Comments of Consumer Reports, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse (PRC)
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments On
Proposed Rulemaking Under Senate Bill 362

By

Matt Schwartz, Policy Analyst, Consumer Reports
Justin Brookman, Director of Technology Policy, Consumer Reports

June 25, 2024

The undersigned organizations appreciate the opportunity to provide feedback on the California Privacy Protection Agency's (CPPA) Invitation for Preliminary Comments on Proposed Rulemaking Under Senate Bill 362 (the Delete Act). We thank the CPPA for initiating this proceeding and for its other efforts to protect consumer privacy.

We are pleased that the Agency is moving quickly to implement critical provisions of the Delete Act, which focuses on the inherently privacy-eroding data broker industry that has a well-documented history of abusive and harmful business practices.[1] The law remedies an oversight in the California Consumer Privacy Act (CCPA), whereby deletion rights only apply to "data about the consumer which the business has collected *from the consumer*" (emphasis added), arguably opening up the interpretation that deletion rights do not apply to entities that collect information about consumers indirectly, as is the business model of many data brokers. It addresses the threshold issue of how deletion rights ought to apply to an industry that many consumers likely do not even know exists, let alone how they might locate and exercise their rights with the specific data brokers that may have collected their personal information.

Importantly, with the mandate that the Agency create an "accessible deletion mechanism" that allows consumers to delete all of their personal information held by the state's registered data brokers in a single action, the law adopts the perspective that many consumers are likely to want to delete their information from the data broker industry as a whole, and that the process for doing so should be as seamless as possible. Now, the Agency seeks comments on how it is to operationalize this system.

We describe our views on each of the potential areas for rulemaking in the course of providing answers to the questions posed by the CPPA in its invitation.

I. Verifiable Consumer Requests

The Delete Act requires the Agency to establish an accessible deletion mechanism that allows a consumer, through a "verifiable consumer request," to request every data broker that maintains any non-exempt personal information about them to delete that personal information.

---

[1] See, e.g., Joseph Cox, The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15, 404 Media (Aug. 22, 2023), https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/;
Douglas MacMillan, Data Brokers are Selling Your Secrets. How States are Trying to Stop Them, Washington. Post (Jun. 24, 2019). https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-yoursecrets-howstates-are-trying-stop-them/; Jon Keegan and Joel Eastwood, From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found
650,000 Ways Advertisers Label You, The Markup, (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you
.

a. *What should constitute a "verifiable consumer request"?*

General Views

In general, our view is that the Agency should create a low bar for consumers to meet in terms of identity verification. The Delete Act was written to focus on data brokers that primarily deal in the creation of data dossiers and individualized marketing profiles, typically without the knowledge or explicit consent of consumers. It only applies to data brokers that "knowingly collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship,"[2] ruling out other types of businesses with direct consumer relationships that nonetheless collect and sell user information (e.g. tech giants like Facebook and Google), but for which a universal deletion mechanism may be too blunt an instrument. For example, while these consumer-facing entities harbor deep tranches of personal data and sell inferences about consumers' behavior, they also maintain information a consumer may have directly provided and may reasonably want to preserve (e.g. important user profile information, photos, and documents).

Beyond that, the Delete Act exhaustively excludes from coverage other types of data that may provide some sort of societal benefit, or, were they to be deleted, could potentially prove harmful to a consumer; the Delete Act exempts any entity to the extent that is covered by FCRA, GLBA, the Insurance Information and Privacy Protection Act, CMIA, and HIPAA, as well as any publicly available data as defined in CCPA.[3] Given that these limitations scope the law to seemingly only cover data brokers' consumer profiles collected from private sources, such as consumer web searches, apps and online behavior, preferences, geolocation, and inferences derived from these factors, it appears that the risk of harm from mistakenly deleting a consumer's record is low, while the risk of harm of *not* deleting a consumer's record upon their request is high.

Direct Consumer Verifications

With this in mind, when the request comes directly from a consumer visiting the accessible deletion mechanism, we believe the request should be considered verifiable when either an email address or a phone number can be authenticated by the Agency. In our view, this authentication method strikes the best balance between ease of consumer use, efficacy, and privacy considerations. Consumers have grown accustomed to authenticating themselves in this manner,[4] and many data brokers already commonly request these identifiers for purposes of effectuating do not sell requests under CCPA.[5] While we considered the merits of additional

---

[2] Delete Act, Section 1(c), https://legiscan.com/CA/text/SB362/2023
[3] *Id* at Section 1(c)(1-4); Section 1(a) (deferring to CCPA's definition of personal information).
[4] Chrysta Cherrie, 2FA Statistics: 2FA Climbs, While Password Managers and Biometrics Trend (noting a rising trend in survey respondents who have used two-factor authentication and that SMS and email were the most common second factors), Duo Labs (September 14, 2021), https://duo.com/blog/the-2021-state-of-the-auth-report-2fa-climbs-password-managers-biometrics-trend
[5] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected? (finding that email address was the most commonly requested identifier, followed by name, address, and phone number), Consumer Reports Digital Lab, (Oct. 1, 2020),

identifiers common to data broker profiles, such as home address, we view this factor to be both impracticable (likely requiring a time consuming mail correspondence) and potentially more privacy invasive than either phone or email verification. Given these considerations, we do not believe the universal deletion mechanism needs to allow for home address verification, though consumers should be able to submit current and past addresses as part of their deletion request.

One of the primary challenges here is the inherent informational asymmetry that exists between consumers and data brokers (as well as the CPPA) — how are consumers to know exactly what information a given data broker *truly* needs in order to successfully process a deletion request? While the Delete Act will increase the amount of information data brokers must share about their data collection practices,[6] they still aren't required to share the key identifiers that they collect or how their data profiles are structured. The CPPA should seek to remedy that with this rulemaking by requiring each data broker to share with the CPPA the minimum necessary set of identifiers able to identify a majority of their consumers.

One of the harms we've encountered when data brokers are allowed to determine the parameters for verification is that they will use the asymmetry to their advantage, requesting information that is clearly not needed to carry out the request. For example, even though Consumer Report's authorized agent, Permission Slip, provides first and last name, verified phone number, verified email, address, signed authorized agent letter, and more with each consumer request, one data broker routinely asked for consumers' birth dates on top of this information. Then, when consumers refused to provide the additional information, the data broker would complete the request regardless — implying that the information was never actually required. Consumer Reports also documented similar abuses during its study of the usability of CCPA rights, finding examples of data brokers requiring consumers to take a selfie or download a third-party app in order to verify identity or applicability of CCPA rights.[7] In some cases, these processes were so onerous that they had the effect of preventing consumers from completing their rights request. On the other hand, if a consumer does not provide enough information, or the right type of information, a data broker acting in good faith may well not be able to complete the request.

Data Broker Treatment of Verified Requests

Many data brokers link several identifiers to a single consumer's data profile (e.g. phone number, email, address, advertising ID). As discussed above, a consumer's request should be considered verifiable when just one one of those identifiers (phone or email) has been authenticated by the consumer. Upon receiving a verified request, data brokers should be

---

https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

[6] *Id at* Section 3(b)(2)

[7] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected? Consumer Reports Digital Lab, (Oct. 1, 2020), https://advocacy.consumerreports.org/wpcontent/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

required to delete all of the corresponding information reasonably likely to be associated with the consumer. A "reasonably likely" standard recognizes that there may be a degree of probabilistic linkage in data broker records but that it might be undesirable for the agency to articulate an arbitrary standard of certainty above which deletion should be required (i.e. should deletion be required when data brokers are 60 percent confident of linkage, or 75 percent certain of linkage)?

Additionally, the CPPA should clarify that the consumer's initial submission of their verified request, either through the accessible deletion mechanism directly or through their authorized agent, should mark the end of the consumer's responsibility to verify themself or provide request information. Data brokers should not be allowed to respond to universal deletion requests by contacting consumers to ask for additional verification or further information to complete the deletion request. The purpose of a universal deletion mechanism is to reduce the burdens on consumers — a benefit that would be largely eroded if data brokers were permitted to respond to universal deletion requests with individualized responses for additional information.

Device IDs

Some data brokers *only* amass consumer profiles using device identifiers, such as IP address, mobile advertising IDs, or cookies, which may make it more difficult for consumers to send a successful request using more traditional personal identifiers like email or phone alone. Though, in some cases, consumers could theoretically look up their device IDs and manually enter them into a field on the accessible deletion mechanism website, this may prove burdensome for consumers[8] or difficult to authenticate. The CPPA should consider how it could provide an alternative process to address deletion requests for this subset of data brokers, potentially by automatically capturing and including IP address or mobile advertising ID with a consumer's request, for example, when a consumer fills out a deletion request using their mobile device. Such a framework would have the benefit of being self-authenticating, reducing additional burden on consumers. While this process may not be capable of capturing domain-specific identifiers, like cookies, the CCPA's universal opt-out mechanism provisions at least allow consumers to suppress cookie-based tracking in the interim while platforms increasingly move toward the deprecation of third-party cookies altogether.[9]

Verifications Through Authorized Agents

Consumers should also be able to authenticate their identity and send a verifiable request through their authorized agent of choice. Some authorized agents already have robust verification measures in place that meet or exceed CCPA's existing requirements. For example, in addition to the signed permission required by the CCPA Rules (Section 7063(a)), Permission

---

[8] *Id* at 24.

[9] See, e.g., Tina Moffett, Google Makes Good On Its Resolution To Deprecate Third-Party Cookies In 2024, Forrester, (January 4, 2024), https://www.forrester.com/blogs/google-makes-good-on-third-party-cookie-deprecation/?utm_source=forbes&utm_medium=pr&utm_campaign=b2cm

Slip currently requires consumers to verify their email address and phone number as part of their onboarding process.[10] In order to provide further certainty about the standing of authorized agents, the CPPA could create a registry of trusted authorized agents that must meet similarly robust standards of identity verification and other indicia of trustworthiness. Those included in the registry could then send consumer requests without additional verification.[11]

II. Privacy Protecting

The Delete Act requires the Agency to determine "one or more privacy-protecting ways" by which a consumer can securely submit information to aid in a deletion request using the accessible deletion mechanism.

a. How should a consumer securely submit information in a "privacy-protecting way?"

Data Minimization

As discussed earlier, one of the best ways to improve consumer privacy is to require that consumers only submit the minimum information possible with their deletion request (i.e. verified phone or email). However, the CPPA may also be considering what optional fields consumers should be allowed to fill out in order to increase their chances of a successful request. In our view, consumers should be able to augment their deletion request with additional identifiers like their home address, date of birth, middle name, maiden name, and alternative emails and phone numbers. However, we do not believe that CPPA should permit the submission of any government identifiers (e.g. social security numbers, passport numbers, driver's license scans) or biometric identifiers with consumer requests. From a data security standpoint, collection of this information creates an unacceptable degree of risk for CPPA when weighed against the risk of mistaken deletion. It would also create the risk of improper use by data brokers, whose business model inherently incentivizes them to create the most accurate consumer profiles possible (notwithstanding the purpose limitation principle discussed below). Improper proliferation of biometric identifiers, for example, can cause irrevocable harm to consumers considering that they cannot be changed when they are compromised.[12]

Purpose Limitation

Though the CCPA already includes a provision that requires that businesses solely use personal information collected from the consumer in connection with the business' verification of the deletion request for that purpose and for no "unrelated purposes", the CPPA should clarify in its

---

[10] Tara Claesgens, How does Permission Slip work?, Consumer Reports Innovation Lab, (November 16, 2023), https://innovation.consumerreports.org/how-does-permission-slip-work/

[11] CCPA Regulations, Section 7063(b), (noting that receiving Power of Attorney prevents a business from requiring 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 the request), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

[12] Woodrow Hartzog, Facial Recognition Is the Perfect Tool for Oppression, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for- oppression-bc2a08f0fe66.

rules that data brokers cannot use *any* personal information (including that which was not used for verification purposes) provided as part of a consumer's deletion request for any other purpose aside from honoring the request.[13] Anecdotally, in Consumer Reports' experience as an authorized agent, some entities appear to be misusing consumer data submitted as part of a request for marketing purposes. In some instances, users and employees have reported receiving marketing emails from entities where the person's only known interaction with the company was submitting a rights request. The marketing emails appeared shortly after the submission of the request. Consumer Reports experienced a similar phenomenon during its study of data brokers' opt-out processes under CCPA; a study author was placed on data broker X-Mode's newsletter despite her only interaction with the company being her opt-out request.[14]

Data Security

The Delete Act states that the CPPA shall establish an accessible deletion mechanism that "implements and maintains reasonable security procedures and practices".[15] At a minimum this should include encryption of the consumer's submission of personal information to the accessible deletion mechanism in transit and at rest. The CPPA should also consider how an API-based implementation of the Delete Act could advance data security objectives.[16] Programmatically exchanging rights requests could help avoid the need to maintain a widely accessible, central registry of consumer records, which would likely serve as a high-value target for hackers. Theoretically, the API could also be structured to send request information in an individualized format for each data broker, so that they only receive the information necessary for them to carry out the request. For example, a data broker that only collects device IDs would not be sent consumer email addresses or phone numbers, helping minimize the potential for misuse described above. Consumer Reports' Permission Slip app has successfully experimented with sending consumer rights requests programmatically via the Data Rights Protocol.[17]

b. In what privacy-protecting ways can data brokers determine whether an individual has submitted a deletion request to the Agency?

As discussed earlier, data brokers should be required to delete the entirety of a consumer's profile upon matching one of the key authenticated identifiers (phone or email). This framework should reduce the amount of data that brokers are looking for in the first place. Upon deleting the consumer's record, the broker should be allowed to retain certain identifiers for the purposes

---

[13] CCPA Section 1798.130(a)(7)
[14] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected? (pg. 34-37), Consumer Reports Digital Lab, (Oct. 1, 2020), https://advocacy.consumerreports.org/wpcontent/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf
[15] Delete Act, Section 6(a)(1), https://legiscan.com/CA/text/SB362/2023
[16] Ryan Rix, Securing and Standardizing Data Rights Requests with a Data Rights Protocol, PEPR '23, (September 11, 2023), https://www.usenix.org/conference/pepr23/presentation/rix
[17] Ginny Fahs, Announcing a Stable Version of the Data Rights Protocol, Consumer Reports Innovation Lab, (September 12, 2023), https://innovation.consumerreports.org/announcing-a-stable-version-of-the-data-rights-protocol/

of maintaining a suppression list (subject to strict purpose limitation requirements). These identifiers should be further limited to include only those the data broker reasonably expects to collect in the future. As discussed earlier, automating the communication of rights requests also could protect consumer privacy. Instead of querying a central database, brokers could automatically receive requests personalized to their verification needs, potentially reducing the amount of personal data they have access to.

III. Status of Request

The Delete Act requires the accessible deletion mechanism to allow the consumer, or their authorized agent, "to verify the status of the consumer's deletion request."

a. *What information should be included in the "status of the consumer's deletion request"?*

The CPPA should ensure that the accessible deletion mechanism is capable of providing clear status updates to the consumer. Again, the benefit of the universal deletion mechanism is its centrality — consumers should be able to use the mechanism as a one-stop-shop for their data broker deletion requests, and data brokers should not be permitted to contact consumers with status updates outside of the system.

There are several components we consider essential to a status update. Most simply, the agency should allow the consumer to query the accessible deletion mechanism to determine which of their personal data were sent to which data brokers. Consumers should be able to subsequently update the data fields if they desire or submit multiple requests if they possess multiple emails or phone numbers they wish to append to their request. The CPPA should also require data brokers to confirm to the accessible deletion mechanism when they've received the initial deletion request and intend to take action, when they've completed a request, or when they couldn't match the exact consumer and thus processed the request as an opt-out of sale or sharing, as required under the Delete Act.[18] This will allow consumers to query the accessible deletion mechanism and confirm how many of the brokers had a match for their submitted data.

In the event that a request is denied, data brokers should include specific information explaining why. For example, data brokers should detail whether the request was denied because the data broker couldn't match the provided identifiers with data in their system, the information is protected under an exemption (clearly explaining which exemption they are relying on), they believed the request was fraudulent, or any other grounds for denial. Data brokers should provide all status updates to the CPPA as soon as reasonably possible after taking an action related to the status update.

IV. Consumer Experience

The Delete Act requires the accessible deletion mechanism to allow a consumer, "through a single verifiable consumer request," to request that every data broker that any personal

[18] Delete Act, Section 6(c)(1)(B), https://legiscan.com/CA/text/SB362/2023

information delete any personal information related to that data broker or associated service provider or contractor.

a. *What should the Agency consider with respect to the consumer experience?*
b. *How can the Agency ensure that every Californian can easily exercise their right to delete and right to opt-out of sale and sharing of their personal information via the accessible deletion mechanism?*

Consumers benefit most from universal controls when they are simple and easy to use. As mentioned throughout, CPPA's rules should clarify that a consumer should only be required to interact with the universal deletion mechanism in order to complete their requests and check for status updates. We note that the data broker industry advocated the opposite approach through legislation they sponsored earlier in the legislative session, by requesting the ability to directly contact consumers using the accessible deletion mechanism or when they used an authorized agent to send a universal deletion request.[19] This could result in consumers receiving hundreds of emails upon submission of a universal deletion request, with data brokers asking consumers to provide additional information in order to "complete the request," to rescind the request, or to whitelist the specific data broker. From the consumer's perspective, the initial request should be the end of their interaction with the accessible deletion mechanism, unless they wish to return to check on the status of their request or append their request with more information.

Additionally, a consumer's decision to use an authorized agent to send a universal request should be respected. Permission Slip regularly encounters businesses that attempt to circumvent them by responding to requests by directly contacting the consumer, often asking consumers to resubmit request information originally submitted by Permission Slip. This behavior typically confuses or angers consumers who have gone out of their way to designate authority to the authorized agent. The forthcoming rules should clarify that, to the extent that communication is ever necessary as a result of a universal deletion request, data brokers must correspond with authorized agents exclusively when consumers have chosen to exercise their rights in this manner.

****

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) or Justin Brookman (justin.brookman@consumer.org) for more information.

[19] Senate Bill 1076, Section 2 (b)(8)(H); Section 2 (b)(11), https://legiscan.com/CA/text/SB1076/id/2925501