Grenda, Rianna@CPPA

From:	Ben Isaacson <ben@lucidprivacy.io>
Sent:	Tuesday, June 10, 2025 3:42 PM
To:	Regulations@CPPA
Cc:	Colin O'Malley
Subject:	Lucid Privacy Group Comments Re: SB 362 'DROP' Rulemaking
Attachments:	Lucid Privacy Group CPPA Delete Act June 2025 Comments.pdf

Greetings,

On behalf of Colin O'Malley and the Lucid Privacy Group, I am submitting the following written comments. We welcome any feedback or the opportunity to further clarify these comments at any time.

Best regards,

--Ben Isaacson
(Counsel to the Lucid Privacy Group)
www.lucidprivacy.io

Lucid Privacy Group, Inc. Comments to the California Privacy Protection Agency (CPPA) Regarding SB 362 'Delete Act' Rulemaking Regarding the Data Broker Registration and Accessible Deletion Mechanism (DROP)

Introduction: Lucid Privacy Group, Inc. ("Lucid" or "We") is a consulting group that serves many companies at the intersection of privacy, data, and technology, and helps provide solutions to those companies balancing commercial objectives, marketplace configuration, and technical constraints. These comments are our own, and do not reflect the opinions of any specific client.

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

ARTICLE 3. DELETE REQUEST AND OPT-OUT PLATFORM REQUIREMENTS

§ 7612. Delete Request and Opt-out Platform Access.

§ 7612(b).

Note that references in this section to an 'automated means' are encouraged, but there are a wide range of potential means that might be proposed that could improve efficiencies or add technical burdens. When contemplating potential specifications for the automated means, existing technical configurations and competencies in the data broker community should be taken into account, and especially the constraints of small and medium sized organizations. We recommend that the CPPA engage with the data broker community in a collaborative requirements gathering process before issuing specifications for the automated means, especially if these means are written into the rules explicitly.

§ 7612(b)(1).

Section 7612(b)(1) defines a required notification process, '*the data broker must notify the Agency of the connection failure in writing through its DROP account*,' but this notification process is not well defined. 'In writing' should be clarified to include that 'email is acceptable,' and the notification process should be defined or reference a process that will be defined at a later date in detail (e.g., 'through a contact mechanism that will be made available in the DROP platform,' or 'to the DROP support email abc@123.gov').

§ 7612(c).

§7612(c), where the proposed regulations discuss subsequent downloads of the consumer deletion lists, includes unnecessary ambiguity. The proposed regulations fail to clarify whether the section applies to each data broker individually or whether the

section applies list-wide to all applicable data brokers. In other words, it would seem that one data broker downloading the list would receive a list of new or amended consumer deletion requests, but a second data broker downloading the list the very next day would only receive a list of new or amended consumer deletion requests that had been submitted since the former data broker downloaded the list the day prior. We recommend that the CPPA clarify this ambiguity by specifying that, for the sake of file sizes, subsequent downloads will only contain the new or amended consumer deletion requests received after the downloading-data broker's previous download.

However, we believe that a better solution to this ambiguity is to permit data brokers to download all the new or amended consumer deletion requests received within a specified period determined by the downloading-data broker, including the option to download the complete deletion list at any time. There should be no restrictions as to what data brokers are allowed to download, as making such information readily available at any scope and any time is invaluable to ensuring compliance with these regulations at all times. A data broker acting in good faith, seeking to ensure that consumers are appropriately opted-out or deleted, should not be dealing with a restrictive and unforgiving system.

§ 7613. Processing Deletion Requests.

§ 7613(a)(1)(A)(iii).

The proposed requirements require that data brokers "Implement any other standardization that the data broker knows will increase the likelihood of a match between its records and the applicable consumer deletion list." Note that matches should be good faith matches of the specific consumer in the DROP file with their record in the data broker's system. An increase in match rate alone is not an indication of success, especially when false positive matches are possible. The language could include "the data broker knows will increase the likelihood of a good faith match/match with the same confidence data broker would use for its own commercial data, between its records and the applicable consumer deletion list."

§ 7613(a)(2)–(a)(2)(A).

Section 7613(a)(2) includes a 50% rule that is unduly complicated and that may result in reduced privacy for consumers and unnecessary confusion. For example, if certain definitive identifiers, like an email address or MAID are associated with a data broker's file, the corresponding consumer can be removed. The 50% rule actually provides a means to avoid opting out of this clear match, especially if other peripheral and potentially less certain data, like gender and ZIP, do not match. Despite a direct email match, data brokers would need not comply with the rule when only one-third of identifiers match with the consumer record, because the less certain gender and ZIP

identifiers do not match. Direct matches on deterministic identifiers should simply be matched. Uncertain or inferred data should never become more impactful than deterministic data. In this section, the initial sentence should stand: “If the consumer deletion list that the data broker is comparing to its own records includes multiple identifiers, the data broker must separately compare each unique category of identifier with the applicable identifiers in its own records.” However, we recommend removing: “If more than fifty percent (50%) of the unique identifiers match with the same consumer record in the data broker’s records, the data broker must delete all personal information associated with that consumer as described in subsection (b). For example, if a data broker compares its records with a consumer deletion list that includes name, date of birth, and zip code, and only finds a match for the name and zip code with a particular consumer record, the data broker must delete that consumer’s associated personal information because approximately sixty-seven percent (67%) of the individual identifiers match with the consumer deletion list.”

Furthermore, the proposed regulations mandate “the data broker must delete all personal information associated with a matched identifier”.[1] We recommend that, following our previous recommendation, the Agency clarify that such personal information does not include inferences made based on personal information, and instead delete only the specifically enumerated data included in lists. Further, some personal information will be associated with multiple consumers, so the rule should specify deletion of personal data ‘solely or primarily associated’ with the individual on the DROP file.

§ 7613(a)(2)(B).

The language presents a loophole where two consumers could be opted-out using the same identifier. A physical address, for example, could apply to multiple consumers when only one made a deletion request. In essence, the proposed language mandates deletion for an improperly-verified, and non-existent, request from other consumers. The loophole would be closed with the following addition: “If a 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, unless the data broker has good faith reasons to assume the request is for a specific consumer and not a set of consumers.” An obvious example is a name and an address, where the request can reasonably be assumed to apply to the named individual, and not everyone that shares the same address.

§ 7613(b)(1).

[1] Cal. Code Regs. tit. 11, § 7613(a)(2) (proposed); *see also*, Cal. Code Regs. tit. 11, § 7613(b)(1) (proposed) (exhibiting language explicitly requiring deletion of inferences).

This section proposes deletion of inferences that are produced based on personal information. In line with our previous recommendations, the Agency should consider curtailing the mandated deletion of inferences, as such inferences will be difficult to connect with the many personal information data points that helped inform the inference.

§ 7613(b)(1)(B).

The section lacks clear upper limits for personal information retention necessary for compliance, potentially leading to under- or over-retention. The drafters may consider defining permissible retention scope to guide data brokers.

§ 7613(b)(1)(C).

The proposals require archive and backup data removal, but Section 7613(b)(1)(C)(i) allows indefinite deletion delays, creating a contradiction. Revisions are needed for a consistent regulatory framework and clear data protection guidelines. Data stored in backups that are regularly deleted according to a set schedule should be exempt from these requirements, unless such data is restored at which point the data broker should be required to re-access the entire DROP list. Further, flexible access to all or parts of the DROP file would open more efficient methods of honoring DROP file requests, rather than requiring the scrubbing of non-production back-up files which may not be even be stored in formats that are easily scrubbed (see comment for § 7612(c)).

§ 7613(b)(2).

The regulation mandates forwarding of requests for deletion to all service providers and contractors, but does not require (or enable) the same forwarding to third party businesses including other data brokers. Permitting or requiring forwarding of requests to additional third party businesses would aid in fulfilling DROP's objectives.

§ 7614. Reporting Status of Deletion Requests.

Section 7614 of the draft regulations involves mandatory status reporting of deletion requests which creates a significant and material cost burden on data brokers with uploading proof of each deletion before permission to download the most recent consumer deletion list. In practice, this requirement may be so costly and burdensome that it substantially delays data brokers ability to access the next file within the required 45 days. The CPPA should not need specific proof in order to establish that data brokers are in compliance with each record shared, which could come in the form of any complaints and or enforcement actions. More importantly, the Delete Act specifically requires all data brokers systems to be audited for compliance with the DROP in 2028 which will clearly satisfy this requirement.

We recommend that the CPPA eliminate this requirement from the final regulations, or delay any such reporting requirement to be in conjunction with the Delete Act auditing requirements beginning in 2028. Requiring auditable records associated with DROP reconciliation would be much more manageable for companies and more consistent with analogous regulatory regimes (as with the GDPR, for example), rather than requiring a direct and record level integration with the regulator.