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

By

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

June 10, 2025

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

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

I. Section 7601 (Definitions)

"Direct Relationship"

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

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

---

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

[2] Proposed Rules, Section 7601(d), https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_text.pdf

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

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

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

Selection of Deletion Lists

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

---

[3] Don Marti et al., Consumer Reports, "Who Shares Your Information with Facebook," (January 2024), https://innovation.consumerreports.org/wp-content/uploads/2024/01/CR_Who-Shares-Your-Information-With-Facebook.pdf

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

[5] Proposed Rules, Section 7601(d)

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

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

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

III. Section 7613 (Processing Deletion Requests)

Limiting Data Leakage From Sharing Hashed Identifiers

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

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

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

---

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

[9] Proposed Rules, Section 7616(a).

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

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

Threshold for Deleting Data

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

Deleting Matching Identifiers

We appreciate that CPPA's proposed definition of "personal information associated with a matched identifier," states that the term includes inferences made personal information subject to applicable exemptions.[11]

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

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

[11] Proposed Rules, Section 7601(i)
[12] CCPA, Section 1798.140(r), https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

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

IV. Section 7614 (Reporting Status of Deletion Requests)

Exempted Data

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

V. Section 7616 (Additional Data Broker Requirements)

Prohibition on Data Broker Verification

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

---

[13] California Privacy Protection Agency, 2025 Data Broker Registry, https://cppa.ca.gov/data_broker_registry/

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

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

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

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

VI. Section 7620 (Consumer Deletion Requests)

Verification of Residency

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

VII. Section 7621 (Authorized Agents)

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

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

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

****

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

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

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