



Jul 31

Open Letter to CalPrivacy Re: Request For Drop Clarifications And A Transitional Enforcement Policy For Good-Faith Drop Compliance

July 31, 2026

To: Tom Kemp, Executive Director & Board Members

California Privacy Protection Agency

400 R Street, Suite 350

Sacramento, CA 95811

Submitted electronically to info@coppa.ca.gov

Cc: Elizabeth Allen, Marissa Rosembat

RE: REQUEST FOR DROP CLARIFICATIONS AND A TRANSITIONAL ENFORCEMENT POLICY FOR GOOD-FAITH DROP COMPLIANCE

In-House Privacy, Inc. ("IHP") respectfully requests that the California Privacy Protection Agency ("CalPrivacy") adopt a one-year transitional enforcement policy for registered data brokers making documented, reasonable, and good-faith efforts to comply with the Delete Request and Opt-Out Platform ("DROP") as regulated under California SB 362 ("Delete Act").

IHP is a law practice that advises businesses engaged in marketing, advertising, and data services, including data brokers subject to the California Delete Act. This letter reflects implementation issues identified through IHP's work with registered data brokers and other advisors, but it is submitted by IHP and not on behalf of any specifically identified client or business.

Table of Contents

[1. Introduction](#)

[2. DROP Technical Implementation Issues](#)

3. Operational Application Issues

4. Legal and Policy Issues

5. Request for Transitional Enforcement and Cure Period

1. Introduction

The Delete Act introduced the DROP as a first-of-its-kind regulatory mechanism to enable automated consumer privacy rights related to the sale of third-party data by registered data brokers. There are no comparable regulatory compliance mechanisms under U.S. state law. While the federal telemarketing-specific 'Do Not Call' registry is similar in its statutory approach, it is not directly comparable to the DROP because it is a simple phone number suppression list that any small business can easily implement. The technical, operational, and legal-policy interpretations necessary to comply with the DROP extend well beyond any other regulatory precedent, and have required registered data brokers to expend significant business resources in order to comply with the DROP specifications.

Common software industry procedures dictate that new enterprise software releases enable the software business customers or end users to test, evaluate, modify, and scale adoption of new software over an extended period of time that begins with an 'alpha' testing phase, and extends into a 'beta' testing phase before the final production release. With the DROP rollout, businesses have only been provided with a 'sandbox' environment for a short period of time that does not include any actual consumer data, and which may not accurately reflect the scope and scale in which the DROP will be applied in a 'live production' environment.

As noted below, we have identified numerous technical, operational, and legal-policy issues that CalPrivacy should address in order to ensure that businesses can effectively comply with the Delete Act and its implementation of the DROP. **In sum, we request that CalPrivacy implement a one-year transitional enforcement policy and 90-day cure period for registered data brokers demonstrating good faith compliance efforts.**

2. DROP Technical Implementation Issues

a. DROP 'Uptime' and 'Downtime' Issues: Neither the Delete Act regulations nor DROP specifications indicate any alerting procedures or required 'service level agreements' for its continuous availability (uptime) or when maintenance windows or technical errors disable accessibility (downtime). These are customary requirements for software providers to detail in writing prior to business customer utilization. During DROP sandbox testing, many data brokers identified downtime situations with no apparent advance notice or estimated time period for resolution. There will undoubtedly be regular downtime situations during the first year of the DROP release where data brokers rely on specific uptime periods, and any downtime without warning could result in data broker compliance errors. At a minimum, CalPrivacy should host a publicly facing uptime status page and incident reporting system.

b. Hashing and Matching Issues: In order to accurately apply deletion requests, data brokers must receive hashed information from DROP and then match these hashes precisely to hashed

data the data broker processes from their own systems. There are numerous issues data brokers have encountered while testing the DROP sandbox data, and may yet encounter with the live production data, including:

i. *Large Scale Processing Errors:* As DROP is currently estimated to include more than 350,000 records across multiple disparate lists which may scale precipitously over time, there may be computational processing challenges matching such large files across multiple lists and systems. These challenges could result in timeouts, memory or hardware deficiencies, and incomplete matching results. Small businesses may be especially ill-equipped to process such large files, and need time to upgrade their systems or outsource these activities to qualified vendors following the immediate release of the DROP and/or over time as DROP registrations potentially increases to include millions of California consumers.

ii. *Matching Discrepancies:* The DROP matching protocols require precise alignment between the consumer-entered information and the data broker-managed information. Simple variations in spelling, syntax, and completeness of records will result in non-matching scenarios. In addition to spelling errors, there are many examples where data brokers process data associated with a DROP consumer, but will not match due to these discrepancies, including:

- Nicknames or length variances of first names;
- First and last name only represented on one list, where it could be differentiated (e.g., marriage) or removed across multiple lists;
- Only processing the first letter of a first name in conjunction with a last name;
- ZIP code differences with previous addresses or recently updated changed addresses;
- Language, formatting, or character variations not yet identified in the DROP specifications; and
- Industry-specific standardization issues, such as the difference between DROP's 32 character hashing protocol and some leading advertising services utilizing 36 character hashing protocols, which leads to a mismatch between DROP and industry standards.

c. Application Programming Interface (API) Issues: A data broker is only issued one key for their entire business, and this key is persistent without the ability to change (only regenerating the same key). This could lead to operational or security issues if the employee managing the keys leaves the company or when authorization credentials are compromised. Data brokers have also identified missing features with the sandbox API, notably the need for more automated testing and real-time reporting capabilities.

d. Reporting Errors: The process for submitting amended reports can use additional clarification, particularly regarding amended reports related to status code differences, amendments that span across multiple months, and/or only are identified during an audit period. In addition, the file naming conventions require complex saving mechanics, where a more universal identifier would be easier to manage across multiple lists.

e. Creation of a DROP Software Development Kit (SDK): Rather than relying exclusively on technical instructions and limited software tools to comply with DROP hashing requirements, CalPrivacy could release an SDK that more fully enables data brokers to standardize their hashing and matching approaches, including support for additional languages and SQL dialects.

f. Creation of a dedicated support team: CalPrivacy is strongly encouraged to hire additional DROP support personnel who can help implement and maintain improved real-time ticketing, support tools, and escalation methods for timely support feedback.

3. Operational Application Issues

a. Date of Birth and ZIP Code Matching Requirements: The current DROP specification requires a date of birth and ZIP code in order to match with a consumer's first name and last name. Many data brokers do not process these two data points, have incomplete or incorrect dates, which will result in a very low match rate even though said data brokers are in possession of those consumers' information. Additional lists with variations of designated attributes should be considered if CalPrivacy is seeking to improve overall match rates. CalPrivacy may also seek to include the consumer's California residency-verified full postal address in addition to, or to replace a date of birth, either of which could improve match rates.

b. Business vs. Technical Account Management: DROP currently only allows for one business registration, with no designated role specificity. Most enterprise software applications allow for businesses to designate additional roles, especially because the person who registers a business with DROP is unlikely to be the same person who manages the technical operations with DROP processing activities. A senior executive or legal representative may be responsible for the account administration, and should be able to delegate access and update any accounts for personnel who manage technical DROP operations. This would also improve security protocols in the event of employee turnover or unauthorized access. There could also be 'view only' access for auditors, or 'sandbox only' access for developers. Finally, any potential delays in managing account recovery access during such turnover or incident-response events could result in a business suffering inadvertent compliance errors.

c. Third-Party DROP Management Services: Numerous service providers have engaged data brokers to provide DROP account and data management services. Neither the Delete Act nor DROP specifications clarify how these third parties may be delegated account access, manage DROP data without potential liability to CalPrivacy (or California enforcement in general), and whether these entities may operate across data brokers to provide combined services such as ensuring licensed data from one data broker to another is DROP compliant. These issues should be addressed in further regulations, account management controls, and/or DROP specifications which may include a 'DROP Certification' for relevant service providers.

d. Operational Application Questions: There are many instances where data broker processing activities results in discrepancies in matching or reporting DROP applications, including in the following examples:

- i. A data broker may choose to maintain a short, automated data retention period, for example, where data is deleted every 30 days. However, the data broker is only required to access the DROP every 45 days, which could occur after the automated deletion takes place. This would result in a business identifying and consistently reporting negligible match rates. The Delete Act regulations do not indicate any requirements for data brokers to align their data retention periods with their DROP synchronization schedule to ensure the highest number of matches, and a consistent lack of matches may result in a regulatory inquiry. Additional clarity from CalPrivacy about how businesses should engage in 'data minimization' practices is welcomed.
- ii. The Delete Act regulations indicate 'deletion before suppression,' whereas some data brokers may choose to apply a DROP list as an automated suppression list prior to attempting to match DROP lists to its databases for deletion purposes. Since this 'suppression first' process would be effective in ensuring no DROP consumers' data are 'sold,' CalPrivacy is encouraged to clarify that any suppression effort prior to deletion efforts is an acceptable practice.
- iii. Data brokers often synchronize numerous attributes and identifiers together in an identity graph or through other 'probabilistic' matching methods. Further regulation or guidance is needed to clarify the use of some of these matching methodologies, and how extenuated a potential identifier or attribute is from being applied to a DROP consumer and/or a DROP household.

iv. Building on the prior item, consumers entering a connected TV identifier (“CTV ID”) into the DROP will commonly be used as a ‘household’ identifier rather than an individual identifier. Businesses utilizing CTV IDs often attempt to match additional device identifiers together with a CTV ID, which could be additional CTV IDs for other TVs in the household, mobile ad IDs, hashed emails associated with the same CTV account, or IP address. These multiple disparate IDs are often probabilistically synchronized together, as these identifiers may not be known to be owned by the same DROP consumer or members of the same DROP consumer household. CalPrivacy should clarify that the CTV ID is deemed to be a ‘household-only’ identifier and be distinct in DROP application from all other probabilistic matched identifiers that are not specifically included on a DROP list. In addition, some mobile ad identifiers (e.g., iPad) may also be deemed a household-level identifier.

e. Residency Validation Issues: Since DROP live production data became accessible July 28, 2026, some data brokers have indicated that a number of identifiers may be associated with postal addresses of residences outside of California. CalPrivacy should engage with registered data brokers to determine a process to ensure that the California residency verification mechanism is accurate. Moreover, CalPrivacy has not indicated in any regulations how residency will be re-verified in 2027, and how businesses are expected to remove non-residents from DROP following invalidation.

f. Exception/Exemption Issues: Data brokers may have multiple different business uses for data that includes exemptions in one application but may yet be deleted or suppressed in another application. The current reporting may create confusion where multiple categories are identified as both deleted and exempted at the same time, which can use additional clarifications how CalPrivacy will review or investigate such instances.

g. Consumer Choice Change Management: The DROP specifications are unclear on the process for businesses to correct DROP registrations when consumers return to their DROP account interface in order to change their data broker-specific preferences. This could occur repeatedly and lead to both application and reporting discrepancies. Additional clarity is requested to confirm the correct methods to apply such consumer-directed changes, and whether CalPrivacy will restrict consumer changes to a certain number per year or restrict to a certain number of days following a previous change. There are additional legal and policy questions whether a consumer choice to remove a specific data broker may be deemed consent for that data broker to continue or resume sales, if that consent indication can be auditable.

4. Legal and Policy Issues

a. Use of Proprietary Pseudonymous IDs: Some businesses that ‘sell’ data to data brokers utilize a proprietary identifier ID, which may be a hashed derivative of an email address but uses a different hashing protocol from DROP. As a result, the data broker licensing this proprietary ID does not maintain any mechanism to apply the DROP hashed email list to this proprietary ID, even though the data may be associated with the same individuals. CalPrivacy should clarify in regulations that licensors of proprietary IDs are legally responsible for sharing DROP updates so data broker licensees can properly apply DROP updates with proprietary ID uses.

b. Clarify Downstream Licensing Requirements: Neither the Delete Act regulations nor DROP specifications specify timing for data licensors to require data licensees to apply updated files that comply with the DROP. When a data broker licenses personal data from another registered data broker, is the data broker licensor required to stipulate any time periods for application of updated DROP records? Or are general ‘compliance with law’ terms sufficient since the data broker licensee maintains independent requirements to comply with the DROP? Are there any ramifications for data brokers who rely on a data broker licensor to comply with the DROP on their behalf prior to the

data broker licensee's synchronization with the DROP where no matches may be required to be identified if all of their licensed data is from other registered data brokers?

c. Reporting issues: There will be instances when a data broker is required to report on corrected data errors, for example, in instances where data brokers identify DROP records in tertiary databases and report that the data broker did not apply DROP deletions in a timely fashion. In some cases, these later match reports could be materially different from their historical reporting, which could trigger regulatory scrutiny by CalPrivacy.

d. Audits and Current DROP Processing: It is unclear how the pending DROP audit regulations will interplay with current consumer DROP requests. Data brokers cannot anticipate all of the potential record keeping requirements as of the effective date of DROP. Will DROP maintain all records necessary for auditing on behalf of data brokers until data brokers are provided with their audit obligations?

e. Notice and Comment Period for DROP Updates: As CalPrivacy updates and/or addresses DROP issues, CalPrivacy should seek input from data brokers prior to making changes. CalPrivacy should hold regular stakeholder meetings to discuss the above issues and future updates. Moreover, CalPrivacy should not update and/or change DROP without providing notice to all data brokers of the changes well in advance of any changes. The same should be done for software updates that change how data brokers and consumers interact with DROP.

f. Interaction between § 1798.99.85 of the Delete Act and DROP Request Reports: It is unclear how the DROP requests interplay with the Delete Act reporting metrics detailed in § 1798.99.85 of the Delete Act. In particular, how do the DROP report categories ("Record Exempted," "Record Deleted," "Record Opted Out," and "Record Not Found") fit into the enumerated reporting metrics (requests received, complied with in whole, complied with in part, denied, if denied the reason for denial, median, and mean? What about redundant requests (i.e. prior requests data brokers have received from consumers directly, or from authorized agents, that the data broker receives again via DROP)?

5. Request for Transitional Enforcement and Cure Period

The DROP is a novel approach to regulatory compliance, as well as a complex enterprise software and data management system. As with all other novel software, it will take time to properly function as intended without technical errors or user issues. If the DROP were being implemented by any software company, the August 1 start date would be a 'beta' period because no live data has been available on DROP for any meaningful time period prior to this date. A beta period would give CalPrivacy time to find bugs, test real-world performance, and gather feedback from enterprises before engaging in any potential enforcement actions related to discrepancies associated with its use.

As currently implemented, CalPrivacy could immediately issue statutory penalties under the Delete Act for any errors by data brokers with their implementation of the DROP. With statutory penalties of \$200 per consumer request per day, any delay or list transmission error could result in significant penalties that could automatically bankrupt enterprises that attempted to comply with the DROP. A data broker could even be penalized where the DROP itself caused the error, such as with downtime or account management delays.

In consideration of the issues identified above, we are requesting that CalPrivacy implement a formal transitional enforcement policy that delays enforcement actions for a minimum of one year against registered data brokers who attempt in good faith to comply with the DROP. Our recommendation for such a safe harbor is detailed below.

1. Applies to registered data brokers that attempt to access DROP every 45 days following the August 1, 2026 implementation date and every 45 days thereafter, and:
 - a. Maintain documented procedures for attempted application of DROP lists, including with any vendors or service providers;
 - b. Attempt to upload data matching reports to DROP within 45 days of list download; and
 - c. Report any discrepancies to CalPrivacy in a reasonable fashion.
2. In the event that CalPrivacy identifies a discrepancy or issue with a data broker's use of the DROP, the data broker is provided with adequate written notice and the opportunity to cure the identified discrepancy within 90 days of notice (while continuing to apply regular DROP updates).

IHP appreciates CalPrivacy's consideration of this request and would welcome the opportunity to meet with CalPrivacy staff, participate in stakeholder discussions, or provide additional technical and operational information regarding DROP implementation.

Signed,

Benjamin Isaacson, Principal, In-House Privacy, Inc. (CalBar #276652)

ben@inhouseprivacy.com

Repost - Amid Industry
Backlash, Some Say NJ Data
Broker Law Adds Important
Consumer Protections

