

Grenda, Rianna@CPPA

From: Monticollo, Allaire <AMMonticollo@Venable.com>
Sent: Monday, August 18, 2025 1:14 PM
To: Regulations@CPPA
Cc: Christopher Oswald; Signorelli, Michael A.
Subject: Public Comment on Accessible Deletion Mechanism – Advertising Trade Associations
Attachments: Joint Ad Trade Comments - Public Comment on Accessible Deletion Mechanism (August 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 in response to the CPPA's July 31, 2025 request for comment on its modifications to the text of the proposed regulations to implement an accessible deletion mechanism under the California Delete Act: the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, 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.

Best Regards,
Allaire Monticollo

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



August 18, 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 modifications to the proposed regulations to develop and deploy the Delete Request and Opt-Out Platform (“DROP”) under the California Delete Act.¹ 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 appreciate and agree with the Agency’s decision to remove the data matching standards as previously proposed in Section 7613(a)(2)(A) of the regulations. Removing this matching requirement will help align the DROP with consumer expectations and avoid overly broad execution of deletion requests. That said, in this comment we renew several points we raised in our prior comment to the Agency on June 10, 2025.² This submission incorporates that prior comment by reference, including our comments on the overly broad definition of “direct relationship,” which will draw many more entities into the scope of the statutorily defined term “data broker”; the need for verification of requests submitted by authorized agents; issues related to “standardizing” database architecture; and potential data security concerns associated with the DROP. As our prior comment explained, these and other aspects of the proposed regulations raise significant constitutional and statutory issues.

In addition to our renewed request, we offer the following comments to reiterate key points from our previous submission related to authorized agent verification and database standardization and to raise additional issues created by the new modifications to the proposed rules. Our primary concern is that the proposed regulations would override the CCPA’s robust verification safeguards in favor of an overly broad “matching” standard—one that conflicts with statutory and regulatory requirements and undermines the State’s goal of protecting consumers from privacy harms while respecting their rights and freedoms. Furthermore, it runs counter to the State’s goals of protecting

¹ See *Notice of Modifications to Text of Proposed Regulations – Accessible Deletion Mechanism*, CALIFORNIA PRIVACY PROTECTION AGENCY BOARD (July 31, 2025), located [here](#); see also *Modified Text of Proposed Regulations – Data Broker Registration and Accessible Deletion Mechanism*, CALIFORNIA PRIVACY PROTECTION AGENCY BOARD (July 31, 2025), located [here](#); California Delete Act, SB 362 (Reg. Sess. 2023) (codified at Cal. Civ. Code §§ 1798.99.80 – 1798.99.89), located [here](#).

² See Joint Ad Trades – Public Comment on Accessible Deletion Mechanism at 7–15 (June 10, 2025), located [here](#).

consumers from privacy harms and respecting the rights and freedoms of consumers. More specifically, we ask the Agency to address three areas before finalizing the regulations: (1) the lack of agent authentication provisions in the DROP; (2) the hashing algorithm and database standardization mandates; and (3) the requirement for data brokers to save and maintain consumer deletion lists.

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 2024.³ By one estimate, over 1.8 million jobs in California are related to the ad-subsidized Internet.⁴ 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 lack of authorized agent provisions in the proposal will result in unauthorized data deletion and raise constitutional and statutory concerns.

The Agency's modifications to the proposed rules still lack authentication measures that ensure verification of agents' authority to submit DROP requests on behalf of California residents.⁵ Although the updated proposal would require the CPPA to verify a requestor's California residency,⁶ the proposal would prohibit data brokers from contacting requestors to verify deletion requests submitted through the DROP, a result that puts the proposal in conflict with the Delete Act and the California Consumer Privacy Act ("CCPA") regulations. The proposal continues to raise significant constitutional concerns given the interplay between the lack of verification safeguards and the DROP's mass deletion mechanism.

The proposed regulations not only decline to incorporate reasonable agent verification mechanisms; they also prohibit data brokers from contacting consumers to verify their requests. For these reasons, the proposed regulations arguably conflict with existing law and violate the California Administrative Procedure Act.⁷ The Delete Act permits a consumer's authorized agents to aid in a deletion request.⁸ Under the Delete Act, an "authorized agent" is defined by reference to the CCPA regulations, which provide that such an agent is a person the consumer "*has authorized*

³ 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.

⁴ *Id.* at 130–32.

⁵ Cal. Code Regs. tit. 11, §§ 7620(b), 7621 (proposed).

⁶ *Id.* § 7620(a), 7621(a) (proposed).

⁷ See *Assoc. Gen. Contractors of Ca., Inc. v. Dep't of Indus. Rels.*, 108 Cal. App. 5th 243, 263–64 (2025) (regulations must be "consistent with the governing law" and "'within the scope of authority conferred' on the agency by the enabling statute" (citation omitted)).

⁸ Cal. Civ. Code § 1798.99.86(b)(8).

to act on their behalf subject to the requirements set forth” in the regulations.⁹ Those regulations expressly permit businesses to verify agents’ authority to act.¹⁰ If a consumer uses an agent to submit a deletion request to a business, the business may require the agent to provide signed proof that the consumer gave the agent permission to submit the request and ask the consumer directly to confirm their identity with the business or confirm that they granted the agent permission to make the request.¹¹

The Agency’s proposed DROP rules conflict with the Delete Act and the CCPA regulations by expressly stating that data brokers may not contact consumers to verify their deletion requests submitted through the DROP.¹² The proposed rules would permit agents to submit requests on behalf of consumers without authorization despite the Delete Act requirements that an agent must be someone the consumer “has authorized” to make a request, and despite the CCPA regulations expressly permitting verification and confirmation from consumers that they have authorized agents to act on their behalf. This structure creates a system where deletion requests served to data brokers by agents through the DROP are subject to different rules than those submitted to businesses directly, raising inconsistency across regulatory regimes and increasing the likelihood of fraudulent requests made through the DROP.

Without authorized agent verification provisions, there will be no deterrent for purported agents to use coercive methods, manipulative processes, dark patterns, or other tactics to persuade consumers to give them authority to act or to act without the knowledge of a consumer. In addition, there will be no means to root out unscrupulous agents who use the DROP to gain a competitive advantage over data brokers with competing business models. For example, entities may assert that they are consumer agents and submit DROP requests to damage their competitors’ businesses and bolster their own position in the marketplace. While the proposed rules require agents to disclose their name, trade name, and email address, the proposed rules provide no process to allow the CCPA or data brokers themselves to validate purported agents’ authority to act. To reduce the likelihood of agent gamesmanship and data deletion that consumers did not request, the Agency should not allow agents to self-certify their authority.

The Delete Act and the proposed regulations also raise constitutional concerns.¹³ Data brokers’ processing of personal information (including sales, disclosures, and other uses of such

⁹ Cal. Code Regs. tit. 11, § 7001(d) (defining “authorized agent”) (emphasis added); Cal. Civ. Code § 1798.99.80(b) (providing that an “authorized agent” has the same meaning as under the CCPA regulations).

¹⁰ See Cal. Code Regs. tit. 11, § 7063(a).

¹¹ See *id.*

¹² Cal. Code Regs. tit. 11, § 7616(c) (proposed).

¹³ Among many other legal infirmities, the statute and the rules may violate the Contracts Clause by impeding data brokers from meeting contractual obligations to provide data-driven products and services to their customers. In addition, by mandating that data brokers delete data through the DROP, and by prohibiting the sale or sharing of any new data collected after such deletion, the Delete Act and the DROP regulations may constitute a regulatory taking in violation of the Takings Clause.

information) is protected speech under the First Amendment.¹⁴ The proposed regulations are content-based and therefore should receive heightened scrutiny. However, if finalized in their current form, the proposed rules would fail any applicable form of First Amendment scrutiny. As explained in our prior comment, among other First Amendment concerns, the regulations’ lack of verification safeguards, when combined with the mass-deletion mechanism, make the regulations more extensive than necessary to advance the State’s privacy interests because they would allow unauthorized agents to effect mass data deletion that Californians did not intend, permit, or expect.¹⁵

II. The proposed hashing algorithm and database standardization requirements are unclear, overly prescriptive, contravene the Delete Act, and run afoul of the First Amendment.

The modifications to the proposed regulations would add new hashing algorithm requirements and additional requirements for a data broker to “standardize” customer records. In particular, the new hashing algorithm requirements would create significant uncertainty and potentially result in matches to data that are *not associated* with a consumer who is requesting data deletion through the DROP—a result at odds with the Delete Act itself as well as the CCPA and its implementing regulations. In addition, the proposed standardization requirements would force data brokers to maintain data in ways that would alter or impact how they deliver their products and services to customers, creating significant operational burdens with impacts on their First Amendment Free Speech rights. Due to these concerns, the Agency should remove these requirements from the proposed regulations.

The proposed regulations to implement the DROP are acutely focused on matching identifiers in consumer deletion lists to data maintained by data brokers rather than ensuring that deletion requests are verifiable. This approach is contrary to the text of the Delete Act, which provides that the deletion mechanism “shall allow data brokers . . . to determine whether an individual has submitted a verifiable consumer request.”¹⁶ The term “verifiable consumer request” comes from the CCPA and its implementing regulations, which define “verify” in relevant part to mean “to determine that the consumer making a request to delete . . . is the consumer about whom the business has collected information.”¹⁷ The CCPA regulations require businesses to verify deletion requests, in some cases using up to three data points for verification.¹⁸ And for good reason. As both the CPPA and the California Attorney General have recognized, verification serves as a crucial safeguard against the real harm that can result from the unauthorized deletion of data or

¹⁴ *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).

¹⁵ *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”).

¹⁶ Cal. Civ. Code § 1798.99.86(b)(3).

¹⁷ Cal. Code Regs. tit. 11, § 7001(mm).

¹⁸ *Id.* § 7062(d).

the application of other rights to consumers who did not make requests.¹⁹ Indeed, by their plain text, the CCPA regulations provide that, when determining their verification processes, businesses “shall consider” factors including the “risk of harm to the consumer posed by any unauthorized deletion,” with a greater risk of harm requiring “a more stringent verification process.”²⁰

The California legislature itself has acknowledged that lack of proper verification can cause consumer harm. In enacting the Delete Act, the legislature incorporated the CCPA’s exceptions.²¹ In the CCPA, the legislature created an exception to honoring deletion and other consumer requests if doing so would “adversely affect the rights and freedoms” of other individuals.²² The same exception further provides that a verifiable deletion request “shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person.”²³ And when the legislature amended the CCPA in 2020, it clarified that requests to delete do not apply to household data,²⁴ a change intended to address what was at its core a verification problem: the concern that deletion and other rights were being effectuated to apply beyond the data of the consumer who made the request to the data of other household members who made no such request.²⁵

In sum, verifying consumer requests—determining that the requestor is who they say they are and is the person about whom data was collected—has been a central consumer safeguard built into the CCPA, the CCPA regulations, and now the Delete Act. It is a safeguard designed to protect consumers from the State-recognized harm of unauthorized deletion. However, the proposed regulations’ focus on data *matching* rather than consumer *verification* would undermine this safeguard, assuming that the mere possession of data about a person suffices for verifying that person’s identity and confirming that they are in fact the individual about whom the data broker collected data. In this respect, the proposed regulations risk applying deletion requests to data associated with consumers who did not request deletion through the DROP, and allowing submission of fraudulent deletion requests by individuals or entities purporting to be the consumer who is the subject of the request.

¹⁹ California Attorney General, *Initial Statement of Reasons for Proposed Adoption of California Consumer Privacy Act Regulations* (Oct. 11, 2019) at 32, located [here](#) (explaining the importance of verifying deletion requests and the risk of consumer harm from unauthorized deletion); California Privacy Protection Agency, *FSOR Appendix A: Summary and Response to Comments Submitted During 45-Day Comment Period* (Mar. 29, 2023) at 278–79, located [here](#) (noting that “certain businesses may require a more stringent verification pathway because of the sensitive nature of the personal information at issue”).

²⁰ Cal. Code Regs. tit. 11, § 7060(c)(3)(B).

²¹ Cal. Civ. Code § 1798.99.86(c)(2)(B).

²² *Id.* § 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.”).

²³ *Id.*

²⁴ *Id.* § 1798.145(p).

²⁵ The California Attorney General expressly acknowledged these concerns when finalizing the original CCPA regulations. *See, e.g.*, Final Statement of Reasons for Proposed Adoption of CCPA Regulations at 44–45 (Jun. 1, 2020), located [here](#) (recognizing issues with effectuating consumer rights on personal information associated with the wrong consumer in the context of households).

Below we address two aspects of the proposed regulations that reflect the focus on matching rather than mandated verification. These aspects of the proposed regulations should be removed, and the proposed regulations should be updated to emphasize consumer verification to ensure the right data is deleted and the person requesting deletion is who they say they are, as was intended by the legislature and approved by the people of California.

A. Hashing Algorithm

Under the modifications to the proposed rules, in the event a consumer deletion list includes multiple identifiers, a data broker must separately “hash each applicable identifier” in its records, “combine the multiple hashed identifiers for each consumer into a single identifier,” and then “hash the combined identifier before comparing to the consumer deletion list.”²⁶ Then, after hashing records in its own systems pursuant to these rules, the data broker must apply the hashing algorithm contained in a consumer deletion list to the combined identifier.²⁷ Because a consumer deletion list may contain one or several identifiers that could match to data associated with multiple consumers, the proposed hashing requirement has the potential to require data brokers to delete or opt out data associated with consumers who did not request deletion through the DROP.

The proposed rules lack sufficient clarity regarding the identifiers that may be included in a given consumer deletion list. “Consumer deletion list” is defined as “a list containing one or more type[s] of consumer identifiers (e.g. email address, phone number, or combination of name, date of birth, and zip code) for every consumer that has submitted a deletion request through the DROP.” Though it is ambiguous, the definition suggests that such a list *could* include name and zip code. As a result, if a data broker creates a combined hashed identifier for John Smith in zip code 95811, a deletion request served through the DROP from one John Smith with those data attributes could impact the data of *all individuals named John Smith in zip code 95811*. In this respect, the hashing algorithm requirements risk depriving data brokers of the ability to verify deletion requests, potentially resulting in the deletion of data associated with consumers who did not request deletion through the DROP. Even if data brokers characterize deletion requests that match to multiple combined identifiers as “unverified” requests, they will still be required to opt all consumer records matching to those data elements out from sales and sharing.

The proposed hashing algorithm therefore contravenes the Delete Act, the CCPA, and its implementing regulations in several respects. The regulations would prevent effective verification even though the Delete Act provides that the deletion mechanism “shall allow” data brokers to determine whether a deletion request is verifiable.²⁸ However, the proposed regulations forbid data brokers from contacting consumers to verify their deletion requests.²⁹ Moreover, should a single individual’s deletion request under the DROP lead to matches in multiple consumers’ records, multiple individuals may have their data/records deleted or opted out, unnecessarily infringing on

²⁶ Cal. Code Regs. tit. 11, § 7613(a)(2)(A) (proposed).

²⁷ *Id.*; see also *id.* § 7026(d) (proposed).

²⁸ Cal. Civ. Code § 1798.99.86(b)(3).

²⁹ Cal. Code Regs. tit. 11, § 7616(c) (proposed).

the rights and freedoms of other Californians—a result that the Delete Act and CCPA specifically forbid.³⁰

The proposed hashing algorithm also conflicts with the CCPA regulations. Under the CCPA regulations, businesses must verify consumer deletion requests to a high or reasonably high degree of certainty, which may involve matching three pieces of personal information provided by a consumer with personal information maintained by a 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.³¹ Businesses are thus given latitude to decide which data elements to request from consumers for verification. A business would likely not, for example, request name, zip code, and date of birth, as those data elements may overlap for many consumers. Even for opt-out requests, which need not be “verifiable,” businesses “may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business.”³² The proposed regulations, which provide no reasonable means to confirm the consumer’s identity and appear to assume that a request via the DROP is automatically verified and free from manipulation,³³ are consequently likely to result in an overbroad application of requests and deletion or opt outs for data that is not associated with the requesting consumer.

For these reasons, the Agency should further modify the proposed regulations to allow verification, consistent with the verification process under the CCPA regulations. Doing so avoids the conflict with the Delete Act and the CCPA and makes it less likely that data brokers will be required to delete the data of consumers whose requests cannot be verified, or to opt out these individuals from sales or sharing—potentially affecting the rights of other consumers who did not make deletion requests.³⁴

B. Database Standardization

Additionally, the proposed modifications would require data brokers to “standardize” their proprietary databases by altering the data they maintain to fit into a prescribed format. The proposed rules would require data brokers to, for example, format date of birth as a string of eight numbers, format zip-codes by removing the plus-4 code entirely (which is essential to improving product delivery accuracy and speed), and format phone numbers without dashes or country

³⁰ See Cal. Civ. Code § 1798.145(k).

³¹ Cal. Code Regs. tit. 11, § 7062(d) (emphasis added).

³² Cal. Code Regs. tit. 11, § 7026(d) (proposed).

³³ This assumption finds no support in the proposed regulations. Beyond the California residency verification requirement, the proposed regulations build no express verification requirements into the DROP. To the contrary, any additional Agency verification processes are *permissive*. Cal. Code Regs. tit. 11, § 7620(b) (proposed) (Agency “may verify” the personal information consumers provide in their deletion requests). This provision, when combined with the prohibition on data brokers contacting consumers to verify their requests, significantly heightens the concerns around unverified requests.

³⁴ *Assoc. Gen. Contractors*, 108 Cal. App. 5th at 263–64.

codes.³⁵ The proposed rules explicitly state that data brokers must implement these methods and any other standardization methods that will “increase the likelihood of a match between its records and the applicable consumer deletion list.”³⁶ In this respect, too, the proposed rules are grounded in a “matching” concept rather than true consumer verification as the Delete Act and the CCPA and its implementing regulations require.

These proposed standardization requirements will be particularly burdensome for small and mid-sized data brokers. In addition, they are likely to create new data security concerns. The proposed regulations’ prescriptive database standardization requirements will give hackers a clear understanding of how data is structured and maintained within data brokers’ systems, thereby making them susceptible to attacks and unauthorized infiltration. The proposed rules also raise First Amendment concerns.³⁷ As noted above, the requirements would mandate that data brokers alter how they compile, use, and communicate consumer data when delivering products and services—in many cases substantively, as evidenced by the requirement to remove plus-4 zip code information and country codes for telephone numbers.³⁸ The standardization requirements therefore limit data brokers’ ability to convey their desired messages to customers. Indeed, the proposed rules are expressly designed to force data brokers to change the contents of their databases to “increase the likelihood of a match” between their own records and identifiers in government-run DROP deletion lists. By mandating that data brokers materially change their proprietary datasets, the standardization requirements will impact the unique data products and services that data brokers provide to their customers.

The proposed rules purport to limit the impact of the standardization requirements by ostensibly clarifying that data brokers must standardize data only for compliance with the regulations and for no other purpose—a change apparently intended to suggest that data brokers need not maintain two separate databases for DROP compliance.³⁹ As a practical matter, however, because of the unique compilation and arrangement of their proprietary databases, data brokers would have virtually no choice but to create and maintain multiple databases. In this respect, the proposal would require data brokers to invest significant additional resources to continue exercising their First Amendment rights in the face of these regulations. To preserve their ability to communicate with customers in the manner they choose, data brokers would need to invest substantial time and resources to create and maintain multiple databases for the same information—one database that meets DROP specifications, and other databases that meet the needs of their

³⁵ *Id.* § 7613(a)(1)(A)(iii), (iv), (v) (proposed).

³⁶ *Id.* § 7613(a)(1)(A)(vi) (proposed).

³⁷ The standardization provisions also present concerns under the California APA. Fundamentally, the provisions appear to exceed the CPPA’s statutory authority, requiring data brokers to reformat their proprietary and custom databases without any specific grant of authority under the Delete Act to impose such far-reaching obligations. *See generally Assoc. Gen. Contractors*, 108 Cal. App. 5th at 265. Moreover, it is far from clear that these provisions are “reasonably necessary to effectuate the purpose” of the Delete Act. *See* Cal. Gov’t Code § 11342.2.

³⁸ *See 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).

³⁹ Cal. Code Regs. tit. 11, § 7613(a)(1)(C) (proposed).

customers, partners, or internal data teams. This result will create significant costs, particularly for small and mid-size data brokers to build and maintain new databases to comply with DROP requirements and while being able to maintain at least some of their rights to communicate with their customers in the manner they choose.

III. The proposed requirement for data brokers to save and maintain a consumer deletion list to compare to newly collected records is operationally burdensome and unnecessary.

The proposed regulations would require data brokers to save and maintain any deletion lists containing personal information that does not match to data within the data broker's records at the time of comparison.⁴⁰ The proposed rules would then require data brokers to compare any newly collected records with those past deletion lists before the new personal information is sold.⁴¹ This proposed rule introduces a manual process of comparing past deletion lists to newly collected data. In addition, the rule sets forth no reasonable end date to the requirement. A data broker who accesses the DROP for the first time in August 2026 may be required to maintain the consumer deletion lists it retrieves *in perpetuity* if the identifiers appearing on the lists are never added to the data broker's systems.

This rule is also unnecessary, because any newly collected data will be subject to deletion once a data broker accesses the DROP, which it must do by law every 45 days. This 45-day cadence for data brokers to access and effectuate deletion request through the DROP is already two times as fast as the time period in which businesses must execute deletion requests under the CCPA.⁴² Moreover, businesses that receive requests from California consumers under the CCPA are not required to save and maintain those requests for consumers they do not maintain data about in their systems. The proposed requirement for data brokers to maintain deletion lists indefinitely to compare to data that may be collected later is another example of how the proposed DROP regulations treat data brokers differently than other businesses are treated under the CCPA. The Agency should not impose an unnecessary and overly burdensome deletion list retention requirement that would treat data brokers differently than other businesses and could force data brokers to permanently maintain lists containing identifiers that may never surface in their systems.

* * *

⁴⁰ *Id.* § 7613(c) (proposed).

⁴¹ *Id.*

⁴² Cal. Civ. Code §§ 1798.130(a)(2), 1798.145(h)(1) (requiring deletion within 45 days of a verifiable consumer request, with an option to extend the compliance period by an additional 45 days for a total of 90 days to complete the request).



We thank you for the opportunity to participate in this regulatory process and 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

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
Brian Tengel, Venable LLP

Grenda, Rianna@CPPA

From: Kris Quigley <kquigley@cdiaonline.org>
Sent: Monday, August 18, 2025 2:01 PM
To: Regulations@CPPA
Subject: Public Comment on Accessible Deletion Mechanism
Attachments: August 18 2025 CPPA DROP 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

Hello

Please accept the comments on behalf of CDIA.

Thank you,
Kris

Kris Quigley
Consumer Data Industry Association
Director, Government Relations
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

August 18, 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

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.

We appreciate that the Agency considered feedback we submitted during the earlier comment round and that it has invited additional perspectives on the updated proposal. In this letter, we address:

1. The burdens created by requirements to reformat or standardize data broker records.
2. The need for deletion lists to include enough identifiers to ensure proper and accurate matching.
3. The importance of verifying consumers beyond residency checks.

We also revisit issues raised previously that remain unaddressed, such as ensuring authorized agents are properly credentialed before acting on behalf of consumers and reconciling conflicts between the California Consumer Privacy Act (CCPA) and the new DROP reporting obligations.

I. Data standardization requirements are impractical and risk reducing accuracy

The proposal would compel data brokers to reformat consumer information before comparing deletion list identifiers against their systems. Such standardization, like truncating ZIP codes to five digits, could make matches less reliable. For instance, two individuals with identical names living in different ZIP+4 areas could be misidentified as the same person.

Similarly, mandates to strip special characters, convert all text to lowercase, or otherwise restructure datasets would interfere with proprietary databases, degrade data quality, and hinder the accuracy of deletion matching. These operational burdens raise constitutional concerns as well, since they regulate how data brokers maintain and communicate information, implicating protected speech interests.

For these reasons, the standardization provisions should be removed.

II. Requirements to track unmatched identifiers create duplicative obligations

The revised rules would require brokers to continually monitor unmatched identifiers and reprocess them if those identifiers later appear in newly collected information. This effectively forces brokers to maintain shadow deletion lists already managed by the DROP system itself. Such redundancy introduces operational inefficiency, creates conflicting compliance duties with existing CCPA rules, and compels the retention of consumer identifiers that businesses may not otherwise hold.

III. Limiting standardization obligations to DROP compliance does not solve the problem

Although the modified rules clarify that standardized data need only be maintained for DROP compliance, the requirement still imposes burdensome restructuring of internal systems. Brokers must nevertheless adopt and maintain database formats dictated by regulation, diminishing their ability to organize information in ways that best serve accuracy and customer needs.

This type of compelled database formatting also raises free speech concerns, since it conditions how businesses may structure and use their data as part of their expressive and commercial activities.

IV. Deletion lists must include enough identifiers to ensure accurate matching

While the prior 50% matching rule has been removed, the current framework still risks overbroad deletions. Under the CCPA, verifying a deletion request often requires matching at least three separate identifiers to confirm the consumer's identity. In contrast, the DROP rules permit requests with only a single identifier, which could force deletion of records that do not actually belong to the requesting individual.

Moreover, the CCPA allows businesses to seek additional information from consumers when necessary to complete a request but DROP lacks such a safeguard. To prevent accidental or unauthorized deletions, the DROP rules should be harmonized with CCPA verification standards.

V. Residency checks are not sufficient consumer verification

We recognize the clarification that California residency must be verified, but verifying residency alone is insufficient. Consumers themselves should be required to confirm their identity and residency using reasonable verification methods. Without such checks, the DROP risks becoming a loophole that allows unverified or fraudulent requests to proceed, undermining the protections built into the CCPA.

VI. Verification of authorized agents is necessary

The proposed rules fail to include meaningful requirements to confirm an agent's authority to act on behalf of a consumer. By contrast, the CCPA regulations allow businesses to require written permission, direct consumer confirmation, or other reasonable methods of verifying agent authority.

Without such safeguards, DROP could be exploited by bad actors or competitors submitting unauthorized or bulk requests, distorting the market and undermining consumer trust. Aligning DROP with existing CCPA agent verification standards would mitigate these risks and avoid inconsistency with the Administrative Procedure Act.



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905
P 202 371 0910 CDIAONLINE.ORG

VII. Aligning response timelines with CCPA requirements

Finally, DROP's reporting timelines should be consistent with the CCPA. The proposed rules require brokers to update request statuses within 45 days, while the CCPA allows up to 90 days if an extension is properly invoked. Harmonization is important to avoid conflicting compliance obligations and to give businesses the same flexibility they currently have under state law.

Conclusion

We value CCPA's commitment to refining these rules and share its goal of creating a clear, fair, and workable deletion mechanism. However, the proposed requirements, particularly around standardization, verification, and reporting must be revised to align with the CCPA, safeguard consumer privacy without introducing inaccuracies, and avoid unnecessary operational and constitutional risks.

Thank you for your time and consideration. Should you have questions please contact me at kquigley@cdiaonline.org.

Sincerely,

A solid black rectangular box used to redact the handwritten signature of Kris Quigley.

Kris Quigley
Director, Government Relations

From: Craig Erickson <[REDACTED]>
Sent: Monday, August 18, 2025 2:24 PM
To: Regulations@CPPA
Subject: Public Comment on Accessible Deletion Mechanism
Attachments: CCPA Public Comment - DROP - Craig Erickson.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: regulations@cppa.ca.gov
From: Craig Erickson, a California Consumer
Subject: "Public Comment on Accessible Deletion Mechanism"
Date: August 18, 2025

SUMMARY

I am Craig Erickson, a California Consumer speaking for myself about the proposed regulations for the Data Broker Registration and the Accessible Delete Mechanism, known as the "DROP". I support the DROP as an expedient one-stop-shop to have all my personal information deleted from all registered data brokers and all their downstream service providers, contractors, and third-parties.

Unlike other consumers who simply want their data deleted, I want businesses to use my data to provide services I need and want. One business that controls my data and governs it according to my preferences is my authorized agent, PrivacyPortfolio. I authorize my agent to share my data with companies I want to engage with, and one control I use to govern my information is by deleting it when necessary. When my authorized agent invoices me for its services, I also receive a report about decisions and actions taken on my behalf, along with a status of success. I do not pay my agent to tell me they were able to get my data deleted with x number of organizations. Without proof, I won't pay.

One of the biggest issues for me is verifying that my data was deleted by every entity that is required to delete it. I map my data to organizations I share it with and then submit CCPA Requests to KNOW to enhance my profile with additional information these organizations possess. If I decide not to engage with these organizations, I know what data should be deleted and often I know where it can be found. Under the CCPA Regulations I am entitled to an acknowledgement that my data was deleted. These proposed regulations for the DROP lacks accessible verification mechanisms for consumers to verify the response status reported by registered data brokers. Unlike the CCPA Regulations, data brokers using the DROP are not required to report response status to California Consumers – in fact, under these proposed regulations data brokers are prohibited from directly contacting the consumer. This is one reason why I will authorize my agent to create and use my DROP account login in some situations, and submit CCPA Delete Requests in other situations. I need to tell my agent when to use the DROP and when to use a CCPA Request to DELETE, and it would be helpful to me if these proposed regulations offered more guidance.

A simple view is that DROP deletion requests are for regulated data brokers and CCPA Delete Requests are for all other CCPA-covered businesses. The reality is that registered data brokers' roles in a digital supply chain includes other CCPA-covered businesses who are service providers, contractors, third parties, and yes, other data brokers. Discovering and deleting personal information as required under these regulations is not a trivial task for organizations, consumers, or authorized agents representing them. I will be using the DROP as a tool for discovering which identifiers data brokers use to match requests (operations) with responses (objects). This also helps me discover non-disclosed subprocessors and third parties that have positive matches to these personal data elements in their written contract authorizations or in their data asset inventory.

My authorized agent is capable of conducting these complex tasks on my behalf, but my agent is not an attorney. No agent, business, or government agency can tell me whether any organization complies with these regulations. The California Privacy Protection Agency is prohibited from representing any individual or organization.

In light of this recognition, I've instructed my agent to make the best decision on my behalf for achieving my goals, and to help organizations find my data, limit its use, and remediate issues that negatively impact me. My right to verify facts and act according to my own judgements based on forensic evidence, audits, and assessments is not something organizations can opt-out of. When challenged, threatened, or otherwise deprived of my rights I must enforce the Agency's regulations myself by publishing formal complaints filed as evidence and disseminating it to relevant stakeholders. I do not need anyone's permission to gather evidence or to enforce my own rights, but I do need an authorized agent to do all this on my behalf and I want to do it in compliance with these proposed regulations.

My comments are directed toward the Agency, all registered data brokers including their customers and suppliers, policymakers, and the entire legal and privacy profession. I hope you'll think through your response to my actions so that when I share it with all stakeholders, they too can have a better understanding of the consequences my actions and your response may have on them.

Regarding these proposed regulations, my first priority is to keep evidence from being deleted. My second priority is knowing what was deleted, and my third priority is evaluating the consequences of these operations so I can make better informed decisions in the future. California Consumers who use the services of Authorized Agents may share some of the same concerns and questions I have about how these proposed regulations helps or hinders the capabilities of my authorized agent to create a DROP account and submit deletion requests on my behalf. In particular:

- how I must comply with these regulations as a California Consumer,
- how my authorized agent must comply with these regulations,
- how I and my authorized agent can verify the compliance status of data brokers vis à vis my personal information, and
- how these regulations may impact exercising privacy rights outside the scope of the Delete Act.

I recognize that the Agency has jurisdiction over enforcing the CPRA-amended CCPA and DELETE Act in general, and cannot represent me in a dispute and cannot provide determinations that a particular business has violated any statutes or regulations. I recognize that the Agency cannot verify any facts or statements I've reported under penalty of perjury, or reveal trade secrets of businesses. I recognize the need to enforce my rights as best I can when businesses claim that whatever authorization or consent they have to process my personal information in their written contracts with third parties is a confidential business matter they cannot disclose to me.

The remainder of my public comment (attached) identifies each itemized question or concern I have as they relate to these proposed regulations, as well as my justification of the specific needs I have regarding each item.

Sincerely,
Craig S. Erickson
A California Consumer

To: regulations@coppa.ca.gov

From: Craig Erickson, a California Consumer

Subject: "Public Comment on Accessible Deletion Mechanism"

Date: August 18, 2025

SUMMARY

I am Craig Erickson, a California Consumer speaking for myself about the proposed regulations for the Data Broker Registration and the Accessible Delete Mechanism, known as the "DROP".

I support the DROP as an expedient one-stop-shop to have all my personal information deleted from all registered data brokers and all their downstream service providers, contractors, and third-parties.

Unlike other consumers who simply want their data deleted, I want businesses to use my data to provide services I need and want. One business that controls my data and governs it according to my preferences is my authorized agent, PrivacyPortfolio. I authorize my agent to share my data with companies I want to engage with, and one control I use to govern my information is by deleting it when necessary. When my authorized agent invoices me for its services, I also receive a report about decisions and actions taken on my behalf, along with a status of success. I do not pay my agent to tell me they were able to get my data deleted with x number of organizations. Without proof, I won't pay.

One of the biggest issues for me is verifying that my data was deleted by every entity that is required to delete it. I map my data to organizations I share it with and then submit CCPA Requests to KNOW to enhance my profile with additional information these organizations possess. If I decide not to engage with these organizations, I know what data should be deleted and often I know where it can be found. Under the CCPA Regulations I am entitled to an acknowledgement that my data was deleted.

These proposed regulations for the DROP lacks accessible verification mechanisms for consumers to verify the response status reported by registered data brokers. Unlike the CCPA Regulations, data brokers using the DROP are not required to report response status to California Consumers – in fact, under these proposed regulations data brokers are prohibited from directly contacting the consumer. This is one reason why I will authorize my agent to create and use my DROP account login in some situations, and submit CCPA Delete Requests in other situations.

I need to tell my agent when to use the DROP and when to use a CCPA Request to DELETE, and it would be helpful to me if these proposed regulations offered more guidance.

The simplest view is that DROP deletion requests are for regulated data brokers and CCPA Delete Requests are for all other CCPA-covered businesses. The reality is that registered data brokers' roles in a digital supply chain includes other CCPA-covered businesses who are service providers, contractors, third parties, and yes, other data brokers.

Discovering and deleting personal information as required under these regulations is not a trivial task for organizations, consumers, or authorized agents representing them. I will be using the DROP as a tool for discovering which identifiers data brokers use to match requests (operations) with responses (objects). This also helps me discover non-disclosed subprocessors and third parties that have positive matches to these personal data elements in their written contract authorizations or in their data asset inventory.

My authorized agent is capable of conducting these complex tasks on my behalf, but my agent is not an attorney. No agent, business, or government agency can tell me whether any organization complies with these regulations. The California Privacy Protection Agency is prohibited from representing any individual or organization. In light of this recognition, I've instructed my agent to make the best decision on my behalf for achieving my goals, and to help organizations find my data, limit its use, and remediate issues that negatively impact me. My right to verify facts and act according to my own judgments based on forensic evidence, audits, and assessments is not something organizations can opt-out of. When challenged, threatened, or otherwise deprived of my rights I must enforce the Agency's regulations myself by publishing formal complaints filed as evidence and disseminating it to relevant stakeholders. I do not need anyone's permission to gather evidence or to enforce my own rights, but I do need an authorized agent to do all this on my behalf and I want to do it in compliance with these proposed regulations.

My comments are directed toward the Agency, all registered data brokers including their customers and suppliers, policymakers, and the entire legal and privacy profession. I hope you'll think through your response to my actions so that when I share it with all stakeholders, they too can have a better understanding of the consequences my actions and your response may have on them.

Regarding these proposed regulations, my first priority is to keep evidence from being deleted. My second priority is knowing what was deleted, and my third priority is evaluating the consequences of these operations so I can make better informed decisions in the future.

California Consumers who use the services of Authorized Agents may share some of the same concerns and questions I have about how these proposed regulations helps or hinders the capabilities of my authorized agent to create a DROP account and submit deletion requests on my behalf. In particular:

- how I must comply with these regulations as a California Consumer,
- how my authorized agent must comply with these regulations,
- how I and my authorized agent can effectively verify the compliance status of data brokers vis à vis my personal information, and
- how these regulations may impact exercising privacy rights outside the scope of the Delete Act.

I recognize that the Agency has jurisdiction over enforcing the CPRA-amended CCPA and DELETE Act in general, and cannot represent me in a dispute and cannot provide determinations that a particular business has violated any statutes or regulations.

I recognize that the Agency cannot verify any facts or statements I've reported under penalty of perjury, or reveal trade secrets of businesses.

I recognize the need to enforce my rights as best I can when businesses claim that whatever authorization or consent they have to process my personal information in their written contracts with third parties is a confidential business matter they cannot disclose to me.

The remainder of my public comment identifies each itemized question or concern I have as they relate to these proposed regulations, as well as my justification of the specific needs I have regarding each item.

Sincerely,

Craig S. Erickson

A California Consumer

IDENTITY, RESIDENCY, AUTHORIZATION

Item 1 What credentials and information I need to create a DROP account as a Consumer.

Need I need to know in advance what information and conditions are required to create and maintain a DROP account before my personal information is processed so I can make an informed decision about using it.

Reference § 7620. Consumer Deletion Requests. (a)

Item 2 What credentials and information my authorized agent needs to create a DROP account on my behalf.

Need My authorized agent impersonates me using my personal identifiers, email, 2FA OTPs, forwarded phone calls, text messages, and chat transcripts when creating, accessing, or deleting digital accounts. I need to know if there will be one DROP account for consumers and another for their authorized agents.

Reference § 7616. Additional Data Broker Requirements. (b); § 7610. Delete Request and Opt-out Platform Account Creation. (a) (1) (A, B)

Item 3 What documentation does the Agency accept as proof of my agent's authority to act on my behalf?

Need I need to know if my agent's notarized statement is legally sufficient to confirm their authority and withstand any challenges, especially since my Authorized Agent Consent Directive doesn't cover access to my DROP account and I can't afford an attorney.

Reference § 7621. Authorized Agents. (a)(b)

Item 4 Which organizational entity attributes are used to identify my authorized agent.

Need I need to know how to disclose the authorized agent's full name, email address, and trade name as a business through my Consumer DROP account for every authorized agent I use prior to submitting a deletion request.

I need the capability of multiple authorized agents because some specialize in OPT-OUTS and DELETES, while other authorized agents specialize in medical records or requests to KNOW, CORRECT, and LIMIT. I want data brokers to know which authorized agent to contact and how.

Reference § 7621. Authorized Agents. (a) (b); § 7616. Additional Data Broker Requirements. (c);

Item 5 Which personal data elements and authoritative sources (public records) verify my identity.

Need I need to prohibit my agent from accessing or sharing copies of my Real ID, Driver's License, and US Passport. I want to use the same personal data elements and authoritative sources that the Agency uses to verify a Consumer's identity and residency as acceptable.

Reference § 7622. Consumer Requirements to Request a Review of Residency Classification.

Item 6 Which personal data elements and authoritative sources (public records) verify my residency.

Need According to multiple disclosures of my personal data by data brokers' fulfillment of my CCPA Request to KNOW, I have residency in multiple states. I want to use the Agency's determination of residency to correct personal information and identifiers which are commonly used as a basis for decision-making – such as whether I have legal rights, engage in fraud, is eligible to receive benefits, etc.

Reference § 7622. Consumer Requirements to Request a Review of Residency Classification. (a.1), (c);

Item 7 What kind of documentation the Agency may request substantiating that I am a California resident.

Need I need to maintain my residency status by making sure the authoritative source is correct, and without inferring other information, such as “what kind of car I drive” or “which political party I associate with”. As a California Consumer who exercises my privacy rights, I am often challenged by Organizations who say they are protecting themselves from fraud.

Reference § 7622. Consumer Requirements to Request a Review of Residency Classification. (b)

Item 8 Documentation that I have had my California residency verified by the Agency prior to submitting a deletion request.

Need I need a way to push back on Organizations that make outrageous demands for specific information and documents to verify my identity and/or my residency when exercising my privacy rights through the DROP or through other means. It makes sense to me that if the Agency issues a letter validating my residency, the Agency has also successfully verified my identity, which should serve as sufficient documentation for data brokers and their third-parties.

Reference § 7622. Consumer Requirements to Request a Review of Residency Classification. (a)(1)(2); (b)(c)

Item 9 How Authorized Agents can submit requests for Residency Classification Reviews.

Need If these regulations require the Consumer to create a DROP account without the assistance of an Authorized Agent and obtain a Residency Classification prior to submitting a deletion request, the Consumer may need the assistance from an authorized agent to manage their Residency Classification Review if the process is too complicated or takes an inordinate amount of time.

Reference § 7621. Authorized Agents. (a) (b); § 7622. Consumer Requirements to Request a Review of Residency Classification. (a)

Item 10 Will the Agency notify the consumer's authorized agent in writing that the Agency has verified the consumer's residency.

Need All my correspondence via email, telephone, and email go directly to my authorized agent who forwards a filtered subset of messages to me.

Reference § 7622. Consumer Requirements to Request a Review of Residency Classification. (c)

Item 11 What authorization the agent needs to obtain from consumers to "sign truthfully under penalty of perjury" on my behalf.

Need I need to know if my agent can legally sign my name to a statement that I am providing only true and correct responses when submitting requests or additional information via the DROP.

Reference § 7602. Registration Submission Requirements. (b)

IDENTIFIERS, SUBMITTING DELETION REQUESTS

Item 12 How Consumers will submit their deletion request through the DROP.

Need I need this section to be clarified so that I know how to use DROP in a manner consistent with these regulations and with the same level of detail specified for data brokers' use of the DROP.

Reference § 7620. Consumer Deletion Requests. (a)

Item 13 How Consumers' authorized agents will submit their deletion request through the DROP.

Need I need this section to be clarified so that I can tell my agent how to use DROP in a manner consistent with these regulations and with the same level of detail specified for data brokers' use of the DROP.

Reference § 7621. Authorized Agents. (a) (b)

Item 14 Which Consumer deletion lists are accessed in the DROP, and which consumer identifiers are contained in each list.

Need To maximize the chances of returning the most consumer records for every registered data broker, I need to have identifiers in every list.

Reference § 7610. Delete Request and Opt-out Platform Account Creation. (a) (3); § 7601. Definitions. (c);

Item 15 Which identifiers each data broker uses to return the most records.

Need I need to avoid disclosing additional personal information, and handle non-unique identifiers for multiple consumers.

Reference § 7610. Delete Request and Opt-out Platform Account Creation. (a) (3) (C)

Item 16 Which personal data elements can be corrected by the Consumer.

Need To maximize the chances of returning the most consumer records for every registered data broker, I need my identifiers to be accurate in every list.

Reference § 7601. Definitions. (c);

Item 17 Which options a consumer has to correct any personal information that is not required to be deleted.

Need When a data broker misspells my first or last name in their correspondence to me as a first-party, and also sells or shares my misspelled name as a third-party, I should have the right to correct my misspelled name in first-party records so that my identifier can be associated with personal data elements that are inaccurate as well as those that are correct. This occurs frequently when email and telephone identifiers are used for accounts that are no longer active.

Reference There are no applicable regulations regarding the Consumer's Right to Correct identifiers used by data brokers to match deletion requests with their first-party and third-party records.

Item 18 When a data broker changes its consumer deletion list selection, my agent needs to be notified when the data broker begins collecting additional categories of personal information about consumers that match to identifiers under previously unselected consumer deletion lists.

Need My agent needs this information to provide its services, and event-driven push notifications are more efficient than thousands of scheduled pull queries.

Reference § 7610. Delete Request and Opt-out Platform Account Creation. (a) (3) (C)

Item 19 Because data brokers must access the DROP to download its selected consumer deletion list(s) at least once every 45 calendar days and many other requirements depend on this timing, I would need to monitor deletions every day to know when a consumers' identifier is in the deletion lists.

Need Dependencies on this timing include: (1) If a data broker's automated connection with the DROP fails; (2) After a data broker downloads each consumer deletion list for the first time, all subsequent downloads of each list will only contain new or amended consumer deletion requests received after the data broker's most recent download.

While the Agency will allow a data broker to re-download a complete consumer deletion list with all current consumer deletion requests for purposes of ensuring compliance with this Chapter, reconciling internal records, or completing the audit required by Civil Code section 1798.99.86, such requests are not allowed from consumers or their authorized agents.

Reference § 7612. Delete Request and Opt-out Platform Access. (c) (1)

Item 20 How to format personal identifier values when submitting all DELETE and OPT-OUT requests to yield the maximum number of matches.

Need To increase odds of positive matches by providing identifiers in the prescribed format.

Reference § 7613. Processing Deletion Requests. (a) (1) (A)

Item 21 Which hashing algorithm is provided in the consumer deletion list to hash the consumer personal information within the data broker's records to test that it is the same category of identifier as in the consumer deletion list.

Need To increase odds of positive matches by using the prescribed hashing algorithm.

Reference § 7613. Processing Deletion Requests. (a) (1) (B)

Item 22 Every possible combination of multiple hashed identifiers for each consumer into single identifiers for comparison with the consumer deletion list.

Need To increase odds of positive matches.

Reference § 7613. Processing Deletion Requests. (a) (2) (A)

Item 23 If the data broker cannot verify the request because multiple consumers are matched to the identifier.

Need All covered businesses including data brokers must provide to Consumers a reason for denying their privacy request. When the given reason is “could not verify identity” the Consumer has no way to challenge or remedy this, and might guess what they did wrong when there are other factors outside of their control. As currently drafted, these regulations only require a response code such as “Record not found”, making it even more challenging for a Consumer to know why their deletion request wasn’t fulfilled.

Reference § 7614. Reporting Status of Deletion Requests. (b) (2) (D)

Item 24 What if any impacts might be to a consumer who shares the same identifier with other consumers. For example, it may be abused to steal one’s identity, disrupt access to products, services, and opportunities, or steal another consumer’s personal information.

Need I need to know if my identity has been linked to another individual to protect myself from harm, and I’ll be using the DROP as a tool to help me do that.

Reference § 7614. Reporting Status of Deletion Requests. (b) (2) (B)

Item 25 The exact date and time a data broker reports the status of every deletion request received since the date and time it was previously accessed.

Need If the data broker reported status changes for the most recent new deletion requests, or amended deletion requests.

Reference § 7614. Reporting Status of Deletion Requests. (a) (1)

Item 26 (1) The transaction identifier associated with each consumer deletion request; and (2) The response code for each transaction identifier that accurately describes the action taken by the data broker with respect to the individual deletion request reported by the data broker through its DROP account.

Need The transaction identifier is my receipt proving a deletion request was made and received. The response code assigned to each transaction identifier is the Organization's receipt proving a deletion request was processed.

Reference § 7614. Reporting Status of Deletion Requests. (b) (1) (2)

Item 27 If the data broker opted out from sale or sharing all the personal information associated with all matched consumers with one identifier.

Need I need to know if another consumer sharing the same identifier as me has caused my records to be deleted or opted-out from sale so I can opt-in again using a different identifier.

Reference § 7614. Reporting Status of Deletion Requests. (b) (2) (B)

Item 28 A comprehensive asset inventory of each data broker's records of consumers' personal information to determine if PI is being withheld from searches intentionally or by accident.

Need To verify if my personal information was deleted, I need to compare my master profile with the data brokers' records, so I'll tell my agent to use the same technology vendors the data broker uses for best fit.

Reference § 7614. Reporting Status of Deletion Requests. (b) (2) (D)

Item 29 If the response status codes are 'misinterpreted' or 'misapplied'.

Need I cannot verify if my data was deleted because I will never know which response code is reported, so I will be exercising my other rights with the data brokers' third parties to help me verify fulfillment.

Reference § 7614. Reporting Status of Deletion Requests. (b) (2) (D)

Item 30 What kind of personal information Consumers may add to their deletion requests, and what if any personal information the Agency verified and at what time.

Need I need to know how I can add personal information to my deletion requests, including any constraints I should be aware of.

Reference § 7620. Consumer Deletion Requests. (b)

Item 31 How a Consumer can cancel requests and other associated processes made via their Authorized Agent after revoking the agent's authorization.

Need While I do not intend to cancel deletion requests because doing so does not benefit me in any way and is likely to cause me additional effort, I will consider this option unless the Agency has a better mechanism for me to revoke my authorized agent agreement(s) and access to my DROP account.

Reference § 7620. Consumer Deletion Requests. (d); § 7621. Authorized Agents. (c)

DELETION DATA REQUIREMENTS & EXEMPTIONS

Item 32 Which personal information is subject to applicable exemptions.

Need How completely a data broker fulfills my delete request depends on this contextual attribute.

Reference § 7601. Definitions. (i); § 7613. Processing Deletion Requests. (b) (1) (A, B); § 7614. Reporting Status of Deletion Requests. (b) (2) (C);

Item 33 What data was voluntarily submitted.

Need How completely a data broker fulfills my delete request depends on this contextual attribute.

Reference § 7601. Definitions. (d, i);

Item 34 If the Consumer has a direct, "first-party" relationship with the data broker.

Need How completely a data broker fulfills my delete request depends on this contextual attribute.

Reference § 7613. Processing Deletion Requests. (b) (1); § 7601. Definitions. (d, i);

Item 35 Which personal information attributes are considered to be ‘inferences’ made from the personal information.

Need How completely a data broker fulfills my delete request depends on this contextual attribute.

Reference § 7601. Definitions. (i);

Item 36 I need to know what data was found but was not required to be deleted.

Need To know if I was successful getting all personal data records deleted.

Reference (no reference)

Item 37 I need to know how long each personal data element or attribute was retained by the data broker to challenge violations of their own retention policies or claims that all personal information was already deleted independent of DROP pulls.

Need To gain insights into which personal data elements were deleted.

Reference (no reference)

Item 38 If the data broker is required to opt each associated consumer out of the sale or sharing of their personal information in accordance with Civil Code section 1798.99.86(c)(1)(B) and (D), and comply with subparagraph (b)(1)(B) of this section.

Need I have no way of knowing if the data broker is required to opt me out, other than my deletion request.

Reference § 7613. Processing Deletion Requests. (a) (2) (B)

Item 39 The entire set of each consumer’s personal information, including inferences based in whole or in part on personal information collected from third parties or “voluntarily submitted” from consumers in a non- “first party” capacity, that is associated with a matched identifier in the DROP.

Need To know if I was successful getting all personal data records deleted.

Reference § 7601. Definitions. (d), (i); § 7613. Processing Deletion Requests. (b) (1) (A)

Item 40 The entire set of each consumer’s personal information, including inferences based in whole or in part on personal information collected from consumers in a “first party” capacity, that is associated with a matched identifier in the DROP, so I know what personal data is not required for deletion.

Need To know if I was successful getting all personal data records deleted.

Reference § 7601. Definitions. (d), (i); § 7613. Processing Deletion Requests. (b) (1) (A)

Item 41 Which statutory exemptions a data broker invokes to use personal information maintained pursuant to this subparagraph for any other purpose.

Need I need to know if personal information was not deleted and the data broker’s reason for maintaining it.

Reference § 7613. Processing Deletion Requests. (b) (1) (B)

Item 42 Whether a data broker “misinterprets” what “delete” means, or “misrepresents” to the consumer what the law requires from data brokers, consumers, and their authorized agents.

Need CCPA-covered businesses, including data brokers, often respond to requests to KNOW, CORRECT, LIMIT, OPT-OUT, and DELETE by saying that they are adding me to their suppression list, deleting all my data, closing this as resolved, or “have complied with all applicable laws”. According to these proposed regulations, these interpretations along with other responses will now be mapped to one of four response codes: “Record deleted”, “Record opted out of sale”, “Record exempted”, or “Record not found”. These regulations do not require these responses to be shared with Consumers and their authorized agents, making it nearly impossible to know if personal information was deleted or not.

Reference § 7613. Processing Deletion Requests. (b) (1) (C)

Item 43 Whether a data broker sources personal information from another data broker, or uses another data broker to process or augment personal information “insights”, to manage potential conflicts between multiple data brokers attempting to delete consumers’ information or opt-out, including constraints on how frequently a consumer can request deletion or opt-outs.

Need Under the DROP system, I submit one deletion request on each consumer deletion list for all registered data brokers to process every 45 days. Nothing in these regulations limit when or how often I can add my identifier to each list. I will also need to do this every 45 days nine times per year to insure that my data is always deleted. “Cascading deletes” between data brokers and their third-parties present potential problems when these entities process deletion lists at different times during 45-day intervals.

Reference § 7614. Reporting Status of Deletion Requests. (a) (1)

Item 44 What personal information cannot be matched within the data broker's records at the time of comparison, that the data broker is required to save and maintain for the sole purpose of complying with Civil Code section 1798.99.86(d) to discover any newly collected records with deletion lists before new personal information is sold or shared.

Need According to the current draft, only the Agency has the right to know what personal information could not be matched because the sole purpose of complying with Civil Code section 1798.99.86(d) does not include sharing this information with Consumers or their authorized agents.

Reference § 7613. Processing Deletion Requests. (c); § 7614. Reporting Status of Deletion Requests. (a) (1)

Item 45 Which service providers and contractors a data broker requested or ordered to delete all personal information in its possession related to a consumer associated with a matched identifier in accordance with Civil Code section 1798.99.86 (c) and (d) so it could be verified.

Need I cannot verify if a data broker deleted all my personal information with third-parties if I don't know who they are, so I will be exercising my privacy rights with all third-parties I discover including their customers.

Reference § 7613. Processing Deletion Requests. (d)

SECURITY, COMPLIANCE, RESPONSIBLE PARTIES

Item 46 How to monitor authorized use of DROP.

Need a) If I authorize my agent to access my DROP account, I want to know what they're doing. b) If other consumers have matching identifiers, I might want to know if any deletion requests were made through the DROP that could impact me. c) I always want to know if a data broker uses my personal information in the DROP for unauthorized purposes.

Reference § 7610. Delete Request and Opt-out Platform Account Creation. (a) (1) (C); § 7613. Processing Deletion Requests. (a) (2) (A, B); § 7613. Processing Deletion Requests. (d, e)

Item 47 How to govern DROP information.

Need I need a degree of confidence that my authorized agent has adequate security and governance controls for DROP information. Some data protection frameworks, such as PCI-DSS require cardholder information to be stored in an isolated environment, or medical records contained within an EHR systems. My authorized agent needs the capability of deleting this information when access to the DROP account is revoked or terminated. As drafted, these regulations only apply to data brokers and not to consumers and their authorized agents.

Reference § 7615. Requirements to Stop Accessing Deletion Requests from the DROP. (a) (2)

Item 48 What responsibilities do I have as a Consumer, to keep DROP information secure and confidential, and what responsibilities does my authorized agent have? Am I responsible for everything my authorized agent does on my behalf?

Need I will know what I need when I know what I'm liable for. For example, as a user of LLMs, I am responsible for my use of AI. If I abuse it, I can be denied access – which would severely limit my opportunities in life. Using an LLM via another vendor's products and services (agent as distributor of LLM) also exposes me to risk if that vendor abuses its use of the LLM.

Reference § 7616. Additional Data Broker Requirements. (b); § 7610. Delete Request and Opt-out Platform Account Creation. (a) (1) (A, B, D)

Item 49 What authorization an Organization maintains to process the Consumer's personal information in its written contracts with third-party entities.

Need Organizations authorize other organizations to process personal data when providing services and is considered to be legally authorized to do so as controllers of personal information regardless of whether consent was given by the data subject or consumer. My agent promised to minimize unauthorized use of my personal information, which excludes a) use mandated by law; b) use consented to by consumer; c) use agreed to in written contracts such as “data processing agreements”, “non-disclosure agreements”, and master service contracts. I consider all other uses to be unauthorized, which includes written contracts I cannot verify because the parties also agreed to keep the information confidential as “trade secrets”.

Reference § 7601. Definitions. (d, i);

Item 50 Which entities, brands, and products are subject to data broker regulations.

Need I need to know if the products, services, or resources I'm accessing are from prohibited countries like Iran, Russia, North Korea, or from individuals, entities, or locations I don't like. I will use this requirement to choose these regulated products, services, or resources over others which aren't listed, as it offers some degree of consumer protection.

Reference: § 7602. Registration Submission Requirements. (a, b); § 7603. Registration Information Requirements. (a, b, c, d)

Item 51 Which internal systems process their information, and the identities of vendor-provided technologies and their sub-processors?

Need My agent needs to verify my data was deleted in all internal systems and all external systems and/or components thereof; and in some cases where investigations, audits, or subpoenas are justified, to collect testimony and evidence.

Reference § 7612. Delete Request and Opt-out Platform Access. (c) (1);

Item 52 Maintain a ledger of who accessed personal information and for which authorized purpose.

Need While one could argue that Consumers don't have legal rights to govern use of their personal information or entitlements to protect it, the "spirit of the California Consumer Privacy Act" is intended to allow consumers like me make informed decisions about the use of my personal information.

Reference § 7610. Delete Request and Opt-out Platform Account Creation. (a) (1); § 7616. Additional Data Broker Requirements. (b)

Item 53 Which authorizations are required for processing the Consumer's personal information in its written contracts with third-party entities?

Need I maintain a dataset of 682 verifiable privacy requests and responses to 646 Organizations, 419 of which are Registered Data Brokers, accompanied by 524 published sworn complaints of privacy violations, and not a single organization has provided me with *just the date* of one written contract with one of its undisclosed third-party subprocessors which could provide valuable evidence for the Chief Auditor of the CPPA.

Reference § 7616. Additional Data Broker Requirements. (b);

Item 54 Who accessed my personal information in DROP on behalf of data brokers and for which authorized purpose to test for unauthorized use.

Need One organization fulfilled my CCPA Request to KNOW with screenshots and a document containing metadata about the author, who is an undisclosed Contractor of a Staffing Agency. This practice is so common that I can only assume the worst, justifying my need to conduct my own cybersecurity audits.

Reference § 7610. Delete Request and Opt-out Platform Account Creation. (a) (1) (B)

Item 55 Which personal data elements were processed by internal systems and/or by vendor-provided technologies.

Need I need to know if my personal data was sufficiently de-identified or aggregated to confirm deletion when these methods are used by data brokers. When vendor-provided technologies are used, I need to evaluate the vendor, their solution, and how it is used and configured. When internal systems are used, I need to evaluate the code or test results. Utilizing standard practices from Vendor Risk Management and Data Privacy Impact Assessments usually satisfies these needs.

Reference § 7601. Definitions. (i, l); § 7613. Processing Deletion Requests. (b) (1) (C)

Item 56 What authorization an Organization maintains to process the Consumer's personal information in its written contracts with third-party entities with and without the Consumer's consent.

Need I cannot verify if a data broker deleted all my personal information with third-parties if I don't know who they are, so I will be exercising my privacy rights with all third-parties I discover including what written authorization includes processing my personal information.

Reference § 7613. Processing Deletion Requests. (d)

Item 57 What personal information a data broker shared with service providers and contractors as the minimum necessary to facilitate compliance with subsection (c) of this section.

Need To determine if the shared personal information exceeds the minimum necessary amount.

Reference § 7613. Processing Deletion Requests. (b) (1) (B)

Item 58 What if any impacts are to Consumers who delete or opt-out from their personal information being shared, such as loss of access to needed products, services, and other resources.

Need Being discriminated against for exercising one's privacy rights might be a rare occurrence, there is a possibility that Consumers who succeed at deleting and opting out may find themselves unrepresented in datasets used to qualify people, make policy, or train data.

Reference The Agency should consider adding a warning to Consumers that "deleting your data may have unintended consequences".

Item 59 If personal information provided by the Agency through the DROP was deleted within thirty-one (31) calendar days after completing registration for the last calendar year during which it operated as a data broker, or after it has concluded its final audit in compliance with Civil Code section 1798.99.86, for businesses ceasing their data broker activities.

Need I need to know if my personal information is no longer subject to these regulations so I can pursue other options for governing the use of my data.

Reference § 7615. Requirements to Stop Accessing Deletion Requests from the DROP. (a) (2)

Item 60 Notification of any breach of reasonable security procedures and practices appropriate to the nature of the personal information provided by the Agency, to protect such personal information from unauthorized access, destruction, use, modification, or disclosure.

Need I need to protect my personal information regardless of who controls or processes it, what legal basis it is used for, and the administrative or technical capabilities of the Organization possessing it. I understand that neither the data broker nor the Agency are required to inform me of a breach or incident related to security or privacy, and am not entitled to know the results of an Agency investigation or audit. I can only rely on my own efforts to assess the effectiveness of an Organizations' security controls. Therefore I will be asking my authorized agent to conduct cybersecurity audits on my behalf to help reduce personal risks of harm.

Reference § 7616. Additional Data Broker Requirements. (b)

Item 61 A designated method for data brokers to contact a consumers' authorized agent for any reason, to insure that data brokers do not contact consumers directly for any reason.

Need I need an out-of-band channel of communication between me, my agent, and Organizations because when situations arise that aren't covered by any statutes or regulations, no proscribed methods exist for handling issues and other mechanisms, like privacy portals and customer support are insufficient or require inordinate effort are restricted in scope. I want my agent to be the point-of-contact for this and I need the means to do so, not merely the right to do so.

Reference § 7616. Additional Data Broker Requirements. (c)

Item 62 How Consumers who Opt-Out from using the DROP will submit deletion requests to data brokers without being re-directed to use the DROP.

Need If I decide not to use the DROP for any reason, I do not want my CCPA Requests to DELETE to fail because the Organization is a registered data broker and insists that all delete requests must be submitted via the DROP.

Reference § 7620. Consumer Deletion Requests. (a)

Item 63 How Consumers who Opt-Out from using the DROP will submit deletion requests via the Consumers' authorized agents without being re-directed to use the DROP.

Need If I decide not to use the DROP for any reason, I do not want my CCPA Requests to DELETE to fail because the Organization is a registered data broker and insists that all delete requests must be submitted via the DROP.

Reference § 7620. Consumer Deletion Requests. (a) (b)

Item 64 What processes and requirements exist for authorized agents to delete all consumer information obtained from the DROP account upon revocation by the Consumer of the agent's authorization.

Need If I am responsible for my agent's use of DROP, I need confirmation that my agent has the capability to delete my consumer information obtained from my DROP account, if I choose to use the DROP for deletion requests.

Reference These regulations as currently drafted only apply to data brokers, but could be equally applied to authorized agents. § 7615. Requirements to Stop Accessing Deletion Requests from the DROP. (a) (2)

Grenda, Rianna@CPPA

From: Hancock, Jeremy <Jeremy.Hancock@experian.com>
Sent: Monday, August 18, 2025 2:07 PM
To: Regulations@CPPA
Subject: Public Comment on Accessible Deletion Mechanism
Attachments: Experian Comments in Response to CPPA Modifications to 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 12th St NW, Suite 504
Washington, DC 20004
www.experian.com

August 18, 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 July 31, 2025 on the modifications to the text of the proposed regulations to stand up the accessible deletion mechanism (i.e., the "DROP") under the California Delete Act.¹

We appreciate the Agency's incorporation of revisions we provided during the initial comment period and welcome the opportunity to provide further input on the modified regulations. Specifically, below we discuss: (1) the requirements to standardize data broker records; (2) the need for deletion lists to contain an appropriate number of consumer identifiers to allow data brokers to accurately match information in deletion lists to information in their own systems; and (3) the need for consumer verification beyond residency. Additionally, we include areas raised in our previous comments that have not been addressed, including the lack of provisions to ensure authorized agents are permitted to act on behalf of consumers and conflicts between the California Consumer Privacy Act ("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.

I. Requirements to standardize certain personal information within a data broker's records are overly burdensome and could result in less accurate deletion matching.

The modified regulations would require a data broker, prior to comparing consumer identifier information between a consumer deletion list and a data broker's records, to standardize certain personal information they maintain in the ordinary course of business. This standardization requirement is likely to have the effect of reducing data brokers' ability to accurately match identifiers in consumer deletion lists to information

¹ 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](#).

in their databases. For example, the proposed requirement to format a zip code to the first five characters and remove additional digits would likely lead to less accurate deletion matches depending on what other identifier information is shared with a data broker.² Removing the additional four digits of a zip code from a data broker's systems renders the zip code information less specific, thereby reducing the data broker's ability to accurately associate that data with specified identifiers in a consumer deletion list. A data broker would not be able to differentiate, for example, a consumer named Mary Jones living in zip code 94115-3519 from a different Mary Jones living in zip code 94115-3120. The effect of this standardization rule would be to create more matches to data associated with consumers who did not actually request deletion through the DROP.

As we raised in our previous comment, 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. 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.³ 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.

II. A requirement to maintain unmatched consumer identifiers for the purpose of future deletion is unnecessary.

The proposed regulations would require a data broker that matches a consumer identifier found in newly collected personal information, after previously not matching the consumer identifier, to report the new status of the deletion request in the next access session.⁴ This obligation would unnecessarily require a data broker to maintain a duplicative deletion list, already maintained by the DROP, into perpetuity. The proposed rule introduces an unnecessary need for data brokers to maintain consumer identifiers that it may otherwise may not collect. Further, the requirement creates an inconsistent compliance obligation from the CPPA, which does not require the reprocessing of deletion requests.

² Cal. Code Regs. tit. 11, § 7613(a)(1)(A)(iv) (proposed).

³ *Id.* at § 7613(a)(1)(A)(ii) (proposed).

⁴ *Id.* at § 7613(c) (proposed).

III. Not requiring a data broker to maintain standardized personal information for any other purpose beyond DROP compliance does not relieve the burden on database structure.

The proposed regulations would require data brokers 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. The revised regulations state that a data broker is only required to standardize its consumer person information "for purposes of complying with the section" and information need not be standardized for any other purpose.⁵ While the clarification appears to acknowledge the obligation to have a specific database structure to comply with the regulations, it does not relieve the burden of data brokers establishing specific database requirements to meet the regulations. The provision should be struck from the proposed regulations.

As we've stated, these proposed standardization mandates are overly burdensome. They also threaten to interfere with data brokers' free speech rights by impacting the way data must be maintained in proprietary datasets. In addition to potentially negatively impacting the quality and accuracy of data maintained in systems, database standardization conditions the expression of protected First Amendment activity on meeting the requirement to maintain data in a specified format. The requirement creates First Amendment concerns because it impacts data brokers' ability to engage in protected speech and format databases to their own specifications in ways their customers expect.

IV. While the 50% matching rate rule has been removed, each deletion list must maintain sufficient personal identifiers to allow data matching in ways that are consistent with existing CCPA matching regulations.

For every match between a consumer deletion list and the data broker's own records, the data broker must delete all personal information associated with a matched identifier. The definition of a "consumer deletion list" means a list containing one or more types of consumer identifiers.⁶ In addition, new hashing requirements under the proposed rules would require data brokers to individually hash identifiers associated with consumers in their systems and hash the combination of those identifiers before comparing them to consumer deletion lists provided through the DROP.⁷ Taken together, these requirements draw into question what degree of data matching will require a data broker to delete data associated with a consumer.

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.⁸ A reasonably high degree of

⁵ *Id.* at § 7613(a)(1)(C) (proposed).

⁶ *Id.* at § 7601(c) (proposed).

⁷ *Id.* at § 7613(a)(2)(A) (proposed).

⁸ Cal. Code Regs. tit. 11, § 7062(c).

certainty requires matching at least three pieces of personal information provided by the consumer with personal information maintained by the business.⁹ Because a consumer deletion list may contain less than three consumer identifiers, the DROP rules are not harmonized with this CCPA requirement. Moreover, even the CCPA's opt out requirements allow businesses to ask consumers for information necessary to complete a request, such as information necessary to identify the consumer whose information shall cease to be sold or shared.¹⁰ The proposed DROP rules contain no such provisions, instead creating a system where a data broker may be required to delete data associated with a consumer if just one identifier in a consumer deletion list matches to data maintained in the data broker's systems. The DROP rules are thus likely to result in overly broad application of deletion requests and application of such requests to data associated with consumers who did not request deletion through the DROP. The proposed DROP rules should be updated so they are interoperable with the CPPA verification requirements. As we stated in our previous comment, conflicts with the CPPA regulations would create significant operational challenges and could also run afoul of the California Administrative Procedure Act.¹¹

V. Residency verification should be expanded to consumer verification directly by the consumer.

While we appreciate the modified requirements to clarify that a resident "will have their California residency verified," residency requirements should also verify that the consumer making the deletion request matches the submitted consumer identifiers. Further, the regulations should clarify that the consumer must verify their residency themselves and may not rely on authorized agents, which do not have any authentication requirements in the regulations to ensure that they are acting at the direction and on behalf of consumers.

As we commented previously, the proposed regulations to implement the DROP do not provide the same verification mandates that are required under existing CCPA regulations.¹² The lack of a 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 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 information provided to verify them is sufficiently robust to protect against

⁹ *Id.* at § 7062(b).

¹⁰ *Id.* at § 7026(b).

¹¹ Cal. Gov. Code §§ 11342.1, 11342.2, 11349(b), (d).

¹² 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).

fraudulent requests or being spoofed or fabricated.¹³ 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.

We further highlight the following areas raised in our previous comment that have not yet been resolved:

VI. 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.¹⁴ 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.¹⁵ 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.¹⁶ 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.¹⁷ It would also create potential constitutional issues. The Supreme Court has affirmed that the processing and disclosure of personal information is protected expression under the First

¹³ 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.")

¹⁴ Cal. Code Regs. tit. 11, § 7621 (proposed).

¹⁵ Cal. Code Regs. tit. 11, § 7063(a).

¹⁶ *Id.*

¹⁷ 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).

Amendment's Free Speech Clause.¹⁸ As presently drafted, the proposed rules would not withstand any level of First Amendment scrutiny.¹⁹


VII. 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.²⁰ 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.²¹ 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 further 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

¹⁸ *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 558–59 (2011).

¹⁹ The Delete Act and the DROP rules also raise concerns under the Takings Clause and Contracts Clause.

²⁰ *Id.* at §§ 7612(a), 7614 (proposed).

²¹ Cal. Civ. Code § 1798.130(a)(2)(A).

Grenda, Rianna@CPPA

From: lamsherwin Manalon [REDACTED]
Sent: Saturday, August 9, 2025 3:03 PM
To: Regulations@CPPA
Subject: Reasons

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](#)

The reason why I have to keep things in private it's because of the job I do it's hard to explain but it's very important that has to do with technology and future works and i can't explain the details because my job is strict when it comes to information and data. I will get terminated for. I hope you understand the hints if not it's okay I'm just applying for some help in my situation and thank you for your time.

Grenda, Rianna@CPPA

From: Justin Perez <noreply@adv.actionnetwork.org>
Sent: Wednesday, August 13, 2025 12:42 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

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](#)

CPPA CPPA CPPA,

I strongly urge the CPPA to adopt its proposed regulations for businesses using automated decisionmaking technologies that would protect Californians' safety, privacy, and informed consent.

These common sense rules are a vital intervention for consumer protection and human rights as unaccountable algorithms increasingly influence our housing, education, employment, and basic freedoms. These rules should reflect the needs of everyday people to be protected from discrimination and data scraping, not Big Tech's appetite for profiting from our personal info.

Please stand strong, defend our rights to algorithmic transparency and accountability, and adopt the amended regulations.

Justin Perez

[REDACTED]
[REDACTED]
[REDACTED]

Grenda, Rianna@CPPA

From: K Dahl <[REDACTED]>
Sent: Sunday, August 3, 2025 4:26 PM
To: Regulations@CPPA
Subject: Public comment

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](#)

There needs to be legislation to protect consumers specifically from a company maliciously weaponizing consumer information against consumer, not limited to but to include doxing, stalking and threats.

It is not enough protection for consumers under cyber harassment penal code 653.2 because often law enforcement will not act with criminal charges unless there's a direct threat though homes, medical information, minors information is being broadcast publicly and often criminal charges are not filed even with proof met.

We would love to have our case used and detail with proof to show why this legislation is absolutely critical.

Thank you for consideration.

Kate Dahl

Grenda, Rianna@CPPA

From: Brian Hofer <brian@secure-justice.org>
Sent: Saturday, August 16, 2025 5:29 PM
To: Regulations@CPPA
Subject: Comment re Accessible Deletion Mechanism
Attachments: CPPA re Accessible Deletion Mechanism 8-16-25.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 our attached letter.

Brian Hofer
Executive Director



Cell: [REDACTED]
X personal: [REDACTED]
X org: @securejustice
Bluesky personal: [REDACTED]
Bluesky org: @securejustice.bsky.social
Mastodon org: @securejustice@techhub.social
Tik Tok org: @secure.justice
San Francisco Bay Area, CA
secure-justice.org
[Hofer bio](#)
[Donate](#) to Secure Justice

**Disclaimer: This email may contain confidential and privileged material, including attachments, for the sole use of the intended recipient(s) named above. Please do not review, use, copy, forward, or in any way distribute or disclose the contents of this e-mail including any attachments unless you are the intended recipient(s) named above. If you are not the intended recipient, or authorized to receive this message for the recipient, please contact the sender by reply email and delete all copies of this message.*



August 16, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Re: Public Comment on Accessible Deletion Mechanism

Dear Board Members and Agency Staff:

We appreciate the opportunity to comment on the proposed changes to the regulations governing the Delete Request and Opt-Out Platform (“DROP”). We commend the Agency for its efforts to strengthen these rules.

Secure Justice is a non-profit organization located in the San Francisco Bay Area, California, that advocates against state abuse of power, and for reduction in government and corporate over-reach, primarily as it pertains to our human right to privacy. We target change in government contracting and corporate complicity with government policies and practices that are inconsistent with democratic values and principles of human rights, working to create a world and criminal justice system free of discrimination and strongly committed to ensuring racial justice and equality under the law regardless of race, gender, religion, age, ideology and all protected classes.

We respectfully offer the following specific comments on the proposed regulations:

1. Definition of “Delete” and De-identified Information (§7613(b)(1)(C))

The current construction of this section leaves ambiguity as to whether brokers may retain de-identified or aggregated information, or whether the definition of “delete” permits brokers to de-identify or aggregate consumer data and continue to maintain it. We recommend clarifying the language to require that brokers delete all de-identified and aggregated consumer information.

2. Flow-down of Deletion Requests (§Section 7613(d))

While brokers are required to forward deletion requests to their service providers and contractors, the rules do not appear to require similar action for other entities with which they may have shared or sold information, such as research organizations or other data aggregators. We recommend extending this requirement to all such entities.

3. Security and Confidentiality of DROP Downloads

The final rule should include more specific guidance on appropriate security measures for handling consumer deletion lists, as well as clear consequences for failing to maintain the required level of security.

We appreciate the Board's leadership and ongoing commitment to data privacy, and we encourage the Agency to incorporate these recommendations into the final rulemaking.

Sincerely,

A large black rectangular redaction box covering the signature area.

Brian Hofer
Executive Director

A small black rectangular redaction box covering a line of contact information.

brian@secure-justice.org
<https://secure-justice.org/>
San Francisco Bay Area, CA

Grenda, Rianna@CPPA

From: Viar, Kate <Kate.Viar@transunion.com>
Sent: Monday, August 18, 2025 2:34 PM
To: Regulations@CPPA
Subject: Public Comment on Accessible Deletion Mechanism
Attachments: TransUnion CPPA DROP Modification 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](#)

Please find attached comments from TransUnion in response to the July 31 modifications to the proposed Accessible Deletion Mechanism requirements. Any questions, please let me know. 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.



August 18, 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 comment on the California Privacy Protection Agency’s (“CPPA”) July 31, 2025, modifications to the proposed 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 Agency’s commitment to responsible data use and commend the recent improvements to the proposed regulations, particularly the addition of consumer residency verification requirements and the updates to data standardization, hashing, and matching requirements.

While these changes represent meaningful progress, we remain concerned that several critical areas require clarification or strengthening to ensure the DROP system operates securely, efficiently, and in a manner that truly benefits consumers.

1. Clarify Data Retention Requirements (§ 7613)

Section 7613 should provide clear and specific requirements regarding the retention of “minimum deleted information” and associated logging or metadata. At present, the regulation does not specify which received data should be retained or deleted, or what the retention period is (or whether company-specific retention policies may govern). This lack of clarity creates compliance uncertainty and prevents a consistent approach to data retention by data brokers.

2. Require Identity Verification to Prevent Fraud (§ 7620)

Section 7620 should require, rather than merely permit, the CPPA to verify all personal information submitted with a deletion request, including date of birth, email address, phone number, and pseudonymous identifiers. Leaving this verification optional creates an avoidable vulnerability to fraudulent requests, undermining both consumer trust and system integrity.

As a federally regulated entity subject to NIST 800-63-3 identity assurance standards, TransUnion must ensure that any system it interacts with adheres to equivalent safeguards. Mandatory verification would align with these standards and materially strengthen consumer protection.

3. Establish Verification Standards for Authorized Agents (§ 7621)

The absence of defined verification standards for authorized agents in § 7621 is currently the most significant security gap within the DROP framework. Merely requiring an agent to be a registered California business is insufficient to meet federal security requirements. Without robust credentialing and monitoring processes, as well as a procedure for furnishing proof of the consumer authorization for the agent to act on their behalf, the system is susceptible to abuse, and bad actors could exploit the system at scale.

The CPPA should distinguish between *personal authorized agents* (such as family members or fiduciaries with valid Power of Attorney) and *commercial authorized agents* (entities that submit deletion requests on behalf of multiple consumers) and establish a distinct verification process for each. Commercial authorized agents should be subject to rigorous consumer credentialing and ongoing oversight modeled after similar roles in the financial services industry — as well as a mechanism for providing proof of customer authorization — before being authorized to furnish data to the DROP system.

This framework would preserve legitimate consumer representation while preventing large-scale fraud and abuse that could undermine the system and rights of consumers.

In addition, the regulations should provide a safe harbor for data brokers against liability resulting from unauthorized deletions initiated by unverified or unauthorized agents.

4. Clarify Timelines for Deletion Compliance (§ 7612)

Section 7612 should clarify that the deletion deadline begins 45 days from the date the data broker downloads the incremental deletion list. There also needs to be clarity around how deadlines are impacted if the DROP system is unavailable.

Absent these clarifications, data brokers may interpret deadlines inconsistently, potentially leading to disputes or inadvertent non-compliance. Clear guidance on these operational timelines will improve uniformity and compliance readiness.

5. Permit Parent-Level Registration for Corporate Groups (§7602)

We reiterate our prior recommendation that the CPPA allow a single, parent-level DROP registration for corporate groups operating under a unified privacy program, rather than requiring each subsidiary to maintain a separate account.

The current proposed approach risks: 1) confusing consumers by presenting multiple, seemingly unrelated entry points for the same company; 2) unnecessarily fragmenting request processing; and 3) creating duplicative administrative and technical burdens without enhancing privacy outcomes. A parent-level registration model would streamline operations while preserving the consumer protections the CPPA seeks to advance.

TransUnion values the CPPA's work to improve the draft regulations and shares its commitment to protecting the privacy of Californians. We stand ready to participate in technical workshops, sandbox evaluations, or advisory groups to help ensure the DROP system functions securely, efficiently, and equitably for all stakeholders.

Thank you for your consideration.

Sincerely,



Kate Viar
Senior Director of Government Relations

Grenda, Rianna@CPPA

From: Elina van Kempen <evankemp@uci.edu>
Sent: Wednesday, August 13, 2025 2:45 PM
To: Regulations@CPPA
Cc: Gene Tsudik
Subject: Public Comment on Accessible Deletion Mechanism
Attachments: UCI-CCPA-DROP-MODS-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

To the CPPA:

Attached are UC Irvine SPROUT Lab's comments on the accessible deletion mechanism proposed regulations - modifications only.

Best regards,

Elina van Kempen

--

Elina van Kempen
evankemp@uci.edu
<https://sprout.ics.uci.edu/>

UCI SPROUT Lab Comments: CPPA DROP (mods only)

7601 (g) and 7613 (a) (1) (A) (ii) (1)

"Extraneous or special characters" means non-alphabetic or non-numeric characters"

→ It would be good to specify which alphabet is meant here.

"non-English language characters, which shall instead be converted to their closest matching English language character. For example, Björn O'Connor-López shall be formatted as bjornoconnorlopez;"

→ examples of "non-English language characters" are letters with diacritics. It is more precise to require the removal of diacritics instead of requiring converting non-English language characters to their closest match. Showing an example of a non-diacritic, non-English language character, if applicable, would otherwise be good.

7613 (a) (2) (A)

This section lacks some information about the hashing algorithm required, and what combine means technically.

"For example, if a consumer deletion list includes first name, last name, data of birth, and zip code, the data broker shall separately hash each of the following: first name, last name, date of birth, and zip code,"

→ The actual hashing mechanism is not specified here.

"After hashing each of the identifiers separately, the data broker shall combine the hashed identifiers for each consumer into a single new identifier, without adding spaces or other characters,"

→ What does "combine" into one mean? Concatenate all hashes? Or hash all hashes? Something else?

"before applying the hashing algorithm pursuant to (a) (1) (B) of this section to the combined identifier."

→ Here the hashing algorithm is specified. If the same algorithm is used throughout, it would be good for it to be explicitly stated.

Grenda, Rianna@CPPA

From: Lindsey Stewart <lindsey.stewart@zoominfo.com>
Sent: Monday, August 18, 2025 11:34 AM
To: Regulations@CPPA
Cc: Bubba Nunnery
Subject: Public Comment on Accessible Deletion Mechanism
Attachments: ZI CPPA Comments 8.18.25.docx.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 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



August 18, 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 appreciate the opportunity to submit comments on the proposed Data Rights of Californians on Online Platforms (DROP) regulations. We respectfully resubmit our comments from the June rulemaking process, as we continue to strongly support the recommendations outlined below.

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,

June 10, 2025

regardless of their individual preferences.

We propose the following addition to the definition of "Personal information 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

