions list(s) through its DROP account. (1) If a data broker's automated connection with the DROP fails and is not the result of the data broker's error, the data broker must notify the Agency of the connection failure in writing through its DROP account within 45 calendar days of its last access to the DROP."**

This section anticipates the utility of automated means such as a 3rd party software provider to automate, document, and act on a data broker's duties under current law. As a provider of such software I highly encourage this and hope that each data broker will be provided an appropriately scoped API key so that 3rd party providers may automate their interface with the DROP platform on their behalf.

I would request that the subsection concerning when the "automated connection with the DROP fails" is expanded upon or clarified so that the CPPA is not inundated with notifications of little value. I read this section and am inferring the spirit to be "if a data broker has chosen a 3rd party provider to automate their responsibilities on the DROP platform and that provider's service is failing such that the data broker would be in breach of its 45 day requirement because of a prolonged failure, that is not the data broker's fault then they must notify the Agency." However the phrase "automated connection with the DROP fails" can be literally interpreted to cover a large number of routine events when one talks about automating a connection via an API, most of which are handled seamlessly when connections fail or servers experience high load, usually handled with subsequent retries. If the DROP platform itself experiences short-lived service issues and returns HTTP 503 codes then under the current text of this regulation I would think that would necessitate writing to the Agency about any failed connections during that time. Given the large number of individual API requests that transpire during what is colloquially thought of as a "connection", this would result in a large number of notifications of little cumulative value.

It would be good to clarify whether this subsection is intended for a) notifying the Agency that an automated service used by a data broker is not fulfilling its responsibilities or b) an enhanced logging feature for all service and connection issues stemming from automatic connection with the DROP platform. I interpret it as a) but suggest different wording if that is the case to avoid an interpretation similar to the latter case.

Proposed change:

**"If a data broker's automated *interaction* with the DROP fails **for more than 14 days** and is not the result of the data broker's error, the data broker must notify the Agency of the failure in writing through its DROP account within 45 calendar days of its last access to the DROP."**

This change would clarify the intent of relieving the data broker of any wrongdoing in fact caused by an intermediary's fault, while also giving a realistic time frame for an intermediary (or the DROP platform itself) to rectify any brief outages which are commonplace in software platforms.

**Re: Section 7613.c:**

I strongly support this measure as it protects the data of a consumer that comes into a data broker's possession after the effective date of that consumer's privacy request. It is not difficult to implement, especially for an automated system.

I look forward to the final versions of these regulations and the implementation of the DROP platform.

Sincerely,  
Jake Boggan

**Grenda, Rianna@CPPA**

---

**From:** Ben Isaacson <ben@inhouseprivacy.com>  
**Sent:** Tuesday, June 10, 2025 3:38 PM  
**To:** Regulations@CPPA  
**Subject:** In-House Privacy, Inc. Comments Re: SB 362 'DROP' Rulemaking  
**Attachments:** IHP CPPA Delete Act June 2025 Comments .pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Greetings,

On behalf of In-House Privacy Inc, I am submitting the following written comments. I welcome any feedback or the opportunity to further clarify these comments at any time.

Best regards,

--Ben Isaacson



**Ben Isaacson** Principal | In-House Privacy, Inc. CIPP/US, CIPP/E m. [REDACTED] w.  
[www.inhouseprivacy.com](http://www.inhouseprivacy.com) e. [ben@inhouseprivacy.com](mailto:ben@inhouseprivacy.com)



## **In-House Privacy, Inc Comments to the California Privacy Protection Agency (CPPA) Regarding SB 362 ‘Delete Act’ Rulemaking Regarding the Data Broker Registration and Accessible Deletion Mechanism (DROP)**

**Introduction:** In-House Privacy, Inc (“IHP” or “We”) is a law firm that serves many companies in the advertising and marketing industry. These comments are our own, and do not reflect the opinions of any specific client.

We respectfully urge the CPPA to consider the following changes to its proposed DROP rulemaking.

### **Index**

- I. General Policy Considerations**
- II. General Technical Considerations**
- III. Specific Rulemaking Comments**
- I. General Policy Considerations**

These comments encompass areas for the CPPA to consider in conjunction with the rulemaking that are not expressly stated in the rulemaking itself.

#### **A. Introduce a ‘cure period’ or ‘warning system’ for erroneous implementation of DROP**

Neither the text of SB 362 nor any existing rulemaking indicates whether the CPPA will consider notifying a data broker of an error in its application of the DROP. As the DROP is anticipated to include numerous operational and technical challenges for data brokers as indicated in the comments below, the CPPA should consider a policy to enable data brokers to correct any such errors with its application. These corrections could take the form of either a formal ‘cure period’ which would be a designated period of time, such as the standard 45 days allocated for regular DROP access, and/or a ‘warning’ policy that the CPPA delivers to data brokers who incorrectly applied the DROP with compliance information how to avoid statutory penalties.

For example, the California Consumer Privacy Act (CCPA) originally required the Attorney General to issue a 30 day cure period during the first two years in which the CCPA was in effect. This cure period was later





amended by the California Privacy Rights Act (CPRA) ballot measure, yet still enables the Attorney General to issue any such cure period notices.<sup>1</sup>

IHP recommends a similar cure period regulation whereby the CPPA will introduce a one year or more cure period and enable data brokers at least 45 days to apply any indicated DROP-related errors following the enactment of the DROP on August 1, 2026.

## **B. Exempt Select Data Broker Intermediaries**

The definition of data broker in SB 362 and subsequent regulations does not explicitly exempt business intermediaries that support data brokers where they engage in ‘making available’ third-party data to other businesses.

In the context of this rulemaking, the CPPA should exempt intermediary businesses that operate under the following criteria:

1. The business contracts with their clients as designated ‘service providers’ in compliance with the requirements set forth in the CCPA and subsequent rulemakings.<sup>2</sup> In that role, they are instructed by their clients to procure third-party data from data brokers on their behalf.
2. They do not create or provide any proprietary ‘data products’ that combine or otherwise utilize any data procured on behalf of clients in a manner that gives their business any independent use of the data.
3. They may receive monetary or other benefits from their services in support of procuring the data broker data, such as fees associated with purchasing media utilizing the data, their labor procuring the data, or payment for services that integrate the data with internal or external applications. However, these intermediaries should not receive a paid commission from data brokers as a ‘reseller’ of the data.

As long as the items above are satisfied, exempted intermediaries

---

<sup>1</sup> Stats. 2024, Ch. 121, Sec. 7. (AB 3286).

<sup>2</sup> Cal. Civ. Code § 1798.140(ag) (defining a ‘service provider’); Cal. Civ. Code § 1798.100(d) (enumerating that a business must enter into an agreement with a service provider when that business sells or shares personal information with such service provider); Cal. Code Regs. Tit. 11, § 7051 (expanding on the contract requirements set forth by the CCPA between businesses and service providers).



would be empowered to procure data broker data on their clients behalf without requiring their clients to execute purchase agreements directly with data brokers, nor would these intermediaries be required to contract with data brokers as their 'service providers.'

Below are three potential categories of intermediary businesses:

1. Advertising or marketing agencies that assist advertisers or marketers with identifying, distributing, and measuring advertising or marketing campaigns. They may procure third party data on behalf of their clients to create lists of prospects to engage with, append demographic information to their client information, or engage in media planning, measurement or market research on their clients behalf.
2. Software as a Service (SaaS) platforms that provide the software and operational mechanisms to procure and enable their clients to utilize third-party data in conjunction with their SaaS platform, such as cloud hosting, call centers, email or postal service providers, and digital advertising services that do not directly engage in cross-contextual behavioral advertising, such as with data clean rooms, measurement, or media planning activities.
3. Data marketplaces that are not commissioned 'resellers' themselves, but rather promote data broker offerings and are paid to integrate or otherwise use the third party data in conjunction with their SaaS or other services.

#### **C. Consider Additional Regulations For Newly Acquired Consent**

SB 362 does not describe a process where data brokers may continue to process the personal information of DROP-registered CA consumers following their initial application of the DROP, but where the consumer has subsequently re-consented for their data to be sold to data brokers. For example, many consumers enter sweepstakes where the terms of the sweepstakes explicitly require their affirmative consent for the sponsor to sell their personal information to data brokers. Under the existing text of SB 362 and these proposed regulations, there is no express exemption for a new sweepstakes entry or other form of affirmative consent for third party data use to override their DROP registration.



There are numerous regulatory examples where such consent can override previous privacy choice registrations, such as with the federal Telephone Consumer Protection Act (TCPA) and FTC ‘Do Not Call’ (DNC) list where an express written consent for telemarketing (or SMS) can override their DNC registration.<sup>3</sup>

California law includes such a ‘consent override’ with the CCPA and subsequent rulemakings around the personal information use associated with minors, sensitive information, financial incentives, and opt-out preference signals.<sup>4</sup>

A new regulation should be established that in the event that a data broker receives new personal information based on affirmative consumer consent to sell their data to data brokers, that any existing DROP deletion or suppression is inapplicable insofar as the data broker can provide evidence that such consent took place following the consumers DROP registration.

## II. **General Technical Considerations**

### A. **Small Business Considerations**

Many data brokers are small businesses and the current rulemaking imposes significant technical and operational burdens. While we identify many of these technical limitations below, it may be helpful for the CPPA to understand that many of the registered data brokers do not ‘compile’ data themselves, but rather ‘pass through’ data from other data brokers to their clients. They merely source lists on behalf of their clients, potentially combine lists together to create an aggregated audience from multiple sources, and then deliver the list to their clients and/or their representatives. In these situations, these data brokers do not store third-party data for a lengthy period of time, but rather only so long as is

---

<sup>3</sup> 47 CFR §§ 64.1200(a)(1)-(3) (carving out ‘prior express consent’ or ‘prior express written consent’ of the called party as an exception to the general rule against use of artificial or prerecorded voice calls, or for advertising or telemarketing purposes); 16 C.F.R. § 310.4(b)(1)(iii)(B) (carving out “express agreement, in writing” as an exception for initiating any outbound telephone call to a person whose telephone number is on the do-not-call registry).

<sup>4</sup> Cal. Civ. Code § 1798.120(c) (permitting the sale or share of a child’s personal information when the consumer or consumer’s guardian has affirmatively authorized the sale or share of the consumer’s personal information); Cal. Civ. Code § 1798.121(b) (permitting the usage or disclosure of sensitive personal information with subsequent consent from the consumer after a consumer had previously opted-out); Cal. Civ. Code § 1798.123(b)(3) (requiring opt-in consent by consumers before enrolling consumers in financial incentive programs); Cal. Civ. Code § 1798.135(b)(2) (allowing businesses to ignore opt-out preference signals with the consumer’s consent).



necessary to complete their delivery or measurement activities. In many cases, they may not even store the data beyond the 45 day period in which they are required to apply the DROP updates to these lists. As a result, many of the burdens being placed on these entities to access and combine data from the DROP to each of their 'passed through lists' every 45 days where they do not maintain any centralized 'database' in which to apply the DROP deletions will lead to their creation of a very large suppression file of every DROP registered user that they will store in perpetuity and apply against every new list they procure on their clients behalf. In essence, the 'DROP' will not operate as intended to 'delete' data, but rather as a suppression file.

As a result, the regulations should be amended to address 'pass through' data brokers who are not 'compilers', and consider separate processes for those entities to be exempt from many of the technical requirements in the regulations as indicated below. In summary, the CPPA should strongly consider enabling data brokers to access and apply a simple 'Do Not Sell' suppression list instead of requiring the comprehensive 'deletion' process specified in the regulations.

#### **B. Data Broker Representative Agent Designations/Services**

The draft regulations assume that registered data brokers will exclusively process the DROP updates on their own behalf. However, many data brokers utilize service providers to assist with managing their data services. These service providers could be given the DROP account credentials by data brokers to process these updates on data brokers behalf. Further, some data brokers may provide these updates on behalf of other data brokers with whom they sell or manage data on their behalf.

The CPPA should specify in the DROP account management process an option for data brokers to delegate access to other entities to manage the DROP updates on their behalf.

#### **C. Pre-Implementation Test Environment**

At least ninety (90) days prior to the August 1, 2026 implementation date, the CPPA should make the DROP available to data brokers in order to test its operational capabilities in advance of the official implementation date. This could be deemed a 'beta test' with actual Californians data, or be a 'test environment' where synthetic (not actual) data is loaded into the



DROP in order for data brokers to attempt to apply it to their systems and provide feedback to the CPPA on operational performance.

#### **D. Explicit Right To Forward Suppression List**

SB 362 does not explicitly grant data brokers the right to forward the suppression lists. In order for data brokers to comply with CPRA's requirement to notify all third parties to whom the business has sold/shared the consumer's personal information, of the consumer's request to opt out<sup>5</sup> or request to delete.<sup>6</sup>

The CPPA should amend the rules to explicitly grant data brokers the right to pass along suppression lists in order to comply with law. Moreover, passing entire lists would better facilitate consumer wishes.

#### **E. Limit Data Hygiene and Combination Requirements**

As noted in the comments below, the draft regulations assume that data brokers have the technical capability to modify and match data across disparate data sets. In other words, the CPPA is proposing that data brokers engage in 'ID Graphing' or 'ID Resolution' services in order to effectuate the DROP updates. The technical requirements for applying the DROP should be designated for the lowest common denominator of data brokers, and not the most sophisticated larger businesses that are capable of such modifications and combinations of data.

The CPPA should amend some of the requirements requiring data brokers to perform technical data hygiene, data modification, and combinations of data that would be a burden on small businesses and less sophisticated data brokers. In the least, these regulations should be delayed for at least one year following the DROP enactment to give these data brokers time to invest in the necessary technology requirements to comply with these compliance obligations, and/or outsource these technical operations to data service providers or other data brokers on their behalf.

Moreover, requiring data brokers to engage in data combinations may be contrary to the privacy preserving intent of this law because it requires data brokers to be provided with and to process or store more personal information than they otherwise would.

---

<sup>5</sup> Cal. Code Regs. tit. 11, § 7026(f)(2).

<sup>6</sup> Cal. Code Regs. tit. 11, § 7022(b)(3).



### III. Specific Rulemaking Comments

To enhance the proposed regulation and address potential vulnerabilities, we submit the following important considerations for the upcoming discussions.

#### **ARTICLE 2. DEFINITIONS AND REGISTRATION REQUIREMENTS**

##### **§ 7601. Definitions.**

As previously discussed, we find that the proposed language does not properly contemplate the potential effects on the wide range of businesses that will fall under the regulations:

##### **§ 7601(a).** “Access the Delete Request and Opt-out Platform (“DROP”)”

- (i) As noted, the CPPA should include the term “or their agent” in association with all references to “data broker” in conjunction with access rights to the DROP. In addition, the concluding statement “and does not include signing into a data broker’s DROP account without retrieving a consumer deletion list” is potentially misaligned with situations where the DROP may be accessed simply to check on the status of newly updated lists and should be removed for simplicity purposes.

##### **§ 7601(c).** “Consumer deletion list”

- (i) The title ‘deletion list’ may also be deemed a ‘suppression list’ should the list not be matched, and the CPPA should consider expanding the scope of this definition to include the specific reference to such use as ‘Consumer deletion or suppression list.’
- (ii) This definition could be simplified to remove the final sentence “When made available...” which should separate and specifically define each term used, notably ‘hashed format’, ‘transaction identifier’, and hashing algorithm’ separately and each with their own regulatory applications in the mechanism in which the ‘Consumer deletion list’ must be applied. As written, the combination of the definition of the ‘list’ with the extra terminology around the ‘mechanism’ in which the list will be applied adds complexity and confusion.
- (iii) Privacy-by-design principles indicate that “date of birth” may not be a necessary attribute to be shared in conjunction with the ‘Consumer deletion list’. While it may be necessary for California residency verification, it is not a widely used attribute by the majority of data broker





activities and could lead to widespread distribution of additional personal information that a consumer would not expect to be shared by their state privacy agency with hundreds of data brokers on a regular basis.

**§ 7601(d). “Direct relationship”**

- (i) This statement should be further clarified with specific exemptions; “A business does not have a “direct relationship” with a consumer simply because it collects personal information directly from the consumer; the consumer must intend to interact with the business.”
  - (1) “Intent” must be accompanied by objective variables that a business can use to defend against potential compliance violations, namely;
    - a) Was the consumer presented with adequate notice and choices about sharing personal information with ‘another business’ that may be operating in conjunction with the website or business owner, notably;
      - i) Through a ‘consent management platform’ (aka; ‘cookie banner’) that presents all of the third party advertising services that may use the visitors’ data for cross-contextual behavioral advertising or other purposes in compliance with a CCPA ‘sale or share’<sup>7</sup>.
      - ii) Through a browser extension or ‘widget’ that presents incentives, coupons or other options for the consumer to interact with while sharing that information with the third party business for monetization purposes.
    - b) Did the consumer sign up for an incentive program, sweepstakes, contest or other third party benefit through the website or business, such as at/following an ecommerce checkout page.
    - c) Did the consumer affirmatively check a box as part of a marketing subscription that included consent for specifically named third party marketing offers with a link to the privacy policy with adequate disclosures about such use.

---

<sup>7</sup> Cal. Civ. Code §§ 1798.140(ad); 1798.140(ah).



**§ 7601(g). “Extraneous or special characters”**

- (i) As noted below, this definition should be removed from the regulations at this time. Data brokers should not be required to conduct forensic analysis and data hygiene in their application of the DROP as it is an unnecessary technical burden on small businesses and unsophisticated data brokers. In the least, this requirement should be pushed out a year or more for data brokers to technically prepare for such a requirement.

**§ 7601(i). “Personal information associated with a matched identifier”**

- (i) The reference to ‘inferences’ should be clarified to apply exclusively to ‘individual identifiers associated with the DROP’ and not all ‘personal information’ which could include ‘households’ or other more aggregate associations such as geographic representations.

**§ 7601(j). “Register”**

- (i) The terms include “or its agent” but “Agent” is not defined nor does the regulations describe the scope that an Agent can operate on behalf of a data broker to access and manage DROP updates.

**§ 7601(k). “Registration period”**

- (i) The CPPA should clarify that the ‘registration period’ definition pertains to DROP renewals, and the CPPA should enable new registrants to register at any time, pursuant to the prorated periods and costs indicated in Section 7611.

**§ 7601(l). “Reproductive Health Care Data”**

- (i) Point (2) and Point (3) by reference includes the term “or desire to have children” which is quite broad and could mistakenly include behavioral activities or casual correspondence between app users and unknowingly implicate the business or third party advertising services. This reference should be removed or include the terms “knowingly” in conjunction with this data use.

**§ 7602. Registration Submission Requirements.**

**§ 7602(b).** *“[Registration must be completed by one with] sufficient knowledge of the data broker’s practices to provide accurate information and otherwise comply with the requirements in section 7603. The employee or agent who registers the data broker*



*must certify under penalty of perjury that to the best of their knowledge the information they submit is true and correct.”*

The regulation mandates that the registering party possess both comprehensive knowledge of the data broker's practices and the operational capacity to execute the registration. We recommend separating these requirements by replacing "and" with "or," thereby enabling multiple individuals to contribute to the registration process, provided that the combined knowledge and operational capacity requirements are met.

Again, as previously stated, the reference to ‘agent’ is not defined nor the scope of the agent’s role in assisting the data broker accessing and managing the DROP updates.

**§ 7602(c).** *“A data broker cannot amend or withdraw a completed registration after January 31, except as set forth in section 7604.”*

We request the Agency establish clear guidelines for amending completed registrations. Given the complexity of these compliance requirements, particularly for data brokers operating in conjunction with multiple data source partners, the ability to adjust registration details to accurately reflect evolving business practices is crucial. This is especially pertinent considering Section 7603(d), which necessitates granular information regarding personal data categories and specific products or services. Emerging businesses, for instance, may undergo significant business model transformations during their development.

As previously stated, a reference to ‘or agents’ should be added to this section.

### **§ 7603. Registration Information Requirements.**

**§7603(b).** *“All website links and email addresses provided in the registration must be accurate and functioning.”*

Website links and email addresses are liable to change as business conditions and strategies change, or as employees join or leave the organization. Data brokers must be required to represent their information only at the time of registration, although the Agency may consider conditioning the limitation with a requirement to amend registrations, when necessary, within a specified period.

(b) All website links and email addresses provided in the registration must be accurate and functioning at the time of submission.

## **ARTICLE 3. DELETE REQUEST AND OPT-OUT PLATFORM REQUIREMENTS**

### **§ 7610. Delete Request and Opt-out Platform Account Creation.**



### **§ 7610(a)–(a)(2).**

The proposed regulations require data brokers to restrict account credentials and access to DROP to persons, including employees, contractors, or other agents, authorized to act on behalf of the data broker. We urge the CPPA to consider enabling business to register as agents to act on the data broker's behalf by adding "or agents" before "authorized to act on the data broker's behalf" in Sections 7610(a)(1)(A) and 7610(a)(1)(B). Permitting businesses to act as an agent on behalf of the data broker would ease the burden of compliance for many small businesses or 'pass through' data brokers which do not have the resources to manage all DROP requirements. In conjunction with enabling business agents, data brokers should be required to disclose said business agent prior to accessing DROP for the first time; a requirement that could be added in Section 7610(a)(2).

(a) Prior to accessing the DROP for the first time, a data broker or agent shall utilize the Agency's website found at [www.cppa.ca.gov](http://www.cppa.ca.gov) to create a DROP account. To create an account, a data broker or agent must:

(1) Establish a secure username and password ("credentials") and maintain its account security using reasonable security procedures and practices.

At minimum, data brokers must:

(A) Maintain confidentiality of account credentials, and restrict access to its credentials to only persons or businesses authorized to act on the data broker's behalf;

(B) Restrict access to the DROP, and information derived from the DROP, to persons or businesses authorized to act on behalf of the data broker;

### **§ 7610(a)(3)–(a)(3)(A).**

The regulations as currently drafted contain inherent ambiguities that could lead to the unwarranted penalization of data brokers. Specifically, a contradiction exists between Sections 7610(a)(3) and 7610(a)(3)(A). The former provision states that data brokers need only select a minimum of one consumer deletion list to establish an account, while the latter mandates the selection of all consumer deletion lists that could potentially contain identifiers matching personal information within the data broker's systems. Furthermore, the regulations operate under the assumption that a consumer deletion list will exist for every category of identifiers collected by data brokers. Consequently, data brokers could face penalties for non-compliance in situations where the DROP system fails to provide a relevant deletion list.

To rectify this ambiguity and prevent potential unfair penalties, we recommend that the CPPA consolidate these two sections. The revised provision should explicitly require



data brokers to select consumer deletion lists available through the DROP that contain consumer identifiers that they reasonably believe may match with personal information held within the data broker's records.

Moreover, IHP is concerned that an obligation to select all consumer deletion lists that contain a consumer identifier or identifiers that match to personal information about the consumer within the data broker's records will be a burdensome obligation for many data brokers who process a wide range of consumer personal information. If a data broker can process the requests from DROP by only accessing a couple of consumer deletion lists then this obligation should be narrowed and data brokers should only be required to access one or two consumer deletion lists.

### **§ 7610(a)(3)(B).**

Additionally, there is significant ambiguity in a data broker's 'collection' of consumer identifiers. The term "collects" could refer to the initial gathering of data, its ongoing storage, or its active processing, and the ambiguity makes it unclear which specific instances the regulations intend to cover. Rather, we propose that in instances where "collects" is used in Section 7610(a)(3)(B), the draft regulations address consumer identifiers as maintained in systems. By specifying this change, the regulations would clarify that they apply to identifiers actively held within a data broker's operational databases, rather than just the initial collection phase.

**§ 7610(a)(3)(C).** *"A data broker may only change its consumer deletion list selection once every forty-five (45) days."*

Mandating rigid limitations with access to consumer deletion list selection, while simultaneously restricting the ability to modify these selections, may result in unnecessary complications when a data broker needs to re-access a list within the 45 day period. Data brokers should have the flexibility to revise consumer deletion list choices as often as necessary to ensure their compliance obligations.

Alternatively, a clear cure period or exemption should be provided for scenarios where personal information matching attempts within the forty-five day window were erroneously omitted from a list.

### **§ 7611. Data Brokers Who Begin Operating After Registration Period.**

We recommend that this Section 7611 be amended to apply to all data brokers under the purview of the regulations, regardless of when they begin operations as a data broker. The current drafted title of this section implies that the section applies only to data brokers that begin operations after January 31 of a given year. However, the



proposed language does not support this implication,<sup>8</sup> and as such the proposed regulations should be amended accordingly.

### **§ 7611(a).**

The language ‘Prior to operating as a data broker’ is quite broad, and should be narrowed only to ‘after data broker sales activities have commenced’. As written, any data services business that ‘intends’ to sell data must register even before they actually ‘sell’ any data that they did not collect directly. This could lead to the unintended consequence of many companies being labeled as data brokers prior to registration, with statutory penalties for non-compliance. Moreover, the clause “prior to operating as a data broker” is in conflict with Cal. Civ. Code § 1798.99.82(a) which requires companies to register as a data broker in January where in the preceding year the company met the definition of data broker (“On or before January 31 following each year in which a business meets the definition of data broker as provided in this title, the business shall register with the Attorney General pursuant to the requirements of this section.”)

### **§ 7611(a)(2).**

Similar to §7611(a), this section should be rephrased to require data brokers to register and access the DROP only after they engage in data broker ‘sales activities’.

### **§ 7611(a)(3).**

We also urge the Agency to reconsider or clarify that the first-time access fees are exclusively applicable to the year 2026, and that the fee structure for 2027 is subject to review and potential change. Specifically, once the DROP is fully operational, consideration should be given to the possibility of reverting these fees back to their original 2024 fee structure and/or creating a ‘sliding scale’ price structure based on the annual revenue of the business or otherwise in conjunction with the Delete Act enforcement budget necessities.

### **§ 7611(b).**

Moreover, a clear provision needs to be included to exempt data brokers from Section 7611(b) who were operating during 2025 from any retroactive enforcement actions related to unregistered or other potential violations in 2025. This exemption specifically applies to enforcement actions that might be pursued in 2026. This “grace period”

---

<sup>8</sup> Cal. Code Regs. tit. 11, § 7611(a)(3)(A) (proposed) prorates DROP costs from January through December. In no circumstance would these prorated first-time access fees not apply to data brokers registering within the registration period.





ensures that businesses are not penalized for actions taken before the full implementation and understanding of the DROP requirements, particularly in its initial phase.

### **§ 7612. Delete Request and Opt-out Platform Access.**

**§ 7612(a).** *“A data broker must access the DROP to download its selected consumer deletion list(s) at least once every 45 calendar days.”*

The term “at least” potentially conflicts with 7610(3)(C) in compliance with maintaining and responding to consumer deletion lists while simultaneously limiting the data broker’s access to such consumer deletion lists.

(a) A data broker or agent must access the DROP to download its selected consumer deletion list(s) ~~at least~~ once every 45 calendar days.

### **§ 7613. Processing Deletion Requests.**

**§ 7613(a)(1)(A).** *“Prior to comparing consumer identifier information between a consumer deletion list and a data broker’s records, a data broker must standardize the applicable personal information from the data broker’s records . . . .”*

The regulations require that data brokers reformat or create secondary databases to meet the formatting requirements prescribed by the Agency: “use all lowercase letters, including changing names to lowercase” and “remove extraneous or special characters.”<sup>9</sup> The former ‘lower case’ requirement requires minimal effort as it does not change the nature of the email address, but modifying or otherwise removing characters from an email or postal address would impose an undue burden on data brokers, shifting data matching efforts that increase storage, inconsistencies, and security risks. It may also conflict with standard data security practices and existing commercial terms that prohibit data alterations. Moreover, this standardization increases the risk of incorrect data points which may, in turn, decrease match rates. It is recommended to minimize this burden by removing any standardization requirements that would materially change the nature of the consumer information.

### **§ 7613(a)(2)–(a)(2)(A).**

Section 7613(a)(2) includes a 50% rule that is unduly complicated and that may result in reduced privacy for consumers and unnecessary confusion. For simplicity, a data broker should be able to match any ‘deterministic’ data that precisely matches the data in its systems, but not ‘probabilistic’ data that may be associated with additional records.

---

<sup>9</sup> Cal. Code Regs. tit. 11, §§ 7613(a)(1)(A)(i)–(ii) (proposed).



Furthermore, the proposed regulations mandate “the data broker must delete all personal information associated with a matched identifier”.<sup>10</sup> We recommend that, following our previous recommendation, the Agency clarify that such personal information does not include inferences made based on personal information, and instead delete only the specifically enumerated data included in lists. Further, some personal information will be associated with multiple consumers, so the rule should specify deletion of personal data ‘solely or primarily associated’ with the individual on the DROP file.

### **§ 7613(b)(2).**

The regulation mandates forwarding of requests for deletion to all service providers and contractors, but does not require (or enable) the same forwarding to third party businesses including other data brokers.

### **§ 7613(c).**

Section 7613(c) codifies the need for data brokers to maintain a suppression list to run against future consumers in their systems. To comply, data brokers need to continuously maintain and update consumer deletion lists for indefinite periods, as a consumer that submitted a deletion request in 2026 would need to be deleted by the data broker when that consumer’s personal information is collected in 2027. This requirement offers significant data retention, maintenance, and security issues, and directly contradicts principles of data minimization. The Agency presumes that all data brokers will retain consumer deletion lists in a centralized database, which is unlikely for those data brokers that do not maintain such a centralized system. As a result, many data brokers will be required to manually and regularly check the suppression list in perpetuity. Data brokers become responsible for the maintenance and security of another database provided by DROP, and in doing so, become a target for further cybersecurity threats. This may not be such an issue for large enterprise data brokers, but for small businesses, the threat of a cybersecurity event becomes greater. Through the combination of this mandate for the maintenance of a suppression list and the broad definition of a data broker, the Agency risks the antithesis of DROP’s goals: exposing all consumers’ personal information listed in DROP. Since the Agency manages this list in perpetuity, would it not be more reasonable for the Agency to be tasked with managing the suppression list?

Finally, as previously noted, the CPPA should draft regulations that enable data brokers to override the DROP based on affirmative consent of the consumer.

---

<sup>10</sup> Cal. Code Regs. tit. 11, § 7613(a)(2) (proposed); *see also*, Cal. Code Regs. tit. 11, § 7613(b)(1) (proposed) (exhibiting language explicitly requiring deletion of inferences).



### **§ 7614. Reporting Status of Deletion Requests.**

Section 7614 of the draft regulations involves mandatory status reporting of deletion requests which creates a significant and material cost burden on data brokers with uploading proof of each deletion before permission to download the most recent consumer deletion list. In practice, this requirement may be so costly and burdensome that it substantially delays data brokers ability to access the next file within the required 45 days. The CPPA should not need specific proof in order to establish that data brokers are in compliance with each record shared, which could come in the form of any complaints and or enforcement actions. More importantly, the Delete Act specifically requires all data brokers systems to be audited for compliance with the DROP in 2028 which will clearly satisfy this requirement.

We recommend that the CPPA eliminate this requirement from the final regulations, or delay any such reporting requirement to be in conjunction with the Delete Act auditing requirements beginning in 2028. Requiring auditable records associated with DROP reconciliation would be much more manageable for companies and more consistent with analogous regulatory regimes (as with the GDPR, for example), rather than requiring a direct and record level integration with the regulator.

### **§ 7615. Requirements to Stop Accessing Deletion Requests from the DROP.**

Regarding Section 7615, the current draft regulations are ambiguous and appear to contradict earlier provisions. There should be a clear mechanism for an entity to cease utilizing the DROP upon affirming that they no longer qualify as a data broker, without necessitating notification and detailed explanation. Specifically, a straightforward procedure should be established to terminate their DROP account after attestation confirming the cessation of data broker activities.

### **§ 7616. Additional Data Broker Requirements.**

**§ 7616(a).** *“A data broker must only use consumer personal information provided by the Agency, through a consumer deletion list or otherwise, for purposes of complying with Civil Code section 1798.99.86. Selling or sharing consumer personal information provided by the Agency is prohibited.”*

This section confusingly contradicts Section 7612(b)(2) which requires that data brokers forward consumer deletion requests to service providers and contractors. While there is a strong public policy that data gathered from DROP should not be sold or shared, we recommend a carve out for compliance with earlier sections.



**§ 7616(c).** *“A data broker shall not contact consumers to verify their deletion requests submitted through the DROP.”*

As noted, the CPPA should consider exempting situations where a consumer provides affirmative consent for their personal information to be sold to data brokers, which could include verification of their submission.

#### **ARTICLE 4. CONSUMER AND AUTHORIZED AGENT DELETE REQUESTS**

##### **§ 7620. Consumer Deletion Requests.**

###### **§ 7620(a).**

The current draft regulation text states *“Consumers **may** be required to have their California residency verified by the Agency prior to submitting a deletion request.”* It is imperative that consumers submitting deletion requests in the DROP **must** be verified as current California residents. Data brokers should have no requirements to verify or determine the residency status of consumers, and the draft regulations do not provide any feedback mechanism for data brokers to question the residency of consumers. The CPPA should revise this draft regulation to ensure that all consumers' residency is verified, and updated each year as well as at any time upon a consumer's request should they forfeit their residency.

###### **§ 7620(b).**

Further in Section 7620(b), the draft regulations inform that consumers “may add personal information to their deletion requests, including date of birth, email address, phone number, and pseudonymous identifiers, such as a Mobile Ad Identifier (MAID).” However, the stated text further states *“The Agency **may** verify such personal information at any time.”* The Agency should clarify that consumers may submit multiple email addresses when consumers own and maintain multiple email addresses, but that each email address **must be** verified through the DROP system before it is available for data brokers to process.

##### **§ 7621. Authorized Agents.**

Much like our prior comments about verifying consumers, we request that the Agency strongly consider that authorized agents must provide written authorization for their agency, and that the CPPA verify such authorizations. Moreover, requiring the authorized agent be verified aligns with the CPPA § 7026(j) “A business may deny a request from an authorized agent if the agent does not provide to the business the



consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf."



**From:** John Engelke [REDACTED]  
**Sent:** Friday, June 6, 2025 10:00 AM  
**To:** Regulations@CPPA  
**Subject:** Please move with haste to allow rapid, easy consumer access to deletion

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Hello Honorable Regulators,

This letter is written to wholeheartedly support the California Privacy Protection Agency (CPPA)'s efforts to set up a system allowing consumers to opt-out and delete personal information from data broker registries. Consumers are at an overwhelming disadvantage in protecting their privacy, and we need your help. There are a number of legitimate but also bad actors in this field. Please move with haste.

Some days I receive over 10 calls proffering to buy my property or to perform contracting work thereon. Without exception I always ask to remove my name and other information from whatever list being used to contact me. These calls clearly often start with robotic dialers and end in a call center. The phone numbers are overwhelmingly spoofed. My experience is that there is zero interest in removing numbers and other private information from lists. In fact, these scam callers are incredibly insolent and often threaten to call more frequently or even greet my request with profanities. Universally, there is refusal to provide business names, contact information or other originating call list information. Furthermore, these callers frequently misrepresent they are calling from the "State of California Green Energy Program" or other affiliated state agencies. In fact, they impersonate state employees as a sales technique.

My number is listed on the Federal Trade Commission (FTC) Do Not Call Registry, and this fact does not seem to impact their actions whatsoever. They have much more detailed information, though -- ALL of my personal information. My experience is these callers have zero interest in abiding by federal limits on data collection and usage. In fact it is an express form of commercial stalking as they offer to "show up at your home" to provide a quote as "we just happen to be in your neighborhood." And, I'm not even discussing the postal mail that I'm receiving, also. (What a waste of precious natural resources and private/public delivery resources.)

I'd like CPPA to pursue some specific remedies:

- Massive fines for using false or spoofed information to contact consumers.
- All lists should be opt-in, not opt-out.
- Pursue telecommunications regulatory or statutory changes to require a nominal charge for every single phone call made to any recipient within the state. Perhaps if every phone call costs \$0.10



(whether answered or not) then the cumulative effect of that will discourage abuse but have little impact on consumers.

- Pursue instituting a system to detect and identify callers who use robotic calls or otherwise spoofed numbers.

This is really an emergency. Some of us CANNOT block large classes of calls on our phones due to other responsibilities, including caring for ill or infirm elderly parents. We need to be reachable by doctors and care professionals at all hours. Similarly I suspect there are occupations that require similar vigilance. It's a travesty that any of this is allowed to continue. Please move with haste to establish these regulations, systems and other governmental protections for consumers. They should universally be tilted toward consumer interests because of the wild criminal abuses that have been perpetrated with impunity by these data broker companies.

Best Regards,

John Engelke

Consumer subject to ongoing disruptive information broker activity



**Grenda, Rianna@CPPA**

---

**From:** Emily Emery <emily@newsmediaalliance.org>  
**Sent:** Tuesday, June 10, 2025 7:46 AM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Proposed Text of Data Broker Regulations  
**Attachments:** News Media Alliance Comment on Proposed Text on Data Broker Registration 06.10.2025.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please see the attached comment from News/Media Alliance.



**Emily Emery**  
VP – Government Affairs  
**News/Media Alliance**  
Cell: [REDACTED]  
[emily@newsmediaalliance.org](mailto:emily@newsmediaalliance.org)  
[www.newsmediaalliance.org](http://www.newsmediaalliance.org)  
**Follow Us!**   



June 10, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Blvd.  
Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: Public Comment on Proposed Text of Data Broker Regulations Regarding the Definition of “Direct Relationship”**

A thriving, free, and independent press is an essential part of any healthy democracy and plays a vital role in supporting California’s economy and local communities. The News/Media Alliance (“The Alliance”) is a nonprofit organization representing the newspaper, magazine, and digital media industries and empowers members to succeed in today’s fast-moving media environment. The Alliance represents over 2,200 diverse publishers in the United States and internationally, ranging from the largest news and magazine publishers to hyperlocal newspapers and from digital-only outlets to papers that have printed news since before the Constitutional Convention. Alliance members are trusted and respected providers of quality journalism, and the Alliance diligently advocates on a broad range of current issues affecting news media entities, including consumer privacy laws and regulations that relate directly to Alliance members’ trusted relationships with their readers.

The Alliance appreciates the support the California Privacy Protection Agency (“Agency”) has shown for an independent and free press and commends the Agency’s exercise of restraint in another recent rulemaking. In recognition of the extreme hardship that could be imposed on businesses, including news media entities, the Agency Board announced<sup>1</sup> at its April 2025 meeting its decision that it would narrow its proposed rulemaking on regulating automated decision-making technologies, consistent with comments filed by hundreds of organizations, including the Alliance.<sup>2</sup>

We urge the Agency to again take a similar moderating approach in its proposed text establishing regulations<sup>3</sup> for data brokers under California Code of Regulations (“CCR”) Title 11, Division 6, Chapter 3, Article 2, Section 7601(d), particularly concerning the revised definition of “direct

---

<sup>1</sup> California Privacy Protection Agency, Proposed Text of Regulations (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (November 2024), available at: [https://coppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_ins\\_text.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf).

<sup>2</sup> News/Media Alliance February 2024 comments available at: <https://www.newsmediaalliance.org/news-media-alliance-submits-comment-on-california-privacy-protection-agency-proposed-rulemaking-on-automated-decisionmaking/>

<sup>3</sup> See California Privacy Protection Agency, Proposed Text (Express Terms), available at: [https://coppa.ca.gov/meetings/materials/20250306\\_07\\_item6\\_draft\\_text.pdf](https://coppa.ca.gov/meetings/materials/20250306_07_item6_draft_text.pdf).



relationship.”<sup>4</sup> The Agency proposes significant modifications to this definition which could expand the applicability and obligations of the data broker registration section to thousands of new businesses of all types, small and large. As such, the Agency’s proposed modification, and resulting expansion, plainly exceeds the Agency’s authority under the California Privacy Rights Act (“CPRA”) to amend regulations “to carry out the purposes and provisions of the California Consumer Privacy Act [(“CCPA”)].”<sup>5</sup>

The Agency’s proposed modification to the definition of “direct relationship” is inconsistent with the definitions in the Delete Act<sup>6</sup>, the Data Broker Registration Act<sup>7</sup>, and the legislative intent of the CCPA. In enacting these laws, which, respectively, establish a data broker registration and an accessible deletion mechanism, the Legislature did not expand the definition of “data broker” or define “direct relationship.” Nor did the Legislature empower the Agency to modify and significantly expand the data broker definitions, contained in both laws it seeks to regulate, to potentially capture thousands of new businesses not contemplated to be data brokers by any of these laws. On the contrary, while the Legislature notes that the Agency is vested with full administrative power to enforce the CCPA, it makes clear that “[e]xisting law defines various terms” for the purposes of effectuating data broker requirements and expressly states that the Delete Act “would incorporate the definitions from the CCPA.”<sup>8</sup>

As a result, the Agency is constrained by and legally prohibited from exceeding the definitions set forth in the laws that empower it, the CCPA and CPRA, and the laws that it seeks to regulate in this rulemaking, namely the Delete Act and the Data Broker Registration Act.

Since the Delete Act and the Data Broker Registration Act limit the definition of data broker to a business that “knowingly collects and sells to third parties the personal information of an individual with whom the business does not have a direct relationship,” the Agency cannot expand the definition of what a data broker is under these laws by attempting to broadly define “direct relationship” beyond the CCR’s current definition of “direct relationship,” which is consistent with the CCPA and Delete Act.

---

<sup>4</sup> See California Code of Regulations. Title 11, Division 6, Chapter 3, Article 2, Section 7601

<sup>5</sup> See California Civil Code Division 3. Part 4. Title 1.81.5. California Consumer Privacy Act of 2018. 1798.199.40.

<sup>6</sup> See California Senate Bill 362, as enrolled on 9/11/2023 and chaptered by Secretary of State on 10/10/2023, Chapter 709, Statutes of 2023.

<sup>7</sup> See California Assembly Bill 1202, as enrolled on 9/11/2023 and chaptered by Secretary of State on 10/11/2019, Chapter 753, Statutes of 2019.

<sup>8</sup> See *id.*



Like many California businesses, publishers use advertising to support their consumer offerings, and this includes augmentation and enhancement from third party sources. In the case of publishers, advertising subsidizes the production of high-quality journalism content and provides readers with more informative, tailored content and advertising. The proposed regulations could stifle long-appreciated and expected benefits for consumers.

As intended by the CCPA, consumers retain at all times the ability to directly opt out of such practices based on their direct relationship with publishers. In addition to providing consumers with vital access to high-quality journalism, personalized advertising is also vital to publishers because it helps keep much quality content free or at a low cost to access. The definition of “direct relationship” in the proposed text could restrict publishers’ ability to leverage common advertising practices that still support consumer opt-out. Alternatively, expanding the definition as proposed could result in costly operational and other obligations for news media and many other businesses operating in the advertising ecosystem, despite not being authorized or intended by the Legislature.

### **Conclusion**

Denying California consumers access to high-quality journalism is not the intent of the CCPA and is inconsistent with the law.<sup>9</sup> The Alliance respectfully requests that the Agency refrain from modifying the definition of “direct relationship” and instead maintain the current definition as it stands, consistent with Legislative intent.

The Alliance respectfully requests that the Agency strike the new language proposed in the definition of “direct relationship” in section 7601(d).

Sincerely,

Emily Emery  
Vice President, Government Affairs

---

<sup>9</sup> California Constitution Article I, Section 2: “A law may not restrain or abridge liberty of speech or press.”





**Grenda, Rianna@CPPA**

---

**From:** Anton Van Seventer <avanseventer@SIIA.net>  
**Sent:** Tuesday, June 10, 2025 9:23 AM  
**To:** Regulations@CPPA  
**Subject:** SIIA Accessible Delete Mechanism Comment  
**Attachments:** SIIA CPPA DROP System Requirements Comment.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

California Privacy Protection Agency,

Please see attached SIIA's comment regarding the CPPA's draft regulations around the DROP system requirements and the Delete Act. Thank you very much in advance for your consideration.

All the best,

**Anton van Seventer**

Counsel, Privacy and Data Policy

SIIA - Accelerating Innovation in Technology, Data & Media

PO Box 34340, Washington, DC 20043

[avanseventer@siia.net](mailto:avanseventer@siia.net)

Telephone: +1-202-789-4471

Mobile: [REDACTED]

LinkedIn: <https://www.linkedin.com/in/antonvanseventer>





## Comments of the Software & Information Industry Association

### California Privacy Protection Agency

#### Delete Request and Opt-out Platform ("DROP") System Requirements

*June 10, 2025*

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide comments on the California Privacy Protection Agency's (CPPA's) proposed delete request and opt-out platform (DROP) [requirements](#) for the [California Delete Act](#) (SB 362). SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include roughly 380 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide, and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value to individual autonomy and a functioning democracy. Data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of data privacy practices. We appreciate the goals of the proposed regulations, yet remain concerned about how the regulations exceed the bounds of the California Delete Act itself. Furthermore, some of the draft regulations would likely create significant unintended practical consequences. As such, we focus this submission on the scope of the "data broker" definition, and the inclusion of "inferences" within the scope of data subject to deletion.

#### **I. The revised definition of "direct relationship" is overbroad and goes beyond the statutory text of the Delete Act.**

The definition of "direct relationship" exceeds the statutory text and would also create widespread confusion and compliance difficulties for companies that find themselves within the proposed scope, even if they do not engage in data brokerage activity per any conventional understanding of their business.

First, the proposed DROP requirements cover a much broader group of companies than are required to register under the Delete Act. The California Delete Act only requires registration as a data broker by businesses that knowingly collect and sell the personal

information of a resident with whom it does not have a direct relationship.<sup>1</sup> Section 7601(d) of the proposed regulations, however, limits the scope of a direct relationship. To qualify for the exemption, not only must a business collect personal information directly from a consumer, but that consumer must “intend to interact with the business.” This expansion goes well beyond the plain language of the Delete Act, which specifically carves out the collection of data in the context of a direct relationship.

Second, expanding coverage to include data obtained through a consumer’s intentional interaction suffers from vagueness and overbreadth. It is rarely clear whether a consumer making an online purchase intends to, for example, interact with cookies, or reveal geolocation information. In fact, the same is often true of a variety of information collected from a consumer pursuant to that consumer’s interaction with a business. Because the proposed regulations turn the Delete Act’s clear bright line rule into what is effectively a case-by-case analysis, they muddy the waters by raising the unclear question of what is sufficient to constitute a consumer’s subjective intent. This, in turn, confuses the question of what operates as a direct relationship, which unmoors the scope of the Act.

Third, the proposed regulations create uncertainty by imposing regulations on organizations rather than on covered activity. It is unclear whether data would be exempt in the scenario that one line of business with which a consumer intended to interact collected that data, which was subsequently brokered by another line of that business. Many organizations have multiple lines of business. In one line of business, the organization could have a direct relationship with a consumer. In another line of business, it may be functioning as a data broker. The regulations, by regulating entities as data brokers rather than data brokerage itself, would place even the component of a business that does not engage in data brokerage within the scope of the draft regulations. This conflict could even exist in the context of the same dataset collected by different lines of a single California business.

## **II. Compelling data brokers to delete inferences based on information they have collected is not found in the Delete Act and risks constitutional infirmities.**

The draft regulations would require data brokers to delete not only third party data — and first party data collected in a third party capacity — but also “inferences” already derived from this data. While the draft regulations helpfully clarify that this does not include inferences collected in a first party capacity, they nevertheless still exceed the four corners of the Delete Act, which does not reference inferences that are themselves new datasets not collected from *any* consumer. In this way, the regulations would also run afoul of the First Amendment in

---

<sup>1</sup> See Cal. Civ. Code § 1798.105.



several circumstances, as was recognized during the drafting of the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

The Supreme Court has made clear that “the creation and dissemination of information is speech for First Amendment purposes.”<sup>2</sup> The State may not infringe these rights to protect a generalized interest in consumer privacy, as such restrictions burden both the businesses whose speech they restrict and the users of the information who are entitled to receive it.<sup>3</sup> For this reason, the CCPA included an exemption for certain kinds of publicly available information (PAI) made available from government records.

However, as was later recognized in the CPRA’s expanded PAI exemption, the constitutionally protected public domain consists not only of information released by the government, but that which is widely available in private hands – as well as opinions or inferences drawn from that information.<sup>4</sup> While legislators can prohibit the *use* of public domain information, regulating the publication of public domain information is therefore almost certainly unconstitutional. Such a requirement will have problems with vagueness, overbreadth, discriminating among speakers, and content – all of which are likely facial violations of the First Amendment.<sup>5</sup>

Here, the draft regulations would interpret the Delete Act to do just that. Section 7613(b)(1) would ostensibly grant consumers the power to delete inferences based on their personal information that were created – not collected from that consumer – and subsequently made publicly available by a data broker. Although the proposed regulations include a carveout for CCPA-exempt uses, this is insufficient. Instead, the proposed regulations would need to reference the CPRA’s PAI exemption to fully exempt such inferences, or, alternatively, walk back the coverage of inferences altogether.

\* \* \*

Thank you for considering our feedback to the proposed regulations. We are happy to discuss any of these comments in further detail. SIIA’s point of contact for this submission is Anton van Seventer, Counsel for Privacy and Data Policy ([avanseventer@siia.net](mailto:avanseventer@siia.net)).

---

<sup>2</sup> *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011).

<sup>3</sup> See generally E. Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1081 (2000); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969).

<sup>4</sup> See Cal. Civ. Code § 1798.100 et seq. (expanding the definition of publicly available information to “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.”).

<sup>5</sup> See *Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 828 (1995) (“In the realm of private speech or expression, government regulation may not favor one speaker over another.”).



**Grenda, Rianna@CPPA**

---

**From:** Tony Ficarrotta <tony@networkadvertising.org>  
**Sent:** Tuesday, June 10, 2025 2:54 PM  
**To:** Regulations@CPPA  
**Cc:** David LeDuc; Jason Snyder; Allen, Elizabeth@CPPA; Leigh Freund; Megan Cox  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** NAI Comments - Accessible Deletion Mechanism NPRM June 10 2025.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To the California Privacy Protection Agency,

The NAI is submitting comments in response to the Agency's Notice of Proposed Rulemaking of April 25, 2025 concerning the accessible deletion mechanism under the Delete Act. Please see the attached pdf for our comments. If you have any questions or would like to discuss further, please do not hesitate to reach out.

Thank you,  
-Tony Ficarrotta

--

**Tony Ficarrotta**

Vice President, General Counsel

**The NAI**

409 7th Street, NW, Suite 250, Washington, DC 20004

P: 719-210-4703 | [tony@thenai.org](mailto:tony@thenai.org)





409 7th Street NW, Suite 250  
Washington, DC 20004

June 10, 2025

*Submitted via electronic mail to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)*

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

**Re: Public Comment on Accessible Deletion Mechanism**

To the California Privacy Protection Agency:

On behalf of the Network Advertising Initiative (“NAI”),<sup>1</sup> thank you for the opportunity to comment on the proposed regulations regarding the Delete Request and Opt-out Platform (“DROP”) System Requirements (the “Proposed Regulations”).<sup>2</sup> The NAI appreciates both the continued commitment the California Privacy Protection Agency (the “Agency”) has shown to transparency and the opportunity to provide written comments throughout this rulemaking.

We offer the following comments and recommendations on the Proposed Regulations, which we hope will assist the Agency in meeting its consumer privacy objectives for the rulemaking while preserving a free, open, and secure internet for all California consumers.

---

<sup>1</sup> The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. The NAI has been a leader in this space since its inception in 2000, promoting the highest voluntary industry standards for member companies, which range from small startups to some of the largest companies in digital advertising. The NAI’s members are providers of advertising technology solutions, and include ad exchanges, demand- and supply-side platforms, as well as other companies that power the digital media industry. Our member companies help digital publishers generate essential ad revenue, advertisers reach audiences interested in their products and services, and ensure consumers are provided with ads relevant to their interests. Earlier this year, the NAI launched its new Self-Regulatory Framework Program (the “NAI Framework”) to promote strong privacy practices for NAI members engaged in behavioral advertising. See *NAI Self-Regulatory Framework*, <https://thenai.org/self-regulatory-framework/>.

<sup>2</sup> Cal. Code Regs. tit. 11, §§ 7601 et seq. (proposed) (hereinafter “Proposed Regulations”), [https://coppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_text.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_text.pdf).

In Section I, we offer comments on how the Agency can update several definitions in the Proposed Regulations to promote uniform interpretation and avoid ambiguity, including by adding a definition for the term “matched identifier.”

In Section II, we offer comments on how the Agency can update the Proposed Regulations on DROP requirements to ease implementation and manage associated costs for data brokers while remaining consistent with the Agency’s goals for the rulemaking. This includes comments on standards for account liability, retrieval of consumer deletion lists, payment of fees, and status reporting for deletion requests.

In Section III, we offer comments on how the Agency can update the Proposed Regulations on consumer and authorized agent delete requests to ensure that consumers submitting personal information through the DROP are properly verified; as well as to promote consumer privacy by obtaining consumer consent before sending personal information to data brokers and by more explicitly limiting what personal information an authorized agent can submit through the DROP.

These comments are set forth in more detail below.

## **I. Definitions**

### **A. The Proposed Regulations should adopt a definition of “matched identifier”.**

The Proposed Regulations use the term “matched identifier” in several places, including as part of the definition of “personal information associated with a matched identifier.”<sup>3</sup> However, the Proposed Regulations do not define that term. To facilitate consistent business compliance with consumer deletion requests submitted through the DROP,<sup>4</sup> the Agency should add a definition of “matched identifier” to the Proposed Regulations.

The key elements of this definition should not only address the intended use of matched identifiers – *i.e.*, to match the identity of consumers who submit requests through the DROP with individuals about whom a business holds personal information; but should also address the specific types of personal information that consumers may submit

---

<sup>3</sup> The term “matched identifier” is used as part of the definition of “personal information associated with a matched identifier.” See Proposed Regulations § 7601(i). Additionally, the term “matched identifier” is used throughout the Proposed Regulations in isolation, further suggesting the need for a standalone definition of the term. See *id.* §§ 7613(a)(2)(B); 7613(b)(1); 7614(b)(2)(A).

<sup>4</sup> *Id.* § 7601(e).



through the DROP to effectuate deletion requests. For example, if the Agency intends to enable consumers to submit only specific types of identifiers through their DROP accounts (e.g. email address, phone number, mobile advertising identifier, etc.) then a definition of “matched identifier” should specify and clarify that fact. Further, adding this clarity to the definition would not limit the scope of the already defined term “personal information associated with a matched identifier” because all other types of personal information that a business associates with a “matched identifier” would continue to be captured by that broader definition for purposes of effectuating consumer deletion requests (e.g., non-standard identifiers such as internal or proprietary identifiers; inferences; consumer profiles; etc.).

By adopting a definition of “matched identifier,” the Agency would have an opportunity to further clarify the meaning of other defined terms, especially “consumer deletion list”<sup>5</sup> and “personal information associated with a matched identifier.”<sup>6</sup> First, by defining “matched identifier” partly in reference to “consumer deletion list,” the Agency can clarify the relationship between the consumer deletion lists maintained by the Agency in the DROP and the matching process a data broker is expected to undergo in effectuating consumer deletion requests submitted through the DROP. Second, by updating the definition of “personal information associated with a matched identifier” in reference to a newly defined term “matched identifier,” the Agency can further clarify what personal information a data broker must delete after it has determined it holds a “matched identifier,” which is one of the Agency’s stated objectives for this part of the Proposed Regulations.<sup>7</sup>

The NAI recommends the following definition of “matched identifier,” which the Agency could build on by appending additional types of identifiers it intends to enable consumers to submit through the DROP and maintain in the consumer deletion list, as follows:

*“Matched identifier” means personal information controlled by a data broker that, alone or in combination, the data broker uses to uniquely identify a consumer and that matches one or more of the following types of identifiers obtained by the data broker from a consumer deletion list: email address; phone number; combination of name, date of birth, and zip code; [mobile advertising ID]; [additional specified types of identifiers].*

---

<sup>5</sup> Proposed Regulations § 7601(c).

<sup>6</sup> *Id.* § 7601(i).

<sup>7</sup> See California Privacy Protection Agency, Initial Statement of Reasons, Accessible Deletion Mechanism (hereinafter “ISOR”) at 5, [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_isor.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_isor.pdf).

**B. The Proposed Regulations should update the definition of “personal information associated with a matched identifier” to clarify the scope of information data brokers must delete in response to a deletion request received from the DROP.**

The Proposed Regulations seek to specify what information a data broker must delete in response to a consumer deletion request submitted through the DROP by adding the following definition of “personal information associated with a matched identifier”<sup>8</sup>:

*[A]ny personal information maintained in a data broker’s records collected from a source other than directly from the consumer through a “first party” interaction. This does not include personal information that is subject to applicable exemptions, but includes inferences made from the personal information.*

The Agency should further clarify the scope of information covered by the proposed definition by taking two steps.

First, the Agency should adopt a definition of “matched identifier” as discussed above<sup>9</sup> and use the newly defined term “matched identifier” in the definition of “personal information associated with a matched identifier.” The NAI’s recommended language is set out below.

Second, the Agency should further clarify which inferences are covered by the definition. The Proposed Regulations specify that certain inferences are personal information that data brokers must delete in response to a consumer deletion request submitted through the DROP.<sup>10</sup> But which inferences are covered is potentially ambiguous, and appear to admit of both a narrower and broader reading.

The scope of covered inferences could be read more narrowly to mean inferences made **only** from the personal information maintained in a data broker’s records collected from a source other than directly from the consumer through a “first party” interaction. However, it could also be read more broadly to mean all inferences about a consumer drawn from personal information maintained in a data broker’s records, regardless of whether the data broker collected the underlying personal information supporting those

---

<sup>8</sup> Proposed Regulations § 7601(i). The Proposed Regulations also specify that a data broker must delete “all personal information associated with a matched identifier” in response to a consumer request submitted through the DROP. See *id.* § 7613(a)(2).

<sup>9</sup> See *supra* Section I.A.

<sup>10</sup> See Proposed Regulations § 7601(i) (referring to “inferences made from the personal information.”).

inferences directly from the consumer in a “first party” context or not. This potential scoping ambiguity also raises a question about whether an inference made about a consumer by a business is ever personal information collected directly from the consumer.

The Proposed Regulations could address these issues by updating the definition of “personal information associated with a matched identifier” to either the narrower or broader meaning, depending on the Agency’s intent. In both cases, the Agency should include the term “matched identifier” in the definition, as discussed above.

Proposed update for a narrower reading:

*[A]ny personal information associated with a “matched identifier” maintained in a data broker’s records collected from a source other than directly from the consumer through a “first party” interaction, including inferences drawn from such personal information. This does not include personal information that is subject to applicable exemptions, ~~but includes inferences made from the personal information~~.*

Proposed update for a broader reading:

*[A]ny personal information associated with a “matched identifier” maintained in a data broker’s records collected from a source other than directly from the consumer through a “first party” interaction. This does not include personal information that is subject to applicable exemptions, but includes any inferences made from ~~the~~ personal information about the consumer, regardless of the source of such personal information.*

By adopting one of these recommended updates, the Agency can promote consistent interpretation of the definition among data brokers as to what information they must delete in response to a consumer’s deletion request submitted through the DROP.

## **II. DROP Requirements**

- A. The Agency should limit data broker liability for DROP account activity to instances of negligent failure to comply with security measures because strict liability is overly burdensome.**

Businesses have an important responsibility to implement and maintain reasonable security measures to safeguard systems and consumer personal information under their control. However, the Proposed Regulations should not hold businesses strictly liable for security breaches, regardless of fault. Currently, the Proposed Regulations state that a

“data broker is responsible for all actions taken through its DROP account,”<sup>11</sup> but this blanket requirement does not take into account whether the broker has followed all required security practices set out in the Proposed Regulations. This imposes a strict liability standard even though the Proposed Regulations also mandate detailed security measures for DROP accounts, including credential confidentiality, access restrictions, and breach notification requirements.<sup>12</sup> These measures, which the NAI supports, are designed to prevent unauthorized activity and represent a reasonable and appropriate standard of diligence for DROP account security.

The Proposed Regulations as currently written would impose liability even in circumstances where a malicious actor gains access to a data broker’s DROP account by compromising the Agency’s systems, and through no fault of the business whatsoever. The NAI therefore respectfully recommends that the Agency adopt a negligence standard that holds data brokers liable only when they negligently fail to implement or comply with the security requirements as described in the Proposed Regulations. This approach would maintain meaningful accountability for deficient security practices while avoiding unfair penalties where reasonable precautions have been taken. For these reasons, the NAI recommends that the Agency revise Section 7610 (a)(1)(D) of the Proposed Regulations as follows:

*A data broker is responsible for all actions taken through its DROP account, except that a data broker shall not be liable for unauthorized actions taken through its DROP account unless such actions result from the data broker’s negligent failure to implement or maintain reasonable security procedures and practices as required by this Section.*

**B. The Agency should not require a data broker to retrieve a “consumer deletion list” if the data broker does not maintain any of the relevant identifiers and where such retrieval would not produce any “matched identifiers.”**

The Proposed Regulations require data brokers to select “at least one consumer deletion list that the data broker will retrieve through the DROP” for purposes of effectuating consumer deletion requests submitted through the DROP.<sup>13</sup> However, this requirement as written appears to apply even in cases where a data broker does not maintain any of the identifiers represented in the consumer deletion list, such as “email address, phone

---

<sup>11</sup> Proposed Regulations § 7610(a)(1)(D).

<sup>12</sup> See *id.* §§ 7610(1)(a)-(c); 7616(b).

<sup>13</sup> *Id.* § 7610(a)(3).

number, or combination of name, date of birth, and zip code.”<sup>14</sup> Some data brokers operate entirely using identifiers – such as proprietary cookie IDs – that do not appear to be under consideration for inclusion on a consumer deletion list. For such data brokers, the requirement to retrieve a list goes against best practices for data minimization by requiring them to access, store, and report on data that they otherwise would not possess and which they cannot match to any of their own records.

Furthermore, when read together with the requirement in the Proposed Regulations that a data broker must save and maintain consumer personal information retrieved through the DROP,<sup>15</sup> the “at least one” requirement would obligate these businesses to store large volumes of identifiers that they have no ability to use, for an indefinite period. This result would undermine the data minimization principles the Agency otherwise seeks to uphold in the design of the DROP,<sup>16</sup> while offering no benefit to consumers.

Moreover, if a data broker later begins processing a new category of personal information that matches a type of identifier included in a consumer deletion list, the Proposed Regulations already require the data broker to update its list selection accordingly.<sup>17</sup> That safeguard ensures consumers are covered in cases where a data broker begins collecting a type of identifier on a consumer deletion list, without requiring the data broker to preemptively retrieve irrelevant lists in advance. The existing framework thus already ensures coverage for consumers without the overbroad “at least one” requirement in the Proposed Regulations.

For that reason, the NAI recommends the Agency amend section 7610(a) to eliminate the “at least one” requirement and clarify that data brokers are only required to retrieve consumer deletion lists containing identifiers that match categories of personal information they actually maintain. The NAI proposes the following revision:

*(a) Prior to accessing the DROP for the first time, a data broker shall utilize the Agency’s website found at [www.cppa.ca.gov](http://www.cppa.ca.gov) to create a DROP account. To create an account, a data broker must:*

...

---

<sup>14</sup> *Id.* § 7601(c).

<sup>15</sup> *Id.* § 7613(c).

<sup>16</sup> The Delete Act directs the Agency to design the DROP in a way that allows consumers to submit requests in “privacy-protecting” ways. See Cal. Civ. Code § 1798.99.86(b)(2).

<sup>17</sup> See Proposed Regulations § 7610(a)(3)(C) (“A data broker must maintain compliance with subparagraph (A) of this section at all times by selecting additional consumer deletion lists before next accessing the DROP if the data broker begins collecting additional categories of personal information about consumers that match to identifiers under previously unselected consumer deletion lists.”).

(3) Select ~~at least one~~ the consumer deletion list(s) that the data broker will retrieve through the DROP to process deletion requests in accordance with Civil Code section 1798.99.86 and this Chapter.

(A) A data broker must select all consumer deletion lists that contain a consumer identifier or identifiers that match to personal information about the consumer within the data broker's records.

(B) Notwithstanding subparagraph (A), a data broker may select fewer lists if the consumer identifiers used across multiple lists will result in matches to a completely duplicative list of consumers within the data broker's records. For example, if a data broker collects both email addresses and telephone numbers for every consumer in its records, then the data broker may select only the email address or telephone number consumer deletion list. If a data broker collects email addresses for some consumers and telephone numbers for other consumers, however, then the data broker must select both lists. If a data broker does not maintain any personal information corresponding to the identifiers in a consumer deletion list, it is not required to retrieve the list.

This revision would better support the principles of data minimization and a more privacy-protective design for the DROP because it would not require data brokers to access and store consumer personal information they cannot use to effectuate consumer requests to delete. Further, it will not excuse data brokers from accessing relevant consumer deletion lists because the Proposed Regulations would still require data brokers to access those lists as soon as they begin associating consumer personal information with a type of identifier covered by a consumer deletion list.<sup>18</sup>

### **C. The Agency should clearly delineate fee requirements for DROP registration and access.**

Data brokers are required to pay an annual registration fee under the Delete Act, which is currently set at \$6,600.<sup>19</sup> The current registration fee of \$6,600 is an order of magnitude higher than registration fees in prior years,<sup>20</sup> and the Agency has indicated that the purpose of the increase in the 2025 registration fees is to fund development and operation of the DROP.

---

<sup>18</sup> See Proposed Regulations § 7610(a)(3)(C).

<sup>19</sup> Cal. Code Regs. tit. 11 § 7600.

<sup>20</sup> See, e.g., California Privacy Protection Agency, Draft Data Broker Registration Regulations (2024) (showing initial data broker registration fees set at \$400), [https://cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_prop\\_text.pdf](https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf).



The Proposed Regulations, however, also refer to a requirement that data brokers pay a “first-time access fee” for DROP participation, starting at \$6,600 and decreasing each month thereafter depending on when access begins on a pro-rated basis.<sup>21</sup> As currently drafted, separate references to a \$6,600 registration fee and a \$6,600 first-time access fee creates confusion and raises questions about whether the Agency expects data brokers to pay a single registration that would cover the first-time access fee as well; or separate fees totaling \$13,200 (\$6,600 for registration plus a \$6,600 first-time access fee).

For that reason, the Agency should revise Section 7611 to add a new subsection (d) explicitly stating that data brokers who pay the annual registration fee are not required to pay an additional first-time access fee for the DROP. The NAI proposes the following amendment:

*(d) A data broker that has paid the annual registration fee pursuant to section 7600 of this Chapter shall not be required to pay an additional first-time access fee under this section during the same calendar year.*

This clarification would promote transparency, prevent redundant charges, and ensure that the fee structure supports full and timely participation in the DROP.

**D. The Agency should replace the proposed status reporting structure with a simplified structure that still enables consumers to verify the status of a request.**

The Delete Act sets out numerous design requirements for the DROP,<sup>22</sup> including a requirement that the DROP “shall allow the consumer . . . to verify the status of the consumer’s deletion request” submitted through the DROP.<sup>23</sup> Under the Proposed Regulations, the Agency is interpreting this requirement to require data brokers to regularly report on the status of each deletion request they receive through the DROP using four separate types of structured, codified responses.<sup>24</sup>

Specifically, the Proposed Regulations would require status reporting for each access session following the initial access to the DROP platform, and would require data brokers

---

<sup>21</sup> Proposed Regulations § 7611(a)(3).

<sup>22</sup> See Cal. Civ. Code § 1798.99.86(a).

<sup>23</sup> *Id.* § 1798.99.86(a)(9).

<sup>24</sup> Proposed Regulations § 7614.

to link each individual deletion request to a specific “transaction identifier” provided by the agency, as well as one of four primary status “response codes.”<sup>25</sup>

This detailed scheme for status reporting will impose significant engineering and operational costs on businesses by pushing them to automate classification of and responses to every deletion request that arrives through the DROP. It imposes a set of requirements beyond complying with consumer requests and would result in new workflows to return information to the DROP in a complex and structured format.

The Delete Act’s requirement that the DROP should allow the consumer to verify the status of their request does not dictate this type of scheme. Instead, the Agency should take a simplified approach to this Delete Act requirement that will reduce costs for the Agency in development and implementation of the DROP as well as businesses integrating with the DROP. A simplified approach would only require the Agency to report to consumers through their DROP accounts whether their request is “pending” or “received” for each data broker with whom the consumer has requested deletion.

This approach provides a key point of transparency to consumers about the status of their deletion requests – as required by the Delete Act – without imposing an unnecessarily complex scheme that will drive up costs for the Agency and businesses. To follow a simplified approach, the NAI recommends that the Agency remove the text of Proposed Regulation 7614 in its entirety and replace it with the following:

*After a consumer submits a deletion request through the DROP to a data broker, the Agency shall cause the DROP to show the status of that consumer’s request to the data broker as “pending” until the data broker accesses the DROP to retrieve the consumer’s deletion request. After the data broker retrieves the consumer’s deletion request through the DROP, the Agency shall cause the DROP to show the status of that consumer’s request as “sent.”*

### **III. Consumer and Authorized Agent Delete Requests**

#### **A. The Agency should ensure that it will establish consumer residency in California before allowing a consumer to use the DROP.**

Because the CCPA and the Delete Act grant deletion and opt-out rights only to California residents, the Proposed Regulations include provisions intended to limit consumer access

---

<sup>25</sup> The four response codes are “record deleted,” “record opted out of sale,” “record exempted,” and “record not found.” *Id.* § 7614(b).

to the DROP to California residents only.<sup>26</sup> Specifically, the Proposed Regulations state that:

*Consumers may be required to have their California residency verified by the Agency prior to submitting a deletion request [through the DROP]. If the Agency cannot verify the consumer's residency, the consumer cannot submit a deletion request through the DROP.*<sup>27</sup>

In order to ensure that only California residents submit requests through the DROP, the Proposed Regulations should make it clear that consumers will always be required to verify their California residency with the Agency prior to submitting a request through the DROP. Clarifying this will help ensure that the resource burden for operating the DROP borne by California residents and registered data brokers results in benefits to California residents, not residents of other states. In addition, it will help ensure that data brokers receiving consumer requests through the DROP have no reason to contact consumers submitting requests in order to verify their status as California residents.

The NAI supports the Agency's position that data brokers should not need to contact consumers in order to verify their residency.<sup>28</sup> The NAI submitted extensive comments in support of that position in response to the Agency's invitation for preliminary comments on the rulemaking under the Delete Act in 2024.<sup>29</sup> However, if the Agency does not commit itself to verifying the California residency of all consumers before they submit requests through the DROP, data brokers may be unsure if a particular deletion request received through the DROP actually originated from a resident of California or a resident of a different state. This would create a reason for data brokers to seek confirmation of California residency and other elements of verification directly from consumers – a requirement the CCPA appears to identify as underpinning all verifiable consumer

---

<sup>26</sup> See ISOR at 19 (stating that a consumer “may be required to have their residence verified by the Agency before submitting a deletion request through the DROP,” and that this is necessary “because the deletion request rights only extend to California consumers.”).

<sup>27</sup> Proposed Regulations § 7620(a).

<sup>28</sup> See *id.* § 7616(c). (proposed). (“A data broker shall not contact consumers to verify its deletion requests submitted through the DROP.”).

<sup>29</sup> See generally Network Advertising Initiative, Preliminary Comments to the California Privacy Protection Agency Regarding SB 362 Proposed Rulemaking (June 25, 2024), <https://thenai.org/wp-content/uploads/2024/06/NAI-Preliminary-Comments-SB362-Proposed-Rulemaking-June-25-2024-copy.pdf>.

requests, including deletion requests.<sup>30</sup> To avoid this tension, the Agency should update Proposed Regulation 7620(a) as follows:

*The Agency shall require ~~Consumers~~ ~~may be required~~ to ~~have their~~ verify their California residency ~~verified by the Agency~~ prior to submitting a deletion request. If the Agency cannot verify the consumer's residency, the consumer cannot submit a deletion request through the DROP.*

**B. The Agency should establish clear standards for how it will verify consumer identifiers before a consumer submits those identifiers for matching through the DROP.**

To ensure that the DROP system operates as intended, it is essential that data brokers acting on requests have no reason to contact consumers to further verify the requests or authenticate the identifiers that consumers provide for purposes of matching through the DROP. This is the case both for a consumer's California residency, as discussed above,<sup>31</sup> as well as for specific identifiers that consumers submit through the DROP. The NAI commented extensively on this issue in response to the Agency's invitation for preliminary comments on Delete Act rulemaking.<sup>32</sup> To help ensure that data brokers will not have reason to contact consumers for purposes of verifying their requests, the Agency should commit itself to properly verifying and authenticating identifiers it allows consumers to submit through the DROP. To do so, the Agency should amend section 7620(b)<sup>33</sup> of the Proposed Regulations as follows:

*Consumers may add personal information to their deletion requests, including date of birth, email address, phone number, and pseudonymous identifiers, such as a Mobile Ad Identifier (MAID). The Agency ~~may~~ shall use reasonable methods to verify that consumers have ownership and control of any such personal information before consumers add the information to their deletion request, and may further verify such information at any time.*

---

<sup>30</sup> See Cal. Civ. Code § 1798.140(ak) ("A business is not obligated to . . . to delete personal information . . . if the *business* cannot verify . . . that the consumer making the request is the consumer about whom the business has collected information[.](emphasis added)."). It is not clear how Proposed Regulations § 7616(c) aligns with this aspect of the CCPA.

<sup>31</sup> See *supra* Section III.A.

<sup>32</sup> See generally Network Advertising Initiative, Preliminary Comments to the California Privacy Protection Agency Regarding SB 362 Proposed Rulemaking (June 25, 2024), <https://thenai.org/wp-content/uploads/2024/06/NAI-Preliminary-Comments-SB362-Proposed-Rulemaking-June-25-2024-copy.pdf>.

<sup>33</sup> Proposed Regulations § 7620(b).

Reasonable methods to confirm control over email addresses, phone numbers, and other identifiers may include requirements for consumers to access confirmation links or use confirmation codes sent by the Agency to email addresses and/or phone numbers. Because the Proposed Regulations also purport to disallow brokers from contacting consumers to actually verify the request,<sup>34</sup> it is essential that the Agency undertake confirmation of consumer control over identifiers they submit through the DROP.

**C. The Agency should obtain consumer consent to disclose personal information for deletion requests through the DROP.**

The Proposed Regulations posit that by virtue submitting a deletion request through the DROP, consumers “consent to disclosure of their personal information to data brokers for purposes of processing their deletion request[.]”<sup>35</sup> However, if the Agency’s position is that consent is the appropriate standard governing consumer permission to submit information to data brokers through the DROP, the Agency should commit itself to obtaining consent from consumers before submitting their personal information to data brokers. Without clearly committing itself to this standard, the Agency would create confusion about whether the term “consent” under the Delete Act and its implementing regulations creates a lower standard than is set out by the CCPA<sup>36</sup> that can be met merely by a consumer submitting information. The NAI recommends the following changes to Proposed Regulation 7620(c) to address this issue:

*~~Before~~ ~~By~~ submitting a consumer’s personal information to data brokers to effectuate the consumer’s a deletion request, the Agency shall obtain the consumer’s consent to ~~disclosure of~~ disclose their personal information to data brokers for purposes of processing their deletion request pursuant to Civil Code section 1798 and this Chapter ~~unless or until the consumer cancels their deletion request.~~*

**D. The Agency should update the authorized agent provisions in the Proposed Regulations to be privacy-protective.**

The Delete Act and the Proposed Regulations contemplate authorized agents using the DROP to aid in submitting consumer requests to delete.<sup>37</sup> However, authorized agents have been known to submit excessive personal information to businesses when seeking to exercise privacy rights on behalf of those consumers in a way that does not promote

---

<sup>34</sup> See Proposed Regulations § 7616(c).

<sup>35</sup> *Id.* § 7620(c).

<sup>36</sup> See Cal. Civ. Code § 1798.140(h) (defining “consent”).

<sup>37</sup> See *id.* § 1798.99.86(b)(8); Proposed Regulations § 7621.

consumer privacy.<sup>38</sup> The Agency appears to be attuned to this concern when it states in the Initial Statement of Reasons accompanying the Proposed Regulations that the Proposed Regulations will “protect consumer privacy by limiting the information provided by authorized agents assisting consumers with delete requests [.]”<sup>39</sup>

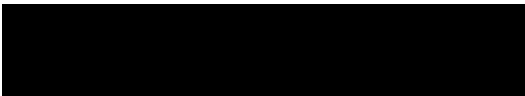
However, the Proposed Regulations at this stage appear to be silent on the issue of what information an authorized agent may or may not provide when assisting consumers with delete requests through the DROP. For example, the section of the Proposed Regulations dedicated to authorized agents does not refer to any limitations on the information an authorized agent may provide through the DROP.<sup>40</sup>

The NAI recommends that the Agency revisit this issue and propose language on how it will limit the information provided by authorized agents assisting consumers with delete requests, as contemplated by the Initial Statement of Reasons.

#### **IV. Conclusion**

The NAI appreciates the opportunity to submit comments to the Agency on the proposed accessible deletion mechanism regulations. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at [tony@networkadvertising.org](mailto:tony@networkadvertising.org), or David LeDuc, Vice President, Public Policy, at [david@networkadvertising.org](mailto:david@networkadvertising.org).

Respectfully submitted,

A black rectangular box redacting the signature of Tony Ficarrotta.

Tony Ficarrotta  
Vice President, General Counsel  
Network Advertising Initiative (NAI)

---

<sup>38</sup> See generally Tony Ficarrotta, Some Authorized Agent Providers Are Selling Privacy Snake Oil and Why It Needs to Stop, IAPP: News (Feb. 13, 2025), <https://iapp.org/news/a/some-authorized-agent-providers-are-selling-privacy-snake-oil-and-why-it-needs-to-stop> (last visited June 10, 2025).

<sup>39</sup> See ISOR at 2.

<sup>40</sup> See Proposed Regulations § 7621(a)-(c).



**Grenda, Rianna@CPPA**

---

**From:** Viar, Kate <Kate.Viar@transunion.com>  
**Sent:** Tuesday, June 10, 2025 3:41 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** TransUnion CPPA DROP Comments.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Attached please find TransUnion's comments in response to the agency's proposed regulations addressing the Accessible Deletion Mechanism. Thank you!

Best regards,  
Kate

**Kate Viar**  
State Government Relations  
kate.viar@transunion.com  
M: [REDACTED]

**TransUnion**

*This email including, without limitation, the attachments, if any, accompanying this email, may contain information which is confidential or privileged and exempt from disclosure under applicable law. The information is for the use of the intended recipient. If you are not the intended recipient, be aware that any disclosure, copying, distribution, review or use of the contents of this email, and/or its attachments, is without authorization and is prohibited. If you have received this email in error, please notify us by reply email immediately and destroy all copies of this email and its attachments.*



June 10, 2025

California Privacy Protection Agency  
400 R Street, Suite 350  
Sacramento, CA 95811

RE: Public Comment on Accessible Deletion Mechanism Rulemaking

Dear Director Kemp:

Trans Union LLC ("TransUnion") appreciates the opportunity to provide comments in response to the California Privacy Protection Agency's ("CPPA") proposed regulations regarding the Accessible Delete Mechanism – Delete Request and Opt-Out Platform ("DROP") System Requirements. We support the CPPA's objectives of promoting consumer privacy, enhancing transparency, and enabling consumers to manage their personal information. We share the CPPA's commitment to using data responsibly and in ways that serve the public good.

As a global information and insights company, TransUnion recognizes the vital role that data plays in today's economy and the accompanying responsibilities for stewarding consumer information. Responsible data governance and a strong commitment to privacy are at the heart of our mission to use "Information for Good." We maintain global information security and privacy programs that meet or exceed regulatory requirements and consumer expectations.

We commend the CPPA's leadership in developing privacy standards that support innovation while protecting consumers. At the same time, we respectfully offer the following comments and recommendations to address areas in the proposed DROP regulations that raise concerns around scope, practicality, consumer experience, security, and consistency with existing law.

### **1. Redundant Subsidiary Registration Requirements Undermine Efficiency and Consumer Clarity**

The proposed regulation requires each business entity qualifying as a data broker—including subsidiaries under a single corporate structure—to create and manage its own DROP account. For a company like TransUnion, this would entail registering multiple

---

separate entities, even though we operate a centralized privacy request system with a single consumer interface that fulfills a consumer's single privacy request across all TransUnion entities.

We are concerned that the existing proposal would result in 1) confusing consumers by presenting multiple, seemingly separate entry points for the same company; 2) fragmenting and complicating request processing unnecessarily; and 3) creating duplicative administrative and technical burdens.

We respectfully request that the CPPA permit a single, parent-level registration for business groups operating under a unified privacy program, provided that the parent entity is responsible for ensuring that all consumer requests are routed and processed across relevant subsidiaries.

We acknowledge that each TransUnion entity classified as a data broker would still be individually registered and subject to the appropriate registration fee.

## **2. Overly Prescriptive Data Standardization Requirements May Reduce Accuracy**

The proposed standardization requirements mandate removal of special characters from consumer-provided information, which may undermine data accuracy, rather than improve it. For example, "1 ½ Main Street" could be misread as "112 Main Street" if the slash were to be stripped. A unit number like "123 #3 Main Street" would lose key address details if the hash symbol were removed, and it becomes "1233 Main Street."

Email addresses—containing hyphens, underscores, periods, and the "@" symbol—could become unrecognizable or unmatched, impeding the ability to fulfill a consumer's deletion request.

Standardizing data at this level could also expose data systems to new security risks by forcing uniform processing patterns that attackers may exploit.

We recommend that the CPPA provide guidelines rather than rigid formatting rules and allow data brokers to apply data matching standards that are demonstrably effective in ensuring accurate matches.

## **3. Inflexible Data Matching Thresholds May Lead to Inaccurate Deletions**

The proposed rule would require data brokers to action a deletion request if more than 50% of the unique identifiers match a consumer record. This approach creates the risk of false positive deletions—deleting data for the wrong person—which may interfere with a

---

consumer's ability to access services or verify identity. Overmatching may violate consumer rights just as undermatching may.

TransUnion typically achieves a match rate that is higher than 50% by employing robust matching logic, which has been developed over decades and generally relies on multiple high-precision data points (e.g., name, address, SSN, date of birth). Our systems are designed to maximize accuracy and reduce both false positives and false negatives, thereby effectuating consumer privacy requests to the highest degree possible.

We strongly recommend that data brokers be permitted to use their existing, validated matching systems. The CPPA should consider sandbox testing to evaluate the efficacy of existing matching systems before enforcing rigid thresholds. Furthermore, requiring parallel systems may increase error rates, reduce reliability, and create potential conflicts.

#### **4. Consumer Residency and Information Verification Provisions Require Clarification**

The proposed rule states that “a data broker shall not contact consumers to verify their deletion requests submitted through the DROP” and that the CPPA *may* verify that consumers submitting DROP requests are California residents. We suggest this be amended to *require* such verification.

The proposed regulation also states that CPPA *may* verify personal information such as “date of birth, email address, phone number, and pseudonymous identifiers, such as a Mobile Ad Identifier (MAID)... at any time.” We suggest that the regulations be amended to *require* that the CPPA verify any additional personal information provided by, or on behalf of, the consumer.

Furthermore, if a data broker has compelling data suggesting a requestor is not a California resident, there should be a clear, documented process to reconcile this discrepancy with the CPPA before being required to act on the request.

We also encourage the CPPA to establish a mechanism for identifying and blocking misuse or fraud, and to provide a safe harbor from liability for data brokers acting in good faith on deletion requests later found to be unauthorized.

#### **5. Lack of Verification Standards for Agents Invites Abuse**

The proposed DROP system lacks sufficient safeguards to verify authorized agents acting on behalf of consumers. Without clear requirements, the system is vulnerable to abuse,

---

particularly when agents submit bulk deletion requests without direct consumer interaction.

Current CCPA regulations (11 CCR § 999.326) allow businesses to require a consumer to 1) provide signed permission to an agent; and 2) verify their identity or confirm agent authorization directly with the business.

By omitting these protections in the DROP framework, the proposed rule opens a compliance loophole and raises questions about the integrity of deletion requests. TransUnion believes it prudent that the CPPA validate agent identity and authorization to submit a request on behalf of each consumer prior to requiring a data broker to effectuate a privacy request. If the CPPA fails to properly verify an agent's identity or the individual consumer request, the CPPA should provide a safe harbor for data brokers facing liability resulting from unauthorized deletions.

## **6. Compliance with NIST Identity Assurance Standards is Critical**

With respect to both consumers and authorized agents, TransUnion is subject to federal obligations that require adherence to identity assurance standards before processing deletion requests. In order to interact with and act upon data from the DROP system, we require an attestation from the CPPA that the DROP meets minimum security standards contained in NIST 800-63-3 for Identity Assurance Level (IAL) 2 for any entity submitting requests. The regulations need to reflect these requirements and contemplate a process for attestation.

## **7. Proposed Timeline for Implementation is Unreasonably Short**

The proposed compliance timeline does not allow sufficient time for data brokers to assess technical impacts, build or reconfigure internal systems, train personnel, and test and validate integrations with the DROP system.

We respectfully recommend that the CPPA adopt an implementation window of at least 18 months from the date the DROP platform is fully operational and documented. Rushed implementation may lead to compliance errors or consumer harm.

In addition, TransUnion recommends that the CPPA allow time for thorough security testing—including penetration testing and “red teaming”—to ensure system integrity before launch.

---

TransUnion appreciates the CPPA's work to strengthen privacy protections for Californians. We are committed to these goals and would welcome the opportunity to participate in technical workshops, sandbox evaluations, or advisory groups to ensure the DROP system functions securely, efficiently, and equitably for all stakeholders.

Thank you for your consideration.

Sincerely,

A black rectangular redaction box covering the signature of Kate Viar.

Kate Viar  
Senior Director of Government Relations



## Grenda, Rianna@CPPA

---

**From:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Sent:** Tuesday, June 10, 2025 7:55 AM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** wyden-letter-to-cppa-drop.pdf

### This Message Is From an External Sender

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Dear CPPA,

Please see the attached comment from U.S. Senator Ron Wyden.

Thanks,

Chris Soghoian  
Senior Policy Advisor for Privacy & Cybersecurity  
Office of U.S. Senator Ron Wyden

RON WYDEN  
OREGON

CHAIRMAN OF COMMITTEE ON  
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING  
WASHINGTON, DC 20510  
(202) 224-5244

United States Senate  
WASHINGTON, DC 20510-3703

**COMMITTEES:**

COMMITTEE ON FINANCE  
COMMITTEE ON THE BUDGET  
COMMITTEE ON ENERGY AND NATURAL RESOURCES  
SELECT COMMITTEE ON INTELLIGENCE  
JOINT COMMITTEE ON TAXATION

June 10, 2025

Jennifer M. Urban  
Chair  
California Privacy Protection Agency Board  
400 R Street, Suite 350  
Sacramento, CA 95811

Dear Chair Urban:

I write to commend California's Privacy Protection Agency (CPPA) for its forthcoming launch of the first universal data broker deletion tool, which will provide Californians a streamlined way to remove their personal information from the hands of shady data brokers. In the future, I suggest the Agency take additional steps to make this tool a more powerful and effective measure to secure the information of U.S. government employees and others whose data is most likely to be targeted by foreign adversaries or criminals.

California deserves significant praise for enacting the Delete Act to provide its residents with an easy-to-use, universal deletion request for data brokers selling their personal information. The status quo — in which Americans have to contact hundreds of individual data brokers, each of which has its own unique deletion request process — places an unreasonable administrative burden on those who wish to protect their privacy, and consequently, very few Americans successfully do so. The Kafkaesque process that data brokers force Americans to go through to prevent the sale of their information is not just a consumer privacy issue; it is an important matter of national security, because foreign governments are buying and exploiting this data.

A universal personal data deletion mechanism is such a common sense idea that California's Delete Request and Opt-out Platform (DROP) will likely prove to be popular with the public, loathed by data brokers, and copied by other states. Certainly, that was my hope when I introduced the Mind Your Own Business Act in 2019 — which contained a universal deletion mechanism that inspired California's Delete Act. While Congress has failed to pass my bill, or anything like it, I worked with the CPPA to codify my idea and I look forward to seeing other states follow.

Beyond protecting ordinary Americans' privacy, the DROP can help to address national security threats by preventing foreign adversaries from acquiring personal information of U.S. government employees living in California or who previously lived there before

911 NE 11TH AVENUE  
SUITE 630  
PORTLAND, OR 97232  
(503) 326-7525

405 EAST 8TH AVE  
SUITE 2020  
EUGENE, OR 97401  
(541) 431-0229

SAC ANNEX BUILDING  
105 FIR ST  
SUITE 201  
LA GRANDE, OR 97850  
(541) 962-7691

U.S. COURTHOUSE  
310 WEST 6TH ST  
ROOM 118  
MEDFORD, OR 97501  
(541) 858-5122

THE JAMISON BUILDING  
131 NW HAWTHORNE AVE  
SUITE 107  
BEND, OR 97701  
(541) 330-9142

707 13TH ST, SE  
SUITE 285  
SALEM, OR 97301  
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

deploying overseas. As then-President Biden emphasized last year in Executive Order 14117, “[t]he continuing effort by countries of concern to access Americans' bulk sensitive personal data and United States Government-related data threatens the national security and foreign policy of the United States.” The sale and AI-enabled analysis of commercial data poses a threat to Federal workers and contractors. Moreover, as the EO further notes, “[c]ountries of concern can use AI to target United States persons for espionage or blackmail by, for example, recognizing patterns across multiple unrelated datasets to identify potential individuals whose links to the Federal Government would be otherwise obscured in a single dataset.”

For understandable reasons — the quick January 1, 2026, launch deadline mandated by the Delete Act and CPPA's resource constraints — the agency chose a relatively simple design that minimizes the difficulty and cost of building and operating the DROP, while compromising on some privacy protections that would be provided by more technologically complex approaches. The agency will make several lists available to registered data brokers — each containing only one type of identifier — for all Californians that have enrolled in the system. Data brokers are required to regularly download these lists and then scrub their own records that match these identifiers. Critically, the identifiers are not linked in the lists that the CPPA releases to data brokers. The data brokers will be told which identifiers to scrub, but will not be told that a particular email address is associated with a phone number or mobile advertising ID.

While the DROP design may be fine for the average person, it is unlikely to meet the heightened security needs of U.S. government personnel. By distributing identifiers of all enrolled users to every registered data broker, the current system design creates a potentially dangerous paradox: data brokers that never possessed certain consumers' information will now receive those consumers' hashed identifiers, albeit without links between the different types of identifiers. Moreover, the CPPA has opted to provide the data brokers with identifiers in hashed form, which the Federal Trade Commission has made clear is not an effective method of protecting private data. As such, it will be easy for data brokers and foreign intelligence agencies receiving data from them to reverse engineer the hashed identifiers and determine if a particular telephone number, email address, advertising ID, or user identified by their name, date of birth and zip code has opted out. While such information is likely available from other sources, this may still prove to be too much for risk-averse agencies to recommend that their California employees enroll in DROP, due to the concern that these identifiers could be used by foreign adversaries to target hacking operations and other forms of espionage.

The DROP is a great first step, and I commend California's legislature and the CPPA for delivering this important privacy protection to Californians. Just as California has led by requiring companies honor the Global Privacy Control tracking opt-out delivered by consumers' web browsers to websites, which other states like Oregon and Colorado subsequently adopted, other states are rapidly creating centralized data broker registries and will likely soon pass laws that provide a similar universal deletion system that mirrors the

California DROP system.

It is for this reason that I encourage the agency to begin working on an improved DROP, immediately after the first version has launched, ideally in partnership with other interested states. This upgraded version should use modern encryption technologies, such as private set intersection, to ensure that data brokers only receive the minimum information necessary to process deletion requests. These technologies can be readily implemented using free, open-source software or using off-the-shelf products offered by commercial cloud providers.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

A large black rectangular redaction box covering the signature of Ron Wyden.

Ron Wyden  
United States Senator

**Grenda, Rianna@CPPA**

---

**From:** Dincer, Melodi <dincer@law.ucla.edu>  
**Sent:** Tuesday, June 10, 2025 4:06 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Accessible Deletion Mechanism - UCLA Law Information Policy Lab Submission  
**Attachments:** UCLA ITLP\_CPPA DROP Comment\_06.10.25.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Greetings,

Attached are Comments from UCLA Law's Information Policy Lab, an offering of the Institute of Technology, Law & Policy at UCLA. Please do not hesitate to reach out to Melodi Dincer at [dincer@law.ucla.edu](mailto:dincer@law.ucla.edu) with any related questions or concerns.

In peace,  
Melodi

—  
Melodi Dinçer (she/ella)  
Policy Counsel : Tech Justice Law Project  
Lecturer : UCLA Law  
Affiliated Fellow : UCLA Institute for Technology, Law & Policy  
Los Angeles, CA

[\[How to say my name\]](#)

*Unless a message is marked urgent or time-sensitive, there is no rush to reply!*

**Melodi Dincer**

Lecturer-in-Law, Information Policy Lab

Affiliated Fellow, Institute of Technology, Law & Policy

Email: [dincer@law.ucla.edu](mailto:dincer@law.ucla.edu)

June 10, 2025

Submitted via email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

**Re: Public Comment on the Accessible Deletion Mechanism Proposed Regulations**

Dear Board Members,

The Information Policy Lab at UCLA Law, an offering connected with the UCLA Institute of Technology, Law & Policy, submits this Comment to help strengthen the Agency's proposed regulations governing the accessible deletion mechanism, or the Delete Request and Opt-Out Platform (DROP) system. A product of California's public university system, the Lab is grateful for the opportunity to offer the following analyses and recommend regulation language as the Agency works towards rolling out this first-of-its-kind system to all Californians by January 1, 2026.<sup>1</sup>

California's enactment of the Delete Act in 2023 reflects the public's growing concern with the massive data broker industry, which trades in their data with almost no legal restrictions in the U.S. The Agency's implementation of the DROP system offers a unique opportunity to protect Californians' privacy in a tangible way. It enshrines core principles of data autonomy, including data deletion rights, in an accessible, consumer-centric tool.

The proposed regulations are largely operational at this stage, detailing technical requirements for data brokers that will use the system to process data deletion requests. The following analyses offer improvements to the existing language and suggest some bigger-picture considerations for the final regulations, focusing on raising the public's awareness of the DROP system and ensuring they can use it with ease, as well as offering a robust legal and constitutional analysis of the system and the Delete Act. These recommendations aim to ensure that the DROP system is not only legally sound, but also maximally functional and effective.

---

<sup>1</sup>This Comment was prepared by the Information Policy Lab during the Spring 2025 semester. The author would like to thank UCLA Law students Ekene Anene, Suzan Bedikian (Class of 2025), Lily Costa, Haley Higa, and Amanda Parham for their diligent research and early substantive drafting.



Our key recommendations are as follows:

- **Clarify scope** to ensure the system will apply consistently and clearly across data brokers, their affiliates, and evolving business models, as well as enhancing consumer education. This includes clarifying key differences between “first-party” and “third-party” data, among other aspects in the proposed regulations.
- **Strengthen enforcement mechanisms** against unregistered data brokers by increasing monitoring and investigations, imposing stronger penalties, using automated compliance tools, and publicizing noncompliant brokers.
- **Increasing direct consumer accountability** by creating a formal appeals process, establishing a consumer hotline and portal, implementing a “Three Strikes” rule, requiring businesses to justify noncompliance, and ensuring dispute resolution transparency.
- **Educating consumers and managing expectations** by ensuring the DROP system is clearly publicized and designed in an accessible, approachable way, while also educating Californians on the scope and limits of the tool.

## I. Background: Data Brokers, Data Privacy Laws, and the DROP System

In today’s digital economy, data brokers play a crucial but often invisible role in shaping consumer experiences and driving business decisions. These companies collect and analyze personal information—including demographic details and browsing habits across devices—to create profiles on individual consumers and their internet habits. They also buy, sell, and disclose this personal data—rendering consumer consent meaningless. These data brokers have made billions in profits by collecting consumer information without any direct consumer interactions.

In 2022, the data broker industry brought in over \$250 billion, revenue that was made possible by the lack of consistent regulation allowing the industry to grow uncontrolled.<sup>2</sup> Data brokers tend to operate behind the scenes and are largely unknown to the average consumer—a characteristic that contributes to the industry’s overall success. When scrolling through feeds and querying LLM-bots, delivering meals for subsistence, or just shopping for immediate gratification, companies increasingly capture peoples’ interactions as valuable data, which data brokers aggregate and sell most often to other companies. In California, consumers—including workers—are some of the few in the country to have legal protections within this dynamic.

In the United States, “notice and consent” continues to dominate privacy law initiatives. California has led the charge to regulate with the creation of the 2018 California Consumer Privacy Act (CCPA), and the 2020 California Privacy Rights Act (CPRA). Both acts were created with the intention of providing consumers with increased control over their personal information by granting them the right to be notified, consent and limit data use, and opt out.<sup>3</sup> Unlike the GDPR’s proactive deletion and use restrictions like the “right to be forgotten,” however, the CCPA and CPRA mostly

---

<sup>2</sup> Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CTR. JUST. (Feb. 13, 2024), <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole>.

<sup>3</sup> *CCPA v. CPRA Flowchart*, BLOOMBERG L., <https://pro.bloomberglaw.com/insights/privacy/ccpa-v-cpra-flowchart/?trackingcode-cta=BLAW23109750> (last visited May 10, 2025).

promote an opt-out model, placing the burden of data management on consumers to prevent their data from being misused.

Escalating digital privacy concerns within the state as well as globally have forced California legislators to increase their efforts in consumer privacy protection. While the CCPA and CPRA represent important initial steps toward ending the misuse of personal information, both acts fall short of providing comprehensive consumer protection.

Despite their best intentions, both the CCPA and CPRA contain loopholes and weak enforcement mechanisms that empower companies to collect data without meaningful consumer consent.<sup>4</sup> The CCPA places a heavy burden on consumers, requiring them to navigate dense, confusing privacy notices and submit individual opt-out requests. The CPRA expanded privacy protections, but maintained the opt-out model, partnering with tools such as the Global Privacy Control (GPC), a browser extension “switch” that lets consumers opt out of sharing personal information with many online businesses. However, this method is not currently standardized and does not always recognize the varied language used by various websites that request personal information usage. This opt-out method continues to place the burden on consumers to monitor their data’s use, and allows businesses to deny data deletion requests at random.<sup>5</sup> Together, these Acts highlight not only the state’s evolving approach to consumer privacy protection, but also the weak points that future regulations must address to ensure true consumer privacy protection.

In recognition and response to these shortcomings, California introduced the Delete Act (SB 362) to expand the state’s privacy framework and reduce consumer burden. This act includes the launch of California’s Delete Request and Opt-Out Platform (“DROP system”), which will allow consumers to request the deletion of all non-exempt personal information from registered data brokers.<sup>6</sup> By creating a centralized system for mass data deletion, the DROP system will ease the burden placed on consumers. The tedium of individual opt-out requests across web platforms will be eliminated, replaced by a more streamlined process. Instead of requiring consumers to navigate dense privacy disclosures and website-specific opt-out procedures, the DROP system will allow consumers to make a single, clear request to remove their personal information — shifting the balance of power away from businesses and back to the individual.

Accordingly, the primary compliance trigger for the DROP system occurs when a consumer or their authorized agent submits an opt-out request, asking businesses to stop the sale of their personal data. Starting on August 1, 2026, data brokers will have an ongoing obligation to access the system at least once every 45 days to address and process all verifiable deletion requests.<sup>7</sup> Once an opt-out request has been submitted, the burden of responsibility shifts to the businesses,

---

<sup>4</sup> *Tech Giants Under Fire for Lax Data Privacy*, ICLG (Aug. 2, 2024), <https://iclg.com/news/21183-tech-giants-under-fire-for-lax-data-privacy>.

<sup>5</sup> See Jacklin Lee, *CCPA/CPRA: Consumers Bear the Burden as Companies Bear the Crown*, 47 HASTINGS INT’L & COMP. L. REV. 129 (2024) (finding that both the CCPA and CPRA are inadequate to protect consumer data).

<sup>6</sup> CAL. PRIV. PROT. AGENCY, PROPOSED REGULATIONS ON ACCESSIBLE DELETE MECHANISM—DELETE REQUEST AND OPT-OUT PLATFORM (“DROP”) SYSTEM REQUIREMENTS (2025), <https://cppa.ca.gov/regulations/drop.html> (last visited May 10, 2025).

<sup>7</sup> California Delete Act, CAL. CIV. CODE § 1798.99.86 (West 2024).

which are obligated to comply. Data brokers will be required to delete that consumer's personal information at least once every 45 days and refrain from selling or sharing any new personal information collected from that consumer. Beginning January 1, 2028, data brokers will undergo an independent third-party audit every three years to assess compliance with the Delete Act.<sup>8</sup> Furthermore, beginning on January 1, 2029, businesses will be required to declare whether they have undergone such an audit in their annual data broker registration. Failure to delete consumer data upon request will result in heavy penalties. By shifting this responsibility, the DROP system provides a necessary step forward in effectuating Californian's existing privacy rights.

## **II. Proposed Regulations Should Better Clarify the Scope of the DROP System to Meet Consumer Expectations, Including Clarifying Exempted Entities and Related Data**

### **A. Linking DROP System Participation to Data Broker Registration Can Be Underinclusive, Especially Considering the Jump in Registration Costs**

The proposed regulations are useful in describing the operation of the DROP system and setting up requirements for complaint data brokers to use the system. But a key question for consumers will be, what are they opting out of exactly? To help answer that question, the Agency should ensure that the final regulations incentivize data brokers to register in the first place, both allowing the Agency to better understand the landscape and increasing public trust that submitting a deletion request through DROP will reach as many data brokers as possible.

The Delete Act defines a 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.”<sup>9</sup> Although California has a data broker registry, many data brokers operate without registering, reducing transparency and making it difficult for consumers to fully exercise their rights. Given that the data broker industry includes thousands of players globally, there is a risk that many companies selling California residents' data are not complying with the law. Currently, the CPPA has a data broker registry with 543 registered data brokers.<sup>10</sup> An industry report described the size of the data broker industry globally as having up to 5,000 players, meaning only about 10% have registered in California as required by law.<sup>11</sup> As North America has the dominant market share, the existing registry likely does not capture every data broker operating in California or trading in Californians' data.

---

<sup>8</sup> Ken D. Kumayama, et al., *California's Data Deletion Law Imposes a Host of New Obligations on Data Brokers*, SKADDEN (Dec. 14, 2023), <https://www.skadden.com/insights/publications/2023/12/californias-new-data-deletion-law-imposes>.

<sup>9</sup> Cal. Civ. Code §§ 1798.99.80–1798.99.89.

<sup>10</sup> CAL. PRIV. PROT. AGENCY, 2024 DATA BROKER REGISTRY (Apr. 2024), [https://cppa.ca.gov/data\\_broker\\_registry/registry2024.csv](https://cppa.ca.gov/data_broker_registry/registry2024.csv) (last visited May 10, 2025).

<sup>11</sup> See *Data Broker Market: Global Industry Analysis and Forecast (2025-2032) by Data Category, Data Type, End-User and Region*, MAXIMIZE MKT. RSCH., <https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670> (last visited May 10, 2025).

The proposed regulations describe how the DROP system will be linked to the data broker registry, but they also erect a considerable barrier to increasing the amount of data brokers that register with the state. Specifically, the first-time registration fee jumped from \$400 to \$6,600. §7611.(a)(3)(A).

Previously, many businesses registered despite not knowing clearly if they fit the definition of a data broker because the \$400 fee was low enough to justify overinclusion.<sup>12</sup> Now, however, several businesses that may otherwise count as data brokers under the Delete Act and who *should* be subject to the DROP system may avoid registering due to the steep increase in costs. This is a significant issue, since the Agency does not have a way of identifying data brokers processing Californians' data until they register as such.

If the current data broker registry is under-inclusive, the DROP system will inevitably fall short of its intended purpose, leading consumers to doubt the utility of submitting deletion requests through the DROP system compared to purchasing similar services from private data management companies. Data brokers that are not registered will escape regulation, allowing them to continue collecting and selling consumer data, ultimately undermining consumer privacy protections and eroding public trust in the mechanism.

The Agency should take additional time and care to ensure that the final regulations incentivize data brokers to register and be transparent with consumers if the costs of building and running the system may compromise industry compliance. The Agency should thus consider how to draft regulations in a way that encourages data brokers to register and how to set up monitoring processes to ensure that the registry—and, by extension, the businesses that must participate in the DROP system—is as inclusive as possible,<sup>13</sup> including structuring fees and other compliance requirements to apply on a scaled basis once businesses have already registered and provided further information concerning their size and relevant operations. Additionally, the Agency may consider working together with the California Department of Technology (CDT) and California-based research universities to further investigate barriers to data broker registration and develop technical and policy interventions that will help ensure the registry is as robust as possible.

### Recommended Actions:

- **Increase Monitoring & Investigations:** The Agency should proactively identify unregistered data brokers through online tracking, industry reports, and consumer complaints.
- **Impose Stronger Penalties:** The current fine of \$200 per day for failing to register may not be a sufficient deterrent, especially for large firms. The Agency should consider increasing fines for prolonged noncompliance and scaling penalty amounts based on size metrics.

---

<sup>12</sup> CAL. PRIV. PROT. AGENCY, PUBLIC COMMENT HEARING TRANSCRIPT at ¶¶ 8-10 (Mar. 7, 2025), [https://coppa.ca.gov/meetings/materials/20250307\\_audio\\_transcript.pdf](https://coppa.ca.gov/meetings/materials/20250307_audio_transcript.pdf).

<sup>13</sup> See Suzanne Smalley, *California Shuts Down Data Broker for Failing to Register*, THE RECORD (Feb. 28, 2025), <https://therecord.media/california-shuts-down-data-broker-for-failing-to-register>.

- **Use Compliance Tools:** The Agency could implement automated tools to track companies that engage in large-scale data transactions to ensure they are registered, working together with the CDT and California universities to develop such interventions.
- **Publicize Noncompliant Brokers:** The Agency should publish an annual report listing companies that fail to register to increase accountability and deter noncompliance.

**Proposed Language:**

Agency Monitoring of Registration Compliance

Pursuant to Cal. Civ. Code § 1798.99.82, the Agency shall proactively identify unregistered data brokers through online tracking, industry reports, and consumer complaints and should assess whether increasing fines for noncompliance would work as a sufficient deterrent. Additionally, the Agency shall publish an annual report listing companies that fail to register.

Restructuring Registration Fees to Incentivize Registration

Data brokers that register within six months of the enactment of these regulations will be eligible to waive the first-time access fee required for accessing the DROP system. If a data broker registers after the initial six-month period, they will pay a first-time access fee based on their scale as detailed below. For each subsequent month, the maximum fee will decrease by \$100:

- (A) If the data broker accesses the DROP for the first time in January, the access fee will range based on the business's providing documents establishing relevant number of customers, amount of data sales per month, and other relevant operations information. For data brokers with no more than 50 customers, the fee shall not exceed \$500. For data brokers with 50-100 customers, the fee shall not exceed \$2,000. For data brokers with 100-1,000 customers, the fee shall not exceed \$5,000. For data brokers with more than 1,000 customers at the time of registry, the fee shall not exceed \$10,000.
- (B) ... [reducing subsequent fees by \$100 per month until the next registration period]

**B. Consumers May Falsely Assume the DROP System Applies to Entities That Trade in Personal Data But That Are Exempt Under the Delete Act, Including the Sensitive Data They May Collect**

Another key question is the state of exempt companies who meet the terms of the Delete Act but are nonetheless exempt because they are covered by the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act, the Insurance Information and Privacy Protection Act, or those processing information pursuant to the Confidentiality of Medical Information Act. When consumers choose to opt out universally through the DROP System, they may believe that companies that are definitionally data brokers but who are exempt from the Delete Act would be included in the opt out. This may give consumers the false impression that submitting a deletion request through the system will cover more data brokers than it really does.

The Agency should take proactive steps to prevent this confusion, clearly communicating

which companies are exempt from the system.<sup>14</sup> This is especially important considering the type of data that is at issue when data brokers operate as health and wellness aggregators, financial and risk assessment firms, people search and background check services, and location data brokers. Notably, some of the largest entities in this space, such as credit reporting agencies, are already regulated under laws like FCRA, and may be exempt from state-level requirements, further narrowing the scope of any registry or opt-out mechanism.

A related concern is that the proposed regulations are not clear as to what kinds of personal information data brokers must delete pursuant to the selected consumer deletion lists.

§ 7610.(a)(3)(A). As raised before the Board during the Public Comment Hearing, the system is built only to collect first and last names, email addresses, phone numbers, ZIP codes, dates of birth, and pseudonymous identifiers (like device IDs).<sup>15</sup> While the proposed definition of “Personal information associated with a matched identifier” is broad, consumers may not understand what “inferences made from the personal information” refers to or, more generally, that this broad definition does not apply for exempted entities.

This is especially significant with more sensitive personal data, like precise geolocation data and biometric data, which a data broker may choose to archive separately from other forms of identifiers contained in the draft regulations. As written, the regulations do not seem to cover instances where a data broker may go through the standardizing processes required in § 7613 but craftily choose to disaggregate valuable sensitive types of data and maintain them separately from the identifiers that would otherwise match the consumer deletion list(s) of their choice. Presumably, if “inferences” do not include this data-structuring activity, businesses may be incentivized to organize some of our most sensitive types of data in a way that eludes the DROP system.

For example, while the proposed regulations define “Reproductive health care data” expansively to include several types of health data, those data may not be covered by the DROP system so long as the collecting data broker is exempt under the Delete Act. § 7601.(I).<sup>16</sup> Even where a data broker is not exempted, however the regulations as written do not prevent that data broker from storing such sensitive data internally in a way where the identifier-based standardization process will not reach that data. Californians who use the DROP system may overestimate the efficacy of the one-click universal opt-out tool as a result.

---

<sup>14</sup> In its preliminary comment to the CPPA on June 25, 2024, data broker Experian noted that:

[T]he CPPA should explain to consumers that requests through the DROP do not apply to personal information and/or entities covered by applicable laws set forth in the Delete Act, ... [and] that a request made through the DROP will not limit retention and use of personal information for fraud prevention and security and integrity purposes by data brokers.

Experian, *Comment Letter on the Proposed Rulemaking Under Senate Bill 362 (The “Delete Act”)* (June 25, 2024), [https://cppa.ca.gov/regulations/pdf/preliminary\\_drop\\_public\\_comments.pdf](https://cppa.ca.gov/regulations/pdf/preliminary_drop_public_comments.pdf).

<sup>15</sup> TRANSCRIPT, *supra* note 12 at ¶¶ 22–25.

<sup>16</sup> Notably, while this term is defined, it does not appear again in the proposed regulation text.



## Recommended Actions:

- **Provide a Public List of Exempt Entities:** The Agency should publish a clear, easily accessible list of companies and industries that are exempt from the DROP tool, with an explanation of why they are excluded. Any outreach materials should clarify the distinction between data brokers covered by the Delete Act and those exempt due to other laws.
- **Require Disclosure from Exempt Entities:** In addition, businesses that qualify for exemptions should be required to notify consumers that they are not subject to DROP, preventing confusion.
- **Evaluate Potential Expansion:** The Agency should assess whether exemptions should be narrowed over time to align with evolving privacy concerns and regulatory needs.
- **Clearly Define What Types of Data the DROP System Covers:** The Agency should clarify which types of data the system will use solely to facilitate data brokers' deletion of personal data—i.e., consumer deletion lists—versus the types of personal data they must delete. With sensitive data, the Agency should limit data brokers' ability to disaggregate such data from the identifiers contained in consumer deletion lists. The regulations should also further clarify the breadth of inferences made from the covered personal information, perhaps aligning with the definition under the CCPA.<sup>17</sup>

## Proposed Language:

### Exempted Entities

Pursuant to Cal. Civ. Code § 1798.99.86, the Agency will publish a clear, easily accessible list of companies and industries that are exempt from the DROP system, with an explanation of why they are excluded. The Agency shall additionally provide materials directly to consumers that clarify the distinction between data brokers covered by the Delete Act and those exempt due to other legal frameworks, including how this interacts with the broad definition of personal information under the regulations. Every two years, the Agency shall review the statutory exemptions together with objective evidence of industry trends to assess whether enforcement actions can expand to align with evolving privacy concerns and regulatory needs.

### Types of Data Covered

“Personal information associated with a matched identifier” means any personal information maintained in a data broker’s records collected from a source other than directly from the consumer through a “first party” interaction. This personal information may include, but is not limited to, the identifiers defined under this section for use in consumer deletion lists. This does not include personal information that is subject to applicable exemptions, but includes inferences made from the personal information. “Inferences” include insights drawn from any personal information as defined in this subsection to create a profile about a consumer reflecting the consumer’s

---

<sup>17</sup> Civ. Code, § 1798.140, subd. (o)(1).

preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

### **C. The Present “Direct Relationship” Definition, Though Laudably Defined by Consumer Intent, Can Be Further Clarified to Prevent Data Broker Gamesmanship**

In the current digital landscape, vast amounts of incidental data are created about an individual without their consent. The Agency recently clarified that companies with whom a consumer has a direct relationship may be considered a data broker where information they process may have been collected by a “source other than the consumer.”<sup>18</sup> The proposed regulations could be much clearer, however, over how the DROP system would apply to incidental data collected by companies that do not have a direct relationship with the consumer.<sup>19</sup>

Regulated data brokers might try to claim “direct relationships” to individuals to circumvent complying with the DROP system, especially when first-party and third-party interactions occur with the same data broker across different contexts. Specifically, businesses may claim that they have a direct relationship with consumers based on indirect or passive interactions, such as users visiting a website, seeing an ad, or being sent a promotional email—as the current regulations do not clarify what it means for a consumer to intend to interact with a business, this vague description might encompass these more passive interactions, so long as the consumer “intended” to engage in them. The Agency has previously noted the ambiguity that a data broker can have both first-party and third-party interactions with a consumer under the Delete Act and should consider building on that awareness both in the final regulations and in related consumer outreach.<sup>20</sup>

To make matter worse, many large data brokers operate through a network of subsidiaries and affiliated entities, allowing them to circumvent opt-out requests by shifting consumer data to legally distinct entities. Without clear rules, a consumer could opt out via the DROP system, but their data could still be retained and used by a parent company or partner firm.

We strongly urge the Agency to maintain its stance regarding incidental data, particularly the requirement that data brokers “[d]elete all consumer personal information, *including inferences based in whole or in part on personal information collected from third parties or from consumers in a non-‘first party’ capacity*, that is associated with a matched identifier in the data broker’s records.” § 7613(b)(1) (emphasis added). This helps prevent companies from using data collected from friends and family who chose not to opt-out as a potential workaround to continue to profit from an opted-out consumer’s data, despite their having used the DROP system.

---

<sup>18</sup> See DATA BROKER REGULATIONS FSOR, *supra* note 6 (Noting that “[i]f consumers are not allowed to take advantage of the protections afforded under SB 362, they will have no way to delete this ‘incidental’ data and will have less control over their personal information. . . .”).

<sup>19</sup> CAL. PRIV. PROT. AGENCY, DATA BROKER REGISTRATION AND ACCESSIBLE DELETION MECHANISM: PROPOSED TEXT (Apr. 25, 2024), [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_accessible\\_deletion\\_mechanism\\_text.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_text.pdf) (emphasis added).

<sup>20</sup> CAL. PRIV. PROT. AGENCY, FIRST STATEMENT OF REASONS: APPENDIX A—SUMMARY AND RESPONSE TO WRITTEN AND ORAL COMMENTS (Sept. 2024), [https://cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_isor.pdf](https://cppa.ca.gov/regulations/pdf/data_broker_reg_isor.pdf).

The Agency might take further steps to clarify the differences between first-party and third-party interactions by narrowing what is considered a “direct relationship” to require clear evidence of a direct transaction or user-initiated interaction. While the current regulations emphasize consumer intent to have the interaction as a hallmark of its “first-party”-ness, the Agency should refrain from requiring consumers to establish this intent and instead impose the burden of proof on data brokers to show that they have this direct relationship. Further regulations may be needed to establish the factors which data brokers will need to use to make a showing of consumer intent and offer consumers a simple way to contest these determinations when necessary. Further, the CPPA might consider shortening the automated expiration of direct relationships from three years under the DELETE Act to one year for the purposes of the DROP system, unless businesses can prove ongoing first-party interactions. The Agency should also mandate that opt-out requests apply across all subsidiaries and third-party affiliates to prevent circumvention of deletion requests.

#### **Recommended Actions:**

- **Mandate Cross-Entity Compliance:** The Agency should require that when a consumer submits an opt-out request, it applies to all affiliates, subsidiaries, and third-party partners of a data broker.
- **Require Transparency in Data Transfers:** Data brokers should be obligated to disclose how they share data within corporate structures and with external partners.
- **Implement a ‘No Repurchase’ Rule:** To prevent companies from reacquiring deleted data through third parties, the Agency should prohibit the repurchase or reintegration of consumer data once it has been deleted under DROP.
- **Audit Corporate Data Sharing Practices:** The Agency should conduct periodic reviews to ensure companies are not using technical loopholes to circumvent consumer deletion requests.

#### **Proposed Language:**

##### Broad Application of Deletion Requests:

Pursuant to Cal. Civ. Code § 1798.99.86 , when a consumer submits an opt-out request, it applies to all affiliates, subsidiaries, and third-party partners of data brokers. Data brokers must disclose how they share data within corporate structures and external partners to increase transparency. Furthermore, to prevent companies from reacquiring deleted data through third parties, the Agency should prohibit the repurchase or reintegration of consumer data once it has been deleted under DROP. Once a year the Agency should conduct a review to ensure companies are not using technical loopholes to circumvent consumer deletion requests.

##### Narrowing the Direct Relationship and First-Party Interaction Distinction

Businesses asserting a direct relationship bear the burden of proving such relationship was initiated by the individual. Any claimed direct relationship with an individual shall automatically expire after one (1) year, unless substantiated by an ongoing consumer-initiated interaction.

### Strengthening Deletion Across All Third-Party Data Processors

§7613.(b)(2) A data broker must direct all service providers, contractors, affiliates, subsidiaries, and any other third-party data processors to immediately delete all personal information in its possession related to a consumer associated with a matched identifier. Within 24 hours of so directing, a data broker must provide a receipt confirming this action was taken that lists all service providers, contractors, affiliates, subsidiaries, and any other third-party data processor involved.

### Incorporating a “No-Repurchase” Rule

Pursuant to Cal. Civ. Code § 1798.99.86, a data broker must legally attest that no version of deleted personal data—including inferences, derived data, and depersonalized or anonymized data—will be used, sold, transferred, or reacquired upon processing a consumer deletion list. A data broker shall not repurchase or otherwise reacquire information that was subject to a delete request, either directly or indirectly, including through affiliates, subsidiaries, or other third parties. A data broker shall not use, retain, sell, or share anonymized data if it was originally derived from a consumer record that is subject to a deletion request under the Delete Act.

## **III. Proposed Regulations Should Strengthen the Agency’s Enforcement Mechanisms to Increase Direct Accountability to Consumers**

Clarity in enforcement of the DROP system is essential for ensuring that both consumers and businesses understand their rights and obligations. Without transparency in enforcement, consumers may experience frustration with the DROP system, which could erode trust and undermine its efficacy and the Agency’s goals of making the tool accessible. The final regulations should be clear and transparent concerning how the Agency plans to both incentivize and enforce data broker compliance. If the enforcement framework is ambiguous, consumers may struggle to exercise their rights effectively, and businesses may face uncertainty in how to implement opt-out requests, leading to inconsistent outcomes.

For consumers, a significant barrier to protecting their personal data is a lack of understanding of both privacy laws and how companies use their personal data.<sup>21</sup> Studies have shown that consumer understanding of privacy language does not match the understanding of

---

<sup>21</sup> See Takahito Sakamoto & Masahiro Matsunaga, *After GDPR, Still Tracking or Not? Understanding Opt-Out States for Online Behavioral Advertising*, 2019 IEEE SECURITY AND PRIVACY WORKSHOPS (2019), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8844599> (finding that 34% of users mistakenly believed that opt-out causes agencies to stop collecting user data, 57.9% of users incorrectly believed that opt-out would stop both web tracking and tailored advertisements, and only 13.4% correctly understood that it is intended to stop tailored advertisements” and “no users correctly understood the meaning of opt-out.”); see also Brooke Auxier, Lee Rainie, Monica Anderson, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), [https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center\\_PI\\_2019.11.15\\_Privacy\\_FINAL.pdf](https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf) (finding that “six-in-ten Americans (63%) say they have very little or no understanding of the laws and regulations that are currently in place to protect their privacy. Only 3% of adults say they understand these laws a great deal, and 33% say they have some understanding” and “[r]oughly eight-in-ten or more U.S. adults say they have very little or no control over the data that government (84%) or companies (81%) collect about them.”).

courts and legal experts.<sup>22</sup> As the Agency is still young, it is crucial to build consumer trust through transparency and consumer-friendly communication regarding enforcement mechanisms of the DROP system, including a step-by-step explanation of (1) how businesses process these opt-out requests, (2) what personal data is and, importantly, is not covered by the opt-out request, (3) how a consumer will be notified that their request has been processed, and (4) what recourse consumers have if a business does not comply.<sup>23</sup>

The present regulations do not contemplate these matters from a consumer's perspective, only outlining technical requirements for data brokers to register, access, and process consumer deletion lists without increasing accountability to Californians directly. We recommend the Agency consider either expanding the current draft or initiate subsequent rulemakings to focus more on the consumer's side of the equation.

#### **A. Develop a Deletion-Dispute Resolution Mechanism and Other Direct Accountability Measures for Consumers**

Consumers should have access to an appeals process when businesses refuse to honor opt-out requests, ensuring stronger consumer protections. While the DROP system provides consumers with a streamlined way to opt out, there is currently no clear process for handling disputes when a data broker refuses to comply. Businesses may reject opt-out requests by claiming that compliance would be too burdensome, fail to register altogether, or otherwise delay action without consequence. While the Agency directs consumers to file a complaint if they become aware of a non-registered data broker, the Agency should consider enshrining a complaint and appeals process in the DROP system regulations and further educating consumers about these important enforcement mechanisms within their direct power.<sup>24</sup>

Without an explicit deletion complaint and appeals process, consumers have limited recourse if their request is ignored or denied. Further, offering an appeals process will help ensure that Californians believe the DROP system does what it states it will do—offer a comprehensive, one-click option to signal data deletion requests across the murky, plentiful data broker industry. If consumers go through the process, they should have some way of assessing personally that their data has been effectively deleted; an appeals process would enable them to do so when a data broker that should be complying with the regulations fails to do so, and the Agency missed it despite the regulation's robust reporting and auditing requirements.

---

<sup>22</sup> See, e.g., Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUDS. 69 (Sept. 9, 2016) (“Context, experience, and [social] norms, rather than privacy policy language, seem to benchmark consumers’ understandings about what conduct they are authorizing, and that is the case even in those instances where one can be confident that consumers have read the relevant policy language rather carefully.”).

<sup>23</sup> Our recommendations are consistent with the Fair Information Practice Principles (FIPPs) and the OECD privacy principles. See *Fair Information Practice Principles (FIPPs)*, FED. PRIV. COUNCIL, <https://www.fpc.gov/resources/fipps> (“Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.”) (last visited May 10, 2025).

<sup>24</sup> Press Release, CAL. PRIV. PROT. AGENCY, *CPPA’s Enforcement Division to Review Data Broker Compliance with the Delete Act* (Oct. 30, 2024), <https://cppa.ca.gov/announcements/2024/20241030.html>.

The Agency might also consider creating a user feedback portal and/or an annual survey where Californians can express concerns and questions about how their data is being used directly, despite using the DROP system, to get real feedback about ways that data brokers may be evading compliance.

We further recommend the Agency implement an annual public-facing report notifying the public of non-compliant data brokers or data brokers that have received above a threshold number of credible complaints for failing to comply with their ongoing burden to delete personal data. This transparency would make data brokers accountable to the public as well as the CPPA, ensuring that data brokers are appropriately incentivized to comply with the DROP system.

#### **Recommended Actions:**

- **Create a Formal Appeals Process:** Consumers should be able to appeal when a business denies an opt-out request. The CPPA should review these cases and intervene if necessary.
- **Establish a Consumer Hotline & Portal:** A dedicated system for submitting complaints about noncompliance should be available, making it easier for individuals to report violations.
- **Implement a ‘Three-Strikes’ Rule:** Data brokers with repeated complaints should face escalating penalties, including higher fines and potential suspension from data sales.
- **Require Businesses to Justify Noncompliance:** If a data broker refuses a deletion request, they should be required to provide a written explanation, subject to CPPA review.
- **Ensure Dispute Resolution Transparency:** The CPPA should publish anonymized data on consumer complaints, outcomes, and enforcement actions to increase accountability.

#### **Proposed Language:**

Pursuant to Cal. Civ. Code § 1798.99.86, if a data broker refuses a deletion request, they must provide a written explanation to both the requesting consumer and the Agency. To ensure enforcement of the Delete Act, the Agency shall establish a dedicated system for submitting complaints of data broker noncompliance. Data brokers with repeated complaints will face escalating penalties. The Agency shall additionally create a formal appeals process where consumers may appeal a denial of an opt-out request. The Agency shall further publish anonymized data on consumer complaints, outcomes, and enforcement actions to increase accountability.

#### **B. Transparent Enforcement of Edge Cases**

Due to complexities in data structures, varying user preferences, and limitations in current data management systems, transparency in enforcement is particularly important in edge cases where implementation of the DROP system may not be as straightforward. From the consumer’s perspective, these edge cases may undermine the efficacy of their opt-out via the DROP system, introducing more confusion than relief.

To ensure effective enforcement, the Agency should consider expanding the draft regulations to address and/or clarify how the system will treat the following scenarios:



**1. Varying Consumer Preferences:** Consumers are not a monolith, and consumer preferences vary regarding what data they wish to protect. Some consumers may wish to opt out of specific data collections like targeted ads but not analytics or personalization, for example.<sup>25</sup> For those consumers, an all-or-nothing approach to opting out may make them less likely to use the DROP system, even if they would prefer to protect their most sensitive personal data. While a comprehensive universal opt-out would be easier for businesses—particularly small businesses—to implement, a more granular system would offer greater consumer control and not necessarily need to be overly complex for businesses to manage.

**Recommendation:** The Agency should clarify whether the DROP system will allow for partial opt-outs, ensuring businesses respect consumer preferences without complicating enforcement.

**2. Revocation of Opt-Out Requests:** If a consumer changes their mind and revokes their opt-out, it may conflict with existing data retention or processing policies provided under the current regulations.<sup>26</sup>

**Recommendation:** The Agency should clarify further how businesses should handle revocations and update their data processing and reporting practices accordingly, preventing mishandling of changes in consumer preferences.

**3. Cross-border Data Transfers:** The movement of data across jurisdictional boundaries presents another challenge as “organizations must comply with two distinct systems that often have conflicting expectations.”<sup>27</sup>

**Recommendation:** If a user in California opts out, but their data is processed in another jurisdiction with different privacy laws, the Agency should clarify how opt-out requests should be handled in such cases, ensuring that consumer preferences are respected even outside California.

**4. Personal Data Used in Machine Learning Datasets and Model Training:** Automated systems and machine learning models add another layer of complexity because even if a consumer opts out, these models may continue to use historical data for training, including

---

<sup>25</sup> Kristen Doerer, *Customers Don’t Trust Businesses with their Data*, DIVE BRIEF (Apr. 8, 2024), <https://www.customerexperiencedive.com/news/customers-concerned-online-data-privacy-mistrust-companies/712464> (“Customers still want some level of personalization . . . . Americans were 25% more likely than their European counterparts to express this desire for personalization.”).

<sup>26</sup> CAL. PRIV. PROT. AGENCY, PROPOSED TEXT (EXPRESS TERMS) (Mar. 06, 2025), [https://coppa.ca.gov/meetings/materials/20250306\\_07\\_item6\\_draft\\_text.pdf](https://coppa.ca.gov/meetings/materials/20250306_07_item6_draft_text.pdf).

<sup>27</sup> See generally Abedemi Adeleye Alabi, Sikirat Damilola Mustapha, Christian Chukwuemeka Ike & Adebimpe Bolatito Ige, *Resolving Cross-Border Privacy and Security Misalignments with a Unified Harmonization Framework for U.S. and Canada*, OPEN ACCESS RSCH. J. OF MULTIDISCIPLINARY STUDS. 60 (Aug, 12, 2023), <https://oarjpublication.com/journals/oarjms/sites/default/files/OARJMS-2023-0036.pdf> (discussing the multifaceted challenges of cross-border data flows and divergent regulatory requirements).

personal data that may be archived in both open source and proprietary datasets to which the consumer requested deletion via the DROP system.<sup>28</sup>

**Recommendation:** The Agency should clarify whether and how companies developing such models must respect opt-out requests when they are also definitionally a data broker under the Delete Act.

**5. Data Retention for Legal or Contractual Purposes:** When accounts are deactivated or terminated, data brokers' retention of account data for legal or contractual purposes may conflict with processing consumer deletion lists.

**Recommendation:** The Agency should provide further guidance on balancing opt-out requests with businesses' legal obligations to retain consumer data.

To address these challenges, the Agency may adopt strategies like further defining edge cases in regulations and offering scenario-based guidance to both businesses and consumers. We have provided recommendations based on the above scenarios, but there are several other edge cases that may arise once the DROP system is in place. The Agency should consider ongoing research into the ways that data brokers may use such scenarios to undermine compliance with the Delete Act and/or the DROP system. To address future scalability and loophole concerns, the Agency might consider audits to specifically identify new methods data brokers use to collect consumer data and update the DROP system's deletion criteria accordingly in subsequent regulations. Further, as more and more states begin to contemplate similar tools, the Agency might consider ways in which the system might integrate with those emergent tools to reduce data broker gamesmanship across state lines.

#### **IV. The Agency Should Consider Including Public Education and Awareness Measures Which Will Be Crucial to the DROP System's Success**

Educating the public about the DROP tool is essential to its success. Many Californians are not aware of their rights under the Delete Act, or even what data brokers are and the extent to which their data is being collected and sold. To ensure the system is widely used and understood, the Agency must communicate this information in a clear, accessible, and engaging way. At the same time, the Agency should take care to manage expectations so that consumers have a realistic understanding of what DROP can and cannot do for them, as discussed in Section I.

At a bare minimum, the Agency should create a clear, accessible informational microsite that explains what the DROP system is, why it exists, and how it works. It should also connect directly with the DROP system, consumer complaint portal, and consumer feedback portals, as described above. This should serve as a central resource for public education, expectation setting, and transparency. The following subsections elaborate on how this site could be used strategically

---

<sup>28</sup> See Comment, UCLA ITLP, NYU Technology Law & Policy Clinic, and USC Annenberg School of Communication and Journalism, to Cal. Priv. Prot. Agency (Aug. 30, 2024), [https://law.ucla.edu/sites/default/files/PDFs/ITLP\\_General/ITLP-CPPA-Comment-GenAI-Training-0624.pdf](https://law.ucla.edu/sites/default/files/PDFs/ITLP_General/ITLP-CPPA-Comment-GenAI-Training-0624.pdf) (describing generative AI companies' systematic noncompliance with CCPA data subject access requests).

to achieve the three most important components of public engagement: reaching the community, managing expectations, and providing proof that the DROP system works.

### **A. Reaching the Community**

The first important step for the Agency is to make sure that the public knows the system exists and understands how to use it. The Agency should prioritize a multi-faceted, comprehensive public education campaign that promotes awareness and provides clear information about this purpose, scope, and limitations.

The strategy could include, but is by no means limited to:

- Digital ad campaigns focused on social media and search engines. These digital ads should use plain but catchy language to direct users to the CPPA's DROP system microsite and system, where users can access information and the tool itself.
- Physical outreach and mailers, which would be especially useful in reaching demographics that are not particularly tech savvy. The Agency could send postcards to California households with information about the tool, with a link or QR code to the DROP microsite and simple instructions on how to use the tool.
- Utilize community partnerships. The Agency could collaborate with libraries, schools, colleges, and nonprofits to distribute materials, inform the community, and potentially even host awareness events. Further, the Agency could host webinars or upload videos explaining the purpose of the DROP system, consumers' rights under the Delete Act, and step-by-step explainers on how to use the tool. The Agency could consider partnering with California-based influencers to further educate the public on social media.

### **B. Managing Expectations Through the DROP System's User Experience (UX) Design**

The Agency should be careful in setting realistic expectations for users to avoid undermining trust in the tool and in the Agency itself. Because most people are unlikely to read the fine print of the Delete Act, the public will not know who must delete their data when they use the tool, as well as who is allowed to retain and use their personal data due to exceptions or other carve-outs. Notably, users might assume that using the DROP system might stop all data collection and targeted ads, when its reach is much more limited in practice. This misalignment of expectations and reality could quickly undermine trust in the Agency's efficacy.

One strategy to get ahead of this is to have clear disclaimers on the website and outreach that the system only deletes data from registered data brokers and does not prevent all online tracking, targeted ads, or data collection via cookies or social media. Further, the CPPA's information page could have a list of specific examples for data brokers and data trades that are not covered by the system, such as browsing history collected via website cookies, data collected by companies' the users directly interact with (i.e. "first-party" data), and any data considered "publicly available." The information page could also have sample FAQs with real life scenarios or common questions users may ask on this topic.

For many users, deleting their data is likely a daunting or confusing task. To address this, the Agency should also ensure that the DROP system is designed to make the user experience smooth, accessible, and simple.

First, any landing page should have simple, easy-to-follow steps listed that guide the user through the process in plain, nontechnical language. Second, the tool should be fully optimized for mobile devices. It is likely that many users will interact with the tool via their smartphones, and the DROP system should be able to function smoothly on this interface or risk excluding large segments of the population. Third, the visual design and tone should be approachable and consumer-friendly, not bureaucratic or intimidating. Calming colors and fonts, clear headings, bold visuals, and reducing unnecessary text can be used to further educate and guide visitors through the deletion process.

Importantly, the Agency should make sure that the system is accessible to all Californians. Specifically, all information and materials regarding the DROP system, as well as the system itself, should be accessible in each of the state's most commonly-spoken languages, so that language is not a barrier. The Agency should also ensure that the system is accessible to individuals with disabilities in accordance with the Web Content Accessibility Guidelines (WCAG). By incorporating user-friendly and accessible design considerations from the outset, the Agency can increase the likelihood that DROP will be widely used and trusted.

### **C. How Users Will Know If the DROP System Works**

Since users' data will still be collected by companies that they have a direct relationship with, as well as indirectly via website cookies and complex ad-bidding systems, it might be difficult for the average user to know that the tool has worked at all.

To address this uncertainty, the Agency might consider sending automated confirmation emails to users after they submitted a request letting them know that their deletion request was processed and completed. Further, the CPPA might consider either including in their informational page that the data must be re-deleted every 45 days, or sending new automated confirmations of deletion every 45 days to let users know their data is continuing to be deleted.

The CPPA's information page might also include a section that lists a few ways users might visibly notice a difference in their ordinary internet use, including receiving fewer junk emails, fewer automated calls, less spam texts, or fewer targeted offers for ads and services based on demographic categories. The Agency might also consider sending follow up surveys to users after a few weeks have passed once their consumer deletion lists have been processed, both as a reassurance mechanism as well as to gather internal information about the efficacy of the tool.

## **V. Additional Policy Considerations: Potential Industry Pushback, Both Practical and Legal**

### **A. Potential Resistance from Industry**

The tech industry is likely to push back against the new DROP tool with various arguments. Primarily, companies will argue that there are compliance burdens and implementation costs, there will be a significant impact on business and advertising revenue, or it will chill innovation.

Companies may argue that implementing a centralized deletion mechanism is both technically complex and prohibitively expensive. They may claim that such a requirement imposes an unfair burden on small and mid-sized data brokers, which lack the financial and technological resources of larger firms. This, they argue, could create an uneven playing field, ultimately favoring dominant industry players while pushing smaller competitors out of the market.

Data-driven businesses are also likely to contend that the DROP system poses a significant threat to the digital advertising ecosystem, which relies on consumer data for targeted marketing. Industry groups may assert that restricting data availability will not only reduce advertising efficiency but also harm small businesses that depend on personalized marketing to reach their audiences. By limiting the ability to deliver relevant ads, the industry may claim, such measures could lead to a decline in ad-driven revenue and overall market competitiveness.

Additionally, some in the industry may argue that broad data deletion requests could stifle AI and machine learning advancements. Access to large datasets is critical for training AI models, and limiting data flows may, they contend, hinder progress in areas such as fraud prevention, cybersecurity, and other tech-driven innovations. They might warn that overregulation could have unintended consequences, restricting the development of new technologies that rely on robust data collection and analysis.

Finally, industry groups may raise concerns about consumer confusion and the overall effectiveness of a mass opt-out system. They may argue that consumers do not fully grasp the long-term implications of deleting their data, which could lead to unintended consequences such as loss of access to personalized services. Additionally, given that many data brokers operate without direct consumer interaction, processing opt-out requests efficiently could prove challenging, potentially undermining the intended benefits of the system.

## **B. Legal and Constitutional Concerns That May Thwart the DROP System**

### **1. Potential First Amendment Issues**

The new DROP system may be put at risk if the underlying Delete Act faces legal challenge, particularly from data brokers and technology companies. These entities may argue that the law infringes upon their First Amendment rights by restricting their ability to store, sell, and share personal data. Such First Amendment challenges are likely to be grounded in either the commercial speech doctrine<sup>29</sup> or the compelled speech doctrine.<sup>30</sup> The threshold question is whether the data implicated by the DROP system constitutes speech versus non-expressive conduct. If courts find that the DROP system targets non-expressive conduct rather than speech, it

---

<sup>29</sup> See *Amdt 1.7.6.2 Central Hudson Test and Current Doctrine*, CONST. ANNOTATED, [https://constitution.congress.gov/browse/essay/amdt1-7-6-2/ALDE\\_00000225](https://constitution.congress.gov/browse/essay/amdt1-7-6-2/ALDE_00000225) (last visited May 10, 2025).

<sup>30</sup> See *Amdt 1.7.14.1 Overview of Compelled Speech*, CONST. ANNOTATED, [https://constitution.congress.gov/browse/essay/amdt1-7-14-1/ALDE\\_00000769](https://constitution.congress.gov/browse/essay/amdt1-7-14-1/ALDE_00000769) (last visited May 10, 2025).

may fall outside the scope of the First Amendment.<sup>31</sup> However, if it found to target protected speech—including expressive or symbolic conduct—the First Amendment would be implicated.<sup>32</sup> In that case, the system’s constitutionality would depend on what level of scrutiny the court applies.<sup>33</sup>

### **a) Commercial Speech**

Commercial speech is speech that “proposes a commercial transaction and occurs in an area traditionally subject to government regulation.”<sup>34</sup> Under commercial speech doctrine, a commercial speech restriction directed at non-misleading speech and concerning a lawful activity typically receives intermediate scrutiny because the Supreme Court is generally more lenient toward regulations implicating commercial speech than those pertaining to other forms of First Amendment protected speech.<sup>35</sup>

A commercial speech challenge to the DROP system would likely raise two main arguments: 1) that the data collected is factual information that, under *Sorrell v. IMS Health*, constitutes commercial speech,<sup>36</sup> and 2) that regulations like the Delete Act, which facilitate the deletion of personal information through the DROP system, effectively impose censorship on that commercial speech.<sup>37</sup>

These arguments were raised in 2018, when the trade association SIIA contended that the CCPA violated the First Amendment by restricting the dissemination of information by allowing consumers to stop first-party sales of their personal data.<sup>38</sup> SIIA argued that the CCPA is (A)

---

<sup>31</sup> See *Wisconsin v. Mitchell*, 508 U.S. 476, 484 (1993); see also *United States v. O’Brien*, 391 U.S. 367 (1968) (holding that symbolic speech may be protected by the First Amendment but disaggregating this conduct into its expressive and non-expressive elements).

<sup>32</sup> See, e.g., Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014) (arguing that data is speech and thus data privacy laws should be subject to First Amendment scrutiny).

<sup>33</sup> See Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VANDERBILT L. REV. 793 (2006) (finding that “30 percent of all applications of strict scrutiny—nearly one in three—result in the challenged law being upheld. Rather than “fatal in fact,” strict scrutiny is survivable in fact.”).

<sup>34</sup> *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y.*, 447 U.S. 557, 561 (1980); see also *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66 (1983) (defining commercial speech as “speech which does no more than propose a commercial transaction”).

<sup>35</sup> See generally VICTORIA L. KILLION, CONG. RSCH. SERV., IF 11072, *THE FIRST AMENDMENT: CATEGORIES OF SPEECH*, (2024); Jonathan H. Adler, *Compelled Commercial Speech and the Consumer Right to Know*, 58 ARIZ. L. REV. 421 (2016).

<sup>36</sup> *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653, 2660–61 (2011). In dicta, the Court recognized that because prescriber-identifying data used in marketing and advertisements is a form of factual information, there is “a strong argument that prescriber-identifying information is speech for First Amendment purposes” but stopped short of saying that data is speech. *Id.* at 580–603. Accordingly, the exact application of *Sorrell* to data privacy laws like the Delete Act remains an open question. For a more in-depth discussion of *Sorrell* and its implications on privacy law, see Molly Cinnamon, *You Have the Right to Be Deleted: First Amendment Challenges to Data Broker Deletion Laws*, 9 GEO. L. TECH. REV. 16 (Sept. 09, 2024).

<sup>37</sup> See Bambauer, *supra* note 32.

<sup>38</sup> Memorandum from Mayer Brown on the Invalidity of the CCPA Under the First Amendment to SIIA, at 1, 4 (Jan. 24, 2019), <https://fisd.net/wp-content/uploads/2021/06/Memo-re-CCPA-FINAL.pdf> (arguing that the CCPA should be evaluated under strict scrutiny because “a business that publishes and sells information for use by other businesses is



content-based regulation because, by prohibiting the sale of an opted-out individual's data, it forecloses all forums for disseminating this information, and (B) speaker-discriminatory because it "selectively burdens the speech of a subset of businesses that maintain and sell personal information."<sup>39</sup>

Although the CCPA was amended to address some of SIIA's concerns, data brokers could revisit these arguments to challenge the Agency's implementation of the DROP system. Data brokers are likely to argue that because the law only applies to data brokers and not others who are similarly situated (platforms, advertisers, or publishers, for example), the system is speaker-discriminatory.<sup>40</sup> However, not all speaker-based distinctions are unconstitutional. Courts have recognized that the government may regulate different speakers differently when the distinction is based on the speaker's function, role, or context.<sup>41</sup> The Agency could argue that data brokers present a unique risk because they trade in information without consumer awareness or consent, unlike first-party data collectors. Thus, the Delete Act and the DROP system draw nuanced distinctions based on the role data brokers play in the data economy, and this regulatory tailoring is justified based on brokers' indirect data relationships with consumers and the harms they impose.

To assess whether a law survives intermediate scrutiny, courts typically apply the commercial speech test established in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.<sup>42</sup> Under the *Central Hudson* test, a court finds speech commercial if: [1] the speech concerns lawful activity and is not misleading; [2] the government interest asserted is substantial; [3] the regulation directly advances that interest; and [4] the regulation is no more extensive than necessary to serve that interest.<sup>43</sup> While scholars continue to debate whether most privacy legislation constitutes a First Amendment violation post-*Sorrell*,<sup>44</sup> lower courts have read

---

producing an information-based product, but that speech is not in the nature of advertising and does not qualify as "commercial speech.").

<sup>39</sup> *Id.*

<sup>40</sup> A First Amendment challenge on the basis of speaker-discrimination will likely rely on the court's decision in *Citizens United v. FEC*. 558 U.S. 310, 394 (2010) ("Prohibited, too, are restrictions distinguishing among different speakers, allowing speech by some but not others. . . . Quite apart from the purpose or effect of regulating content, moreover, the Government may commit a constitutional wrong when by law it identifies certain preferred speakers.").

<sup>41</sup> *Zauderer v. Office of Disciplinary Counsel*, for example, upheld rules requiring attorneys to include certain disclosures in their advertising. 471 U.S. 626 (1985) ("Because the extension of First Amendment protection to commercial speech is justified principally by the value to consumers of the information such speech provides, [the state] retains the right to require commercial speakers to disclose factual information."). See also *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622 (1994) ("*Turner I*") (upholding "must-carry" rules that applied only to cable operators); see also *National Association of Manufacturers v. SEC* (D.C. Cir. 2015) (reaffirming that speaker-based rules can be valid under *Zauderer* if the disclosure is factual, uncontroversial, and tied to commercial activity).

<sup>42</sup> 447 U.S. 557 (1980).

<sup>43</sup> *Id.*

<sup>44</sup> Compare Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (arguing that the commercial speech and speech on matters of private concern doctrines were "a poor fit for privacy laws" and concluding that it would not be possible to create information privacy rules that can withstand the First Amendment's scrutiny test) and Bambauer, *supra* note 32 with Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005) and Paul M.

*Sorrell* as limited to its specific facts and determined *Central Hudson* is still good law.<sup>45</sup> In fact, in the years since *Sorrell*, many limitations on sharing of commercial data in the U.S. have successfully survived First Amendment challenges.<sup>46</sup>

The DROP Tool is also likely to survive intermediate scrutiny. In enacting the Delete Act and creating the framework for the DROP Tool, the California legislature explicitly aimed to a) advance consumer privacy and b) protect against the downstream harms of inadequate digital privacy, including harassment, discrimination, identity theft, and financial exploitation.<sup>47</sup> Courts and constitutional scholars have long recognized privacy as a substantial government interest.<sup>48</sup> By offering consumers a means to limit the availability of their sensitive personal data online, as well as help regulators and consumers ensure compliance with deletion and opt-out rights, the DROP system directly addresses these aims.

One area of potential compelled speech challenge, for example, pertains to the affirmative reporting requirements, including the annual registration and disclosure requirement,<sup>49</sup> the public disclosure of consumer request metrics,<sup>50</sup> and the required reports from the triannual independent third-party audits.<sup>51</sup> To answer such a challenge, the Agency could argue that these affirmative reporting requirements serve three important government interests: 1) protecting consumer privacy, 2) ensuring transparency and accountability in how data brokers collect, use, and share

---

Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

<sup>45</sup> See KILLION, *supra* note 35; see also G.S. Hans, *No Exit: Ten Years of 'Privacy vs. Speech' Post-Sorrell*, 65 WASH. U. J. OF L. & POL'Y 20 (2021); see also Adler, *supra* note 35 at 425; see also Evan Enzer, *Privacy Laws and Strict Scrutiny*, CAL. LAWS. ASS'N, <https://calawyers.org/privacy-law/privacy-laws-and-strict-scrutiny> (last visited May 10, 2025). For a timeline of cases showing the evolution of commercial speech doctrine, see Robert Post, Coleen Klasmeier, Jane Bambauer & Joel Kurtzberg, *Commercial Speech Post-NIFLA v. Becerra: Legitimate Check on Compelled Speech or Weaponization of the First Amendment?*, YALE L. SCH.'S ABRAMS INST. FOR FREEDOM OF SPEECH (June 3, 2019).

<sup>46</sup> See *King v. Gen. Info. Servs., Inc.*, 903 F. Supp. 2d 303 (E.D. Pa. 2012) (upholding the Fair Credit Reporting Act (FCRA) which restricts consumer reporting agencies from reporting any "adverse items of information" about a consumer); *Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427 (S.D.N.Y. 2016) (upholding the Video Rental Privacy Act (VRPA)); *ACA Connects v. Frey*, 471 F. Supp. 3d 318, 318 (D. Me. 2020) (Upholding Maine's Act to Protect the Privacy of Online Customer Information, which requires ISPs to obtain approval from customers before selling their data); *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452, at \*1 (Ill. Cir. Ct. Aug. 27, 2021) (upholding Illinois' Biometric Information Privacy Act (BIPA), which prohibits collecting biometric data without subject consent); *Saunders v. Hearst Television, Inc.*, No. 23-CV-10998-RGS, 2024 WL 126186, at \*1-2 (D. Mass. Jan. 11, 2024) (upholding the Video Privacy Protection Act (VPPA) which limits distributors of prerecorded media from disclosing consumer information to third parties). See Hans, *supra* note 45; see also Cinnamon, *supra* note 36.

<sup>47</sup> See SB-362, Sen. Jud. Com. Rep., 2023-2024 Reg. Sess., at 11 (Cal. Apr. 22, 2023); see also Cinnamon, *supra* note 36, at 36.

<sup>48</sup> See Scott Skinner-Thompson, *Privacy Isn't in the Constitution, But It Is Everywhere in Constitutional Law*, THE CONVERSATION (June 15, 2022), <https://theconversation.com/privacy-isnt-in-the-constitution-but-its-everywhere-in-constitutional-law-183204> ("[T]hough the word isn't in the Constitution, privacy is the foundation of many constitutional protections for our most important, sensitive and intimate activities.").

<sup>49</sup> § 1798.99.85(b).

<sup>50</sup> § 1798.99.85(a)(1)(C); § 1798.99.86(c)(1)(C).

<sup>51</sup> § 1798.99.86(e)(2).

personal data, and 3) empowering consumers to exercise control over their information, especially sensitive data like geolocation or health data.

The Agency could further argue that the Delete Act and the DROP system are substantially related to achieving all three interests. The Delete Act and the DROP system both avoid blanket bans or speech restrictions and focus on transparency, not content suppression. As the above content restrictions require disclosure of factual and uncontroversial information, the Agency could argue that they are transparency- and disclosure-based rather than speech-restrictive. Accordingly, courts may be more likely to find them permissible.<sup>52</sup> Given the substantial government interests in privacy protection, transparency, and accountability and that the Delete Act is narrowly tailored to serve those interests, the regulation is likely to survive intermediate scrutiny.

It is worth noting that in recent years, the U.S. Supreme Court has seemed open to applying heightened scrutiny to laws that treat commercial speech less favorably based on the content of that speech.<sup>53</sup> Under such inquiry, regulations that do not depend on who is speaking or what is being expressed would be deemed speaker- and content-neutral and be assessed under intermediate scrutiny,<sup>54</sup> but content-based, speaker-based, or viewpoint-based regulations would be subject to strict scrutiny, the highest form of judicial review.<sup>55</sup> To date, only the Sixth Circuit has explicitly applied strict scrutiny to a commercial speech case.<sup>56</sup> However, this debate was at the center of Clearview AI's argument in the 2020 case *ACLU v. Clearview AI, Inc.*,<sup>57</sup> and the Ninth Circuit recently applied strict scrutiny in a limited way to the DPIA report requirement of the California Age-Appropriate Design Code Act (CAADCA) in *NetChoice, LLC v. Bonta*.<sup>58</sup> As courts have found privacy to be a substantial governmental interest, but not a compelling government interest, it is likely that the DROP system would not survive strict scrutiny if deemed content- or speaker-based speech.

---

<sup>52</sup> See *Zauderer v. Off. Disciplinary Counsel*, 471 U.S. 626, 651 (1985) (holding compelled disclosure in advertising speech permissible where the compelled disclosures were of factual and uncontroversial information, were reasonably related to an adequate government interest, and were not unjustified or unduly burdensome). However, it is worth noting that, to date, courts disagree over whether *Zauderer* applies outside advertising disclosures. See KILLION, *supra* note 35.

<sup>53</sup> Skinner-Thompson, *supra* note 48.

<sup>54</sup> *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452, at \*7 (Ill. Cir. Ct. Aug. 27, 2021) (rejecting the argument that Illinois' BIPA law, which limits biometric data collection, was content-based regulation and reasoning that "[i]f BIPA regulated, say, capture of faceprints of people yelling but not faceprints of people smiling, that would be a content-based distinction. BIPA does nothing of the sort.>").

<sup>55</sup> For an example of the arguments made for importing strict scrutiny into commercial speech doctrine, see Nat Stern & Mark Joseph Stern, *Advancing an Adaptive Standard of Strict Scrutiny for Content-Based Commercial Speech Regulation*, 47 UNIV. OF RICHMOND L. REV. 1171 (2012).

<sup>56</sup> See *International Outdoor, Inc. v. City of Troy, Mich.*, No. 19-1399 (6th Cir. 2020) (vacating the dismissal of the claim that the City of Troy, Michigan's sign ordinance imposed content-based restrictions without a compelling government interest and remanded this issue for reconsideration under the strict scrutiny).

<sup>57</sup> *ACLU v. Clearview AI, Inc.*, 2021 WL 4164452, at 9.

<sup>58</sup> See *NetChoice, LLC v. Bonta*, 113 F.4th. 1101, 1121 (9th Cir. 2024) (holding that the DPIA report requirement of the California Age-Appropriate Design Code Act (CAADCA) was content-based regulation that warranted strict scrutiny).

Given these recent developments, as well as the current Supreme Court's propensity for overturning precedent<sup>59</sup> and the difficulty of regulations in overcoming strict scrutiny,<sup>60</sup> it is important that the Agency be prepared in case of a potential shift in commercial speech jurisprudence. Moreover, we recommend that the Agency ensure that the DROP system's design, implementation, and related rulemaking are not content-based, speaker-discriminatory, or viewpoint-based, reducing the danger that a court subjects the Delete Act and related DROP regulations to strict scrutiny review.

### **b) Compelled Speech**

If the DROP system compels data brokers to delete certain types of data from their records or systems, data brokers may argue that this "deletion" constitutes a form of compelled expression or speech that is proscribed by the First Amendment's compelled speech doctrine.<sup>61</sup>

Under the compelled speech doctrine, the First Amendment applies when the government seeks to compel speech just as much as when it seeks to restrict speech.<sup>62</sup> While the Delete Act does not directly mandate that companies express or suppress a viewpoint, data brokers could argue that requiring the deletion of specific data using the DROP system either a) imposes a form of "silence" on their commercial speech, or b) forces them to "speak" indirectly by preventing the data's use for targeted advertising, marketing, or other forms of commercial speech. In other words, by restricting the use or dissemination of particular data, the DROP system could be seen as compelling expression and limiting data brokers' abilities to communicate freely or engage in commercial speech that is central to their operations.<sup>63</sup>

The Agency could respond by arguing that the compelled speech doctrine does not apply in this case because the deletion of data via the DROP system is not compelling the data broker to speak or express a message, but rather regulating their commercial conduct—the use and handling of consumers' personal data. It is a regulatory action to control the use of data for a particular purpose (e.g., preventing targeted ads, marketing, etc.). Such action may be comparable to the disclosure of certain information (such as labeling requirements on products) or restrictions on the

---

<sup>59</sup> See, e.g., *Loper Bright Enterprises, et al. v. Raimondo*, 603 U.S. \_\_\_\_ (2024) (overruling Chevron deference); see also *Dobbs v. Jackson Women's Health Org.*, 142 S. Ct. 2228 (2022) (overturning *Roe v. Wade*, 410 U.S. 113 (1973), and *Planned Parenthood of Se. P.A. v. Casey*, 505 U.S. 833 (1992)).

<sup>60</sup> See Winkler, *supra* note 33, at 793 (finding that "[o]verall, 30 percent of all applications of strict scrutiny—nearly one in three—result in the challenged law being upheld. Rather than "fatal in fact," strict scrutiny is survivable in fact.").

<sup>61</sup> For a discussion of compelled speech doctrine, see Jennifer M. Keighley, *Can You Handle the Truth? Compelled Commercial Speech and the First Amendment*, 15 J. CONST. L. 539 (2012).

<sup>62</sup> See *United States v. United Foods, Inc.*, 533 U.S. 405, 410 (2001) ("Just as the First Amendment may prevent the government from prohibiting speech, the Amendment may prevent the government from compelling individuals to express certain views."); see also *Riley v. Nat'l Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781, 796–97 (1988) ("There is certainly some difference between compelled speech and compelled silence, but in the context of protected speech, the difference is without constitutional significance, for the First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what *not* to say.").

<sup>63</sup> For more information on compelled commercial speech, see Robert Post, *Compelled Commercial Speech*, 117 W.VA. L. REV. 867 (2015) and Adler, *supra* note 35. See also Caroline Mala Corbin, *Compelled Disclosures*, 65 ALA. L. REV. 1277, 1293 (2014) ("[C]ompelled speech might actually *chill speech*").

use of specific materials (such as hazardous substances). In these cases, businesses are not compelled to speak; they are simply required to alter or limit their practices in ways that align with public policy objectives, like consumer protection.

## 2. Potential Dormant Commerce Clause Issues

Another potential legal challenge to the Delete Act and its DROP system is that it could impose an undue burden on interstate commerce, particularly for businesses that operate across state lines.<sup>64</sup> If, for example, the DROP system applies to businesses located outside California but handling data related to California residents, data brokers could argue that this broad application—affecting companies that do business across state lines or internationally—amounts to an unconstitutional extraterritorial reach, which states are generally prohibited from regulating under the dormant Commerce Clause.<sup>65</sup> If the Delete Act imposes regulations that disproportionately affect out-of-state businesses—such as stricter data deletion requirements or inconsistent regulatory frameworks—those businesses could raise a dormant Commerce Clause challenge.<sup>66</sup>

Their argument could follow that, as more states move to enact their own versions of data deletion laws, businesses would need to tailor their operations to meet a variety of different standards in every state where they operate.<sup>67</sup> The Delete Act’s mandating data deletion and the DROP system regulations could result in significant compliance costs, making it difficult for businesses to operate efficiently across state borders. This could “gravely burden” such entities,<sup>68</sup> disrupt interstate commerce,<sup>69</sup> and create substantial regulatory burdens.<sup>70</sup>

Another potential future Commerce Clause challenge is that the Delete Act may conflict with or preempt federal laws.<sup>71</sup> If Congress enacts nationwide privacy standards, companies could argue that the Delete Act and the DROP system overreaches the state’s authority by creating

---

<sup>64</sup> For examples of cases the Supreme Court has struck down in violation of the Commerce Clause, see *Granholm v. Heald*, 544 U.S. 460, 489 (2005) (holding that state laws regulating alcohol distribution violated the Commerce Clause by restricting out-of-state commerce) and *Comcast Corp. v. Behrend*, 133 S. Ct. 1426 (2013) (emphasizing that laws affecting interstate commerce must not impose unnecessary burdens).

<sup>65</sup> See Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 TEXAS L. REV. 1083 (June 21, 2022); see also Ayesha Rasheed, *Dormant Commerce Clause Constraints on Social Media Regulation*, 25 YALE J.L. & TECH SPECIAL ISSUE 101 (2023).

<sup>66</sup> See Kiran K. Jeevanjee, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California’s CCPA From Setting National Privacy Law*, 70 AM. U. L. REV. F. 75 (2020); see also *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989) (holding a state law per se invalid if it “controls commerce occurring wholly outside the boundaries” of the enacting state).

<sup>67</sup> Scott Clark, *The State of Consumer Data Privacy Legislation in 2025*, CMSWIRE (Mar. 3, 2025), <https://www.cmswire.com/customer-experience/examining-the-current-state-of-consumer-data-privacy-legislation>.

<sup>68</sup> See Goldsmith & Volokh, *supra* note 65.

<sup>69</sup> See Jennifer Huddleston & Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*, FEDERALIST SOC’Y REGUL. TRANSPARENCY PROJ. (Dec. 19, 2019), <https://rtp.fedsoc.org/paper/potential-constitutional-conflicts-in-state-and-local-data-privacy-regulations>.

<sup>70</sup> *Id.*; Goldsmith & Volokh, *supra* note 65.

<sup>71</sup> In cases like *Gonzales v. Raich*, the Supreme Court has upheld federal preemption of state laws when they interfered with interstate commerce. 545 U.S. 1 (2005).

inconsistent regulations that disrupt national data privacy standards, thereby hindering interstate commerce. Were such a national privacy law to be enacted, businesses might contend that state laws like the Delete Act, and by extension the DROP system, must yield to federal standards.

## **VI. Conclusion**

For the DROP system to be most effective, the tool must be easy to use and built around the everyday consumer's online experiences. Consumers should be able to quickly understand their rights, act without getting stuck in legal or technical complexity, and feel confident that their deletion requests are truly being honored. At the same time, data brokers must clearly understand what is expected of them and face tangible consequences for noncompliance. Strong enforcement, transparent communication, and a focus on usability will be key to the DROP system's success.

We offer the above recommendations and proposed regulation language in hopes that these humble contributions can help advance the DROP system's efficacy as a groundbreaking, dynamic intervention in our often-frustrating, lacking data protection landscape. The DROP system has the potential to be more than a mere technical platform. It is a chance to build public trust, demonstrate that privacy rights have teeth, and reaffirm California's global leadership in protecting peoples' data online to empower them more offline.

Sincerely,

A black rectangular box redacting the signature of Melodi Dinger.

Melodi Dinger

Lecturer-in-Law, Information Policy Lab

Affiliated Fellow, UCLA Institute for Technology, Law & Policy (ITLP)



**Grenda, Rianna@CPPA**

---

**From:** Lindsey Stewart <lindsey.stewart@zoominfo.com>  
**Sent:** Tuesday, June 10, 2025 7:50 AM  
**To:** Regulations@CPPA  
**Cc:** Bubba Nunnery  
**Subject:** Public Comment on Accessible Deletion Mechanism  
**Attachments:** ZI CPPA Comments 6.10.25.docx.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Attached are ZoomInfo's comments for the Accessible Deletion Mechanism.

Thank you for your consideration and this opportunity.

Lindsey

--

**Lindsey Stewart** (she/her/hers), CIPP/US  
**Senior Director, Government and Regulatory Affairs**  
**M:** [REDACTED]  
**E:** [lindsey.stewart@zoominfo.com](mailto:lindsey.stewart@zoominfo.com)  
[zoominfo.com](https://zoominfo.com)



June 10, 2025

California Privacy Protection Agency  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Dear California Privacy Protection Agency,

ZoomInfo is a software and data company that provides information for business-to-business sales, recruiting, and marketing. We support consumer privacy rights and believe that, in large part due to the work of this Agency, we are on the path to developing a healthy privacy framework for the State of California (and beyond).

We are grateful for the opportunity to submit these comments as part of the rulemaking process on the Data Rights of Californians on Online Platforms (DROP) regulations, and submit the following comments:

### **1. Notice and Choice about Potential Consequential Business Actions**

When a business owner submits a deletion request through California's DROP system, they likely have a specific context in mind: removing their personal data from consumer-focused databases that track shopping habits, demographic information, or household details. However, they may not fully consider the broader implications for their professional presence across various business databases. An opt-out in this instance could result in harm to a business owner's commercial interests, marketplace visibility, and economic opportunities—all without their awareness or informed consent. To address this important issue, we propose including the following to the Delete Act Rules:

**(a) Provide targeted deletion options for those that may want their business information removed from professional databases:**

- **Personal/household information only**
- **Professional/business information only**
- **Both categories**

**(b) Provide notice on the consumer facing DROP webpage where users are requesting opt-outs by warning users that "This deletion may affect your visibility in professional databases."**

**(c) Provide Post-Deletion Protection for consumers by notifying individuals when professional information is removed, with simple restoration options for unintended deletions.**

## 2. "Matched Identifiers" Definition

While we appreciate the DROP system's approach to implementing the Delete Act, the current regulations would benefit from clearer definitions around "matched identifiers." Specifically, the rules don't explicitly state whether a name alone constitutes sufficient identification for various deletion purposes.

This creates practical challenges. Many names are common and non-unique, potentially resulting in incorrect consumer identification and unintended data removal. Without clear guidance, businesses may interpret matching requirements differently, leading to inconsistent deletion outcomes across the industry. These definitional gaps could undermine consumer privacy goals and legitimate business operations.

Overly broad matching could remove data belonging to different individuals, while overly narrow matching might fail to fulfill valid requests. To that end, we recommend establishing a comprehensive definition of "matched identifier" that specifies the minimum data elements required for accurate consumer identification. This would provide clear compliance guidance while ensuring deletion requests are fulfilled accurately and completely. We propose the following:

**"Matched Identifier" means an exact first and last name match combined with one of the following identical identifiers in both the consumer deletion list and a data broker's data set:**

- **Complete email address**
- **Complete direct telephone number with area code**
- **Government-issued identification number**
- **Complete postal address (street number/name, city, state, ZIP)**

## 4. Multiple Match Opt-Out Definition

The proposed DROP regulations state: "If the data broker associates multiple consumers with a matched identifier from the consumer deletion list, the data broker must opt each associated consumer out of the sale or sharing of their personal information."

This provision needs further definition to identify what precisely is included as a multiple-person match. For example, a 200-person real estate firm that uses a central reception line that appears in the professional profiles of all realtors could face a situation where a single deletion request matching this phone number would result in every company employee being removed from professional databases, regardless of their individual preferences.

We propose the following addition to the definition of "Personal information

June 10, 2025

associated with a matched identifier." We believe this language both honors the state's requirement to process opt-out requests even when consumer identity cannot be fully verified, while also putting in place reasonable boundaries to prevent unintended opt-outs:

"Personal information associated with a matched identifier" means any personal information maintained in a data broker's records collected from a source other than directly from the consumer through a "first party" interaction. This does not include personal information that is subject to applicable exemptions, but includes inferences made from the personal information. **Non-specific identifiers that correspond to large numbers of consumers shall not constitute a partial match, including: (A) a first name and last name alone or (B) a business phone number alone when associated with more than ten consumers.**

Thank you for your consideration. Please feel free to contact me if you have any questions.

Sincerely,

Bubba Nunnery  
Vice-President, Government and Regulatory Affairs  
ZoomInfo  
bubba.nunnery@zoominfo.com

