Catbagan, Christian@CPPA

From: Seamus Abshere <seamus.abshere@faraday.ai>
Sent: Tuesday, April 7, 2026 4:33 PM
To: Regulations@CPPA
Subject: Preliminary Comment – DROP Audits

I am the CTO at Faraday, a registered CA data broker. For the audit, I recommend you follow this procedure:

1. Document for and screenshare with the auditor to show how suppression works
    1. Show the auditor where allowed suppression information is stored (database)
    2. Show the auditor what logs indicate that suppression is happening
2. Provide the auditor with access to the outputs of the data broker that include CA residents
    1. Have the auditor randomly pick 10-100 CA residents **from the outputs**
    2. Have the auditor submit them as suppressions
3. After X days, audit the system
    1. Ensure that the chosen people have been suppressed from the output
    2. Ensure allowed suppression information is in the expected storage
    3. Ensure that logs indicate suppression happened

Therefore the auditor needs:

- Access to output BEFORE random suppression
- Access to storage (database)
- Access to logs
- Access to output AFTER random suppression

This causes random CA residents to be suppressed from the data broker output. However this does not harm those CA residents and guarantees all other CA residents are protected.

--
Seamus Abshere
Co-founder and CTO
Faraday
Office: (802) 458-0441 ext. 305
Cell: [redacted] (plz SMS first, 8am-8pm Eastern OK)
[redacted]

https://faraday.ai
https://github.com/seamusabshere
https://www.linkedin.com/in/seamusabshere
https://seamus.abshere.net

Catbagan, Christian@CPPA

From: Milo Palacios <mpalacios@m1-data.com>
Sent: Thursday, April 9, 2026 7:54 AM
To: Regulations@CPPA
Subject: PRELIMINARY COMMENTS for DROP Platform Audits

Good morning,

Please see the feedback below regarding the comments for audits. My responses are in blue.

Questions for Preliminary Comment

1. What credentials, certifications, or independence requirements do you recommend third party auditors possess to ensure they are qualified and sufficiently independent?

Third-party auditors should hold a SOC 2 certification at minimum, since it covers the core areas relevant to this kind of work — data security, availability, and confidentiality. On top of that, auditors should have hands-on experience in data privacy, not just general auditing. DROP audits deal with things like data matching, hashing, deletion, and suppression lists, so the auditor needs to actually understand how that stuff works in practice.

2. What records, documentation, or other evidence would demonstrate in an audit whether a data broker has properly processed consumer deletion requests?

Data brokers should be required to maintain documentation that shows how they match incoming deletion requests to their existing data — whether that's through hashed identifiers or plain text matching when provided. For each deletion request processed, there should be a timestamp showing when the request was received and when it was completed. Brokers should also be able to demonstrate that matched records were actually deleted and that the only data retained from those requests lives on a suppression list used solely to prevent that consumer's data from being re-added in the future.

3. What audit practices, methods, standards, and/or technical tools should CalPrivacy consider adopting as requirements for data broker audits? Are there additional or different audit requirements you recommend when a data broker uses artificial intelligence (AI) or agentic AI systems?

Reporting-based audits should be sufficient.

4. What audit requirements would allow CalPrivacy to determine if it should be requesting different identifiers from consumers to generate the highest number of matches between the DROP data and the data broker's data?

Zip code alone is too loose of an identifier to reliably match consumers to a data broker's records. Without more specific information, there's no way to guarantee the correct person is being matched and opted out. CalPrivacy should consider collecting additional identifiers such as full name, email address, and full street

address including zip code. The more data points available for matching, the higher the accuracy and the lower the risk of false matches or missed deletions.

Thank you,

Catbagan, Christian@CPPA

From: [redacted]
Sent: Monday, April 13, 2026 6:41 PM
To: Regulations@CPPA
Subject: Unethical practices
Attachments: Gmail - [redacted]pdf; Screenshot 2026-04-13 at 6.29.32 PM.png

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

To whom it may concern,

I have dealt with numerous data brokers throughout 20 years that have kept me hostage and required an insurmountable amount of my time to monitor and continue removing mmy info.

Today, I tried to remove my info from this site that is unethically creating a grey area by forcing and subjecting us to provide personal information in order to have our info removed.

Their trick is that they've listed me and my family with the unique last name of [redacted] and they use [redacted] but everyone's city and state are incorrect. Therefore based on their policy, if our ID or document doesn't have the correct address exactly as shown on "their" website, we cannot get it removed. They have deliberately got the city and state wrong because they know that we wouldn't have that address on our ID in order to request that it be removed.

I searched for my name [redacted]
found my info on their site:
[redacted]

Saw my family's info too and although [redacted] the city and state has been replaced so that they would have a legal excuse to not remove it. based on their removal policy. I have followed all their instructions and have included their emall response which I've attached here.

This needs to stop as they are causing stress and simply taking our time hostage at their will. Please do something about this once and for all and share this with your complaints department. They should be fined.

Sincerely,
[redacted]

Catbagan, Christian@CPPA

From: Mansoor Siddiqui <mansoor@ephemeralsocial.com>
Sent: Monday, April 20, 2026 12:12 PM
To: Regulations@CPPA
Subject: Preliminary Comment – DROP Audits April 2026
Attachments: Siddiqui_Preliminary_Comment_DROP_Audits_April_2026.pdf

Hi there,
Thank you for the opportunity to comment and please find attached my submission.

Thanks,
Mansoor Siddiqui
Ephemeral

Date: April 20, 2026

To:
California Privacy Protection Agency
Attn: Legal Division, Regulations
400 R St., Suite 350
Sacramento, CA 95811
regulations@cppa.ca.gov

Re: Preliminary Comment – DROP Audits April 2026

Statement of Interest

My name is Mansoor Siddiqui. I am the developer of Verifiable Delete, an open-source (MIT-licensed) deletion verification framework built in TypeScript and deployed on Cloudflare Workers.[1] The technical recommendations in this comment are informed by building and deploying this system: envelope encryption, threshold key management, post-deletion storage scanning, W3C Verifiable Credential deletion receipts, and a Merkle tree transparency log. I submit these comments in my capacity as an independent software engineer and technologist, not on behalf of any trade association or advocacy organization.

I appreciate the opportunity to respond to CalPrivacy's Invitation for Preliminary Comments on data broker audit requirements under Civil Code Section 1798.99.86(e). The recommendations below are organized by the six questions CalPrivacy has posed.

[1] Source code: https://github.com/ephemeral-social/verifiable-delete (263 tests, MIT license). Landing page and deletion receipt browser: https://verifiabledelete.dev. Scanner Agent (12 backend connectors): https://github.com/ephemeral-social/verifiable-delete-scanner-agent.

Executive Summary

CalPrivacy is designing the first audit framework in the United States for verifiable data deletion at scale. The technical standards adopted here will define what "deletion" means in practice for the 575+ registered data brokers processing deletion requests from the more than 242,000 Californians who have registered on DROP since its January 2026 launch.

Four recommendations:

1. Distinguish process compliance from outcome verification. Current enterprise deletion tools confirm that a deletion command was executed. They do not confirm that data is actually inaccessible. Audit standards

should require evidence of both.

2. Require cryptographic erasure with key-lifecycle documentation for data stored in backup systems. The European Data Protection Board's CEF 2025 Report on the right to erasure found that half of the 32 participating supervisory authorities flagged backup erasure as a systemic failure.[2] Cryptographic erasure (encrypting data and destroying the key) is the only practical technique for rendering backup data inaccessible without locating and overwriting every copy. NIST SP 800-88 Rev. 2 classifies cryptographic erasure as a Purge-level technique and states that for virtual and logical storage, there may be no viable purge alternative to cryptographic erase (§ 3.1.2).[3]

3. Require machine-readable deletion records, not screenshots. Auditors should be able to verify deletion evidence programmatically. ISO/IEC 27040:2024 specifies minimum elements for certificates of sanitization (control TC-SNTZ-G09). CalPrivacy should adopt equivalent requirements.

4. Require simulated deletion testing as an audit practice. CalPrivacy's own Cybersecurity Audit Regulations (approved September 2025) require auditors to evaluate data retention schedules and proper disposal of personal information (§ 7123(c)(16)), and mandate that audit findings be based on specific evidence, including sampling and testing, rather than management assertions (§ 7123(e)).[4] The EDPB's CEF 2025 Report identifies simulated erasure requests as a best practice for testing staff readiness to handle deletion requests.[5] The DROP audit framework should extend these principles: auditors should submit test deletion requests and verify end-to-end processing, including downstream service providers.

---

[2] EDPB, 2025 Coordinated Enforcement Action: Implementation of the right to erasure by controllers (CEF 2025 Report), adopted 10 February 2026, published 18 February 2026, Issue 6 ("Deletion of personal data in the context of back-ups").

[3] Chandramouli R, Hibbard EA (2025) Guidelines for Media Sanitization. NIST SP 800-88r2, § 3.1.2.

[4] CPPA, Cybersecurity Audit Regulations, Cal. Code Regs. tit. 11, §§ 7120-7124, approved by the Office of Administrative Law on 22 September 2025; effective 1 January 2026.

[5] EDPB, CEF 2025 Report, Issue 2 ("Absence of, or inadequate training"), best practices identified by participating supervisory authorities.

Response to Question 1: Auditor Qualifications and Independence

What credentials, certifications, or independence requirements do you recommend third party auditors possess?

CalPrivacy should require auditors to demonstrate both privacy-law competence and technical competence in data storage and deletion verification. The current landscape of privacy auditing is dominated by policy-focused assessments. DROP audits must go further because the question is not whether a data broker has a deletion policy, but whether deletion actually occurred across their storage systems.

Recommended qualifications. Auditors should hold or demonstrate equivalence to one of: AICPA SOC 2 Type II attestation authority, ISO/IEC 27001 Lead Auditor certification, or CISA (Certified Information Systems Auditor) designation. At least one member of each audit team should have demonstrated competence in database administration, cloud storage architecture, or data engineering sufficient to evaluate deletion across relational databases, object stores, search indices, and backup systems.

Independence standards. CalPrivacy should adopt independence requirements comparable to those governing AICPA attestation engagements. AICPA AT-C Section 105 requires unconditional independence for all attestation engagements (§ 105.26), and the AICPA Code of Professional Conduct (ET § 1.295) prohibits auditors from providing certain nonattest or consulting services to attest clients.[6] CalPrivacy should codify similar protections: the auditor must not have provided consulting, implementation, or technology services to the data broker within the 12 months preceding the audit engagement, and the auditor must disclose any financial relationships with the data broker or its affiliates.

CalPrivacy's recent enforcement actions demonstrate the agency's willingness to impose ongoing compliance monitoring requirements. The $1.35 million Tractor Supply settlement (September 2025) required annual compliance certifications, quarterly technology scans, and annual third-party audits for four years.[7] The DROP audit regulations should build on this precedent by establishing formal auditor independence conditions.

Proposed regulatory language:

> "*An independent third-party auditor conducting an audit pursuant to Civil Code Section 1798.99.86(e) shall: (1) hold current certification as a Certified Information Systems Auditor (CISA), AICPA SOC 2 attestation practitioner, or ISO/IEC 27001 Lead Auditor, or demonstrate equivalent qualifications acceptable to CalPrivacy; (2) include on its audit team at least one individual with demonstrated technical competence in database systems, cloud storage, or data engineering; (3) not have provided consulting, implementation, or technology services to the data broker within the preceding 12 months; and (4) disclose to CalPrivacy any financial relationships with the data broker or its affiliates.*"

[6] AICPA, AT-C Section 105, Concepts Common to All Attestation Engagements, § 105.26 (independence requirement); AICPA Code of Professional Conduct, ET § 1.295 (nonattest services).

[7] CPPA, Stipulated Final Order, In the Matter of Tractor Supply Company, 30 September 2025.

Response to Question 2: Evidence of Proper Deletion Processing

What records, documentation, or other evidence would demonstrate whether a data broker has properly processed consumer deletion requests?

This is the central question. The California Attorney General's DoorDash settlement (February 2024, $375,000) illustrates what happens when data dissemination outpaces deletion capability. DoorDash sold consumer personal information through marketing cooperatives, and the data was subsequently re-sold downstream by data brokers. Even after DoorDash halted the sales and ordered deletion, the AG found that DoorDash "could no longer control, audit, or restrict further dissemination" of the data because it lacked contractual audit rights over the marketing cooperative.[8] The DROP audit framework should require evidence that deletion actually occurred across all storage systems and downstream recipients, not merely that it was requested.

Recommended evidentiary requirements. Data brokers should be required to maintain, for each deletion request processed through DROP:

a) Request-matching documentation. A record of how the data broker matched the hashed consumer identifiers received from CalPrivacy to records in the broker's systems. This should include: the matching algorithm used, the number of records matched, the number of records not matched (with explanation), and whether any matched records were retained under a statutory exception (with the specific exception cited per record).

b) Deletion-completion records. For each matched record, a timestamped record confirming deletion from every storage system where the record existed. This should distinguish between:

- Primary storage (operational databases): confirmation of row deletion or record removal.
- Secondary storage (search indices, caches, derived datasets): confirmation of removal or invalidation.
- Backup and archival storage: either confirmation of removal from backup sets, or documentation of cryptographic erasure rendering backup data inaccessible (see Question 3 below).

• Downstream service providers and contractors: confirmation from each service provider that the data was deleted pursuant to Civil Code Section 1798.99.86(c)(3).

c) Suppression-list integrity documentation. Evidence that the data broker maintains a suppression list (containing identifiers of consumers who have submitted DROP requests) and uses it to prevent re-acquisition of deleted data, as required by Section 1798.99.86(d). The audit should verify that the suppression list is checked against new data acquisitions at least as frequently as the broker acquires new data.

d) Key-lifecycle documentation (where cryptographic erasure is used). If the data broker uses cryptographic erasure (encryption of data with subsequent key destruction) to address backup persistence, the following documentation should be required: the encryption algorithm and key length used; confirmation that data was encrypted prior to storage (not retroactively); identification of all key copies and their storage locations; timestamped confirmation of key destruction for each copy; and the method of key destruction (zeroization per ISO/IEC 19790 or equivalent).[9]

e) Machine-readable format. Deletion records should be maintained in a structured, machine-readable format (JSON, CSV, or equivalent), not as screenshots, email confirmations, or narrative descriptions. Machine-readable records enable programmatic audit verification and reduce the cost and duration of audits. ISO/IEC 27040:2024 control TC-SNTZ-G09 specifies minimum elements for certificates of sanitization, including manufacturer, model, serial number, sanitization method and technique, tool used, verification method, and signatures.[10]

---

[8] California Attorney General, Settlement with DoorDash, 21 February 2024; analysis from Arnold & Porter, DoorDash Fined $375,000 by California AG in Second-Ever Publicly Disclosed CCPA Settlement, 15 April 2024.

[9] NIST SP 800-88 Rev. 2 (September 2025), § 3.2.5 ("Traceability of CE Operations"), specifies ten required documentation elements for cryptographic erase operations. ISO/IEC 27040:2024 control TC-SNTZ-G05 requires organizations relying on cryptographic erasure to audit their key management architecture to confirm whether destroyed encryption keys are recoverable.

[10] For an open-source implementation of machine-readable deletion records using the W3C Verifiable Credentials Data Model 2.0, see https://github.com/ephemeral-social/verifiable-delete. Each deletion generates a cryptographically signed receipt containing: threshold key-destruction attestations, storage-scan results, a Sparse Merkle Tree non-membership proof, and a Merkle tree inclusion proof. Receipts are browsable at https://verifiabledelete.dev.

Response to Question 3: Audit Practices, Methods, Standards, and Tools

What audit practices, methods, standards, and/or technical tools should CalPrivacy consider adopting?

CalPrivacy should adopt a tiered audit methodology that distinguishes between process audits (evaluating policies, procedures, and documentation) and outcome audits (verifying that deletion actually occurred in the data broker's storage systems). Most existing privacy audit frameworks perform only process audits. DROP audits should require both.

a) Process-audit standards. For evaluating policies, procedures, training, and governance, CalPrivacy should reference AICPA SOC 2 Type II (Trust Services Criteria CC6.5, covering the discontinuation of logical and physical protections only after data is rendered unreadable, and P4.3, covering the secure disposal of personal information) and ISO/IEC 27001:2022 Annex A control 8.10 (information deletion).[11]

b) Outcome-audit practices. For verifying that deletion actually occurred, CalPrivacy should require:

- Simulated deletion requests. CalPrivacy's own Cybersecurity Audit Regulations (approved September 2025) already require auditors to evaluate data retention and disposal practices based on specific evidence, including sampling and testing, rather than management assertions (§ 7123(c)(16) and § 7123(e)). The DROP audit framework should extend this principle: auditors should submit test records to the data broker, request deletion through the broker's systems, and verify end-to-end removal from all storage systems, including backups. The EDPB's CEF 2025 Report identifies simulated erasure requests as a best practice for testing staff readiness to process deletion requests.[12] This is analogous to penetration testing in cybersecurity audits.

- Direct storage-system verification. For a sample of completed deletion requests, auditors should query the data broker's storage systems directly (databases, object stores, search indices, caches) to confirm absence of the consumer's data. This is the equivalent of a financial auditor reviewing bank statements directly rather than relying on the auditee's internal ledger.

- Key-destruction verification (where cryptographic erasure is used). Auditors should verify that encryption keys have been destroyed by attempting decryption of retained test ciphertext. Successful decryption indicates the key was not properly destroyed. Failed decryption confirms key destruction.[13]

c) Cryptographic erasure as a recognized deletion method. NIST SP 800-88 Rev. 2 (September 2025) classifies cryptographic erase as a Purge-level sanitization technique and states that for virtual and logical storage, there may not be a

viable purge alternative to cryptographic erase (§ 3.1.2).[14] ISO/IEC 27040:2024 classifies cryptographic erase within Purge and specifies four conditions for valid cryptographic erasure (control TC-SNTZ-R08): all data must have been encrypted prior to storage; the algorithm must provide at least 128-bit security strength; key entropy must equal or exceed the key length; and all copies of the encryption key must be sanitized.[15]

CalPrivacy should recognize cryptographic erasure as a valid deletion method for backup and archival storage, subject to these conditions and to key-lifecycle documentation requirements.

d) Audit requirements for AI and agentic AI systems. CalPrivacy's invitation asks whether additional audit requirements are needed when data brokers use AI. This question is well-placed. AI systems that process personal information often create derived data (embeddings, model weights, inference caches) that may not be addressed by a standard row-level deletion. Auditors should verify: whether deletion requests remove data from model training datasets and prevent future training on deleted data; whether inference caches or embedding stores containing personal information are cleared; and whether AI-generated profiles or inferences derived from deleted data are also removed.

Proposed regulatory language:

> "*An audit conducted pursuant to Civil Code Section 1798.99.86(e) shall include: (1) a process audit evaluating the data broker's policies, procedures, and training for processing deletion requests; and (2) an outcome audit in which the auditor (a) submits simulated deletion requests and verifies end-to-end processing including deletion from backup systems and downstream service providers, (b) directly queries the data broker's storage systems for a sample of completed deletion requests to confirm data absence, and (c) where the data broker uses cryptographic erasure, verifies key destruction through attempted decryption of retained test data.*"

---

[11] AICPA, 2017 Trust Services Criteria (with revised points of focus, 2022). CC6.5 states: "The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives." P4.3 states: "The entity securely disposes of personal information to meet the entity's objectives related to privacy."

[12] EDPB, CEF 2025 Report, Issue 2 (best practices section). Additionally, a 2025 study by researchers submitting verifiable consumer requests to all 543 California-registered data brokers found a 43% non-response rate, demonstrating that systematic compliance failures are detectable only through test submissions. See Consumer Beware! Exploring Data Brokers' CCPA Compliance, arXiv:2506.21914v2.

[13] This technique is implemented as `verifyKeyDestruction()` in the Verifiable Delete core library. See https://github.com/ephemeral-social/verifiable-delete, packages/core/src/crypto/index.ts.

[14] Chandramouli R, Hibbard EA (2025) Guidelines for Media Sanitization. NIST SP 800-88r2, § 3.1.2 ("Purge Sanitization Method"). Section 3.2 provides detailed guidance on the cryptographic erase

technique, including applicability (§ 3.2.2), key sanitization (§ 3.2.3), quality of cryptographic implementations (§ 3.2.4), and traceability requirements (§ 3.2.5).

[15] ISO/IEC 27040:2024, Information technology, Security techniques, Storage security, § 10.6.5, controls TC-SNTZ-R08 (cryptographic erase conditions) and TC-SNTZ-G05 (key management audit).

Response to Question 4: Identifier Matching

What audit requirements would allow CalPrivacy to determine if it should be requesting different identifiers from consumers?

This question is outside my primary area of technical expertise, but I will note one relevant consideration. Auditors should be required to report the match rate for each audit cycle: the percentage of DROP consumer identifiers that matched records in the data broker's systems. A consistently low match rate (e.g., below 10%) may indicate either that the data broker genuinely does not hold data on most requesting consumers, or that the identifier format used by DROP is insufficient for matching. Auditors should be required to assess which explanation applies and report accordingly.

Additionally, auditors should evaluate whether the data broker's internal hashing and standardization practices are consistent with CalPrivacy's hashing specifications, and identify any systematic causes of match failure (e.g., name normalization differences, address formatting inconsistencies, or lack of a shared identifier such as a hashed email address).

Response to Question 5: Materials Accompanying the Audit Report

What other materials should be submitted to CalPrivacy alongside the audit report?

CalPrivacy should require the following materials at minimum:

1. The audit report itself, including findings, the methodology used, and a compliance determination for each requirement under Section 1798.99.86.

2. A summary of simulated deletion test results, including the number of test records submitted, the percentage successfully deleted from all storage systems, and any failures with root-cause analysis.

3. A data-system inventory listing all storage systems, databases, search indices, caches, and backup systems where consumer personal information is stored, with a statement from the data broker confirming completeness.

4. A downstream service-provider inventory listing all service providers and contractors to whom the data broker has disclosed personal information, with confirmation of deletion from each provider for the audit period.

5. Deletion-method documentation. If the data broker uses cryptographic erasure, a description of the encryption algorithm, key management architecture, key-destruction procedure, and key-lifecycle documentation for the audit period.

6. Match-rate statistics for the audit period: total DROP requests received, total records matched, total records deleted, total records retained under statutory exceptions (with exception category breakdown).

7. A corrective action plan for any deficiencies identified, with timelines.

NIST SP 800-88 Rev. 2 (§ 4.6 and Appendix C) provides a sample certificate of sanitization that includes many of these elements. CalPrivacy should consider adapting this template for DROP audit reporting.

Response to Question 6: Additional Considerations

What else should CalPrivacy consider?

a) The backup erasure problem is the most significant gap in current deletion practice. The EDPB's CEF 2025 Report found that half of the 32 participating supervisory authorities flagged backup erasure as a systemic failure. Many controllers "do not delete or remove personal data from back-ups at all, nor do they have processes to prevent previously deleted data from being restored when back-ups are reinstalled."[16]

This is not a California-specific problem. It is a technical limitation: backup systems are designed to preserve data, and selectively removing individual records from backup tapes, snapshots, and replicated storage is operationally impractical for most organizations.

Cryptographic erasure is the only practical solution for backup storage. If data is encrypted before it is written to any storage system (including backups), and the encryption key is subsequently destroyed, the data is computationally inaccessible regardless of physical persistence. NIST SP 800-88 Rev. 2 states that for virtual and logical storage, there may not be a viable purge sanitization alternative to cryptographic erase (§ 3.1.2). ISO/IEC 27040:2024 specifies four conditions under which cryptographic erasure constitutes a valid Purge-level technique (control TC-SNTZ-R08).[17]

CalPrivacy should explicitly address backup erasure in the audit regulations. Data brokers should be required to either: (a) demonstrate the ability to selectively delete individual records from all backup systems within 45 days of a DROP request; or (b) implement cryptographic erasure meeting the conditions specified in NIST SP 800-88 Rev. 2 and ISO/IEC 27040:2024, with key-lifecycle documentation subject to audit.

b) Downstream service-provider verification is critical. The DoorDash settlement demonstrated that a company's own deletion is insufficient if personal information has been shared with downstream recipients who retain their own copies and lack contractual audit provisions. Section 1798.99.86(c)(3) requires data brokers to "direct all service providers and contractors to delete." The audit regulations should require auditors to verify that this direction was given and that service providers confirmed compliance. For a sample of downstream recipients, auditors should independently verify deletion.

c) Penalty structure should incentivize investment in verification. Under Section 1798.99.82(d), the penalty for failure to comply with Section 1798.99.86 is $200 per deletion request per day. For a data broker processing thousands of DROP requests, non-compliance penalties accumulate rapidly. CalPrivacy should consider whether data brokers that invest in verifiable deletion infrastructure (cryptographic erasure, audit-ready documentation, automated deletion records) should receive favorable audit treatment, such as extended audit cycles or reduced audit scope for demonstrated compliance.

d) Audit transparency. CalPrivacy should consider publishing anonymized, aggregate audit results to establish industry benchmarks. Over time, this data would reveal whether match rates, deletion completion rates, and backup-erasure compliance are improving across the data broker industry, informing future regulatory refinements.

[16] EDPB, CEF 2025 Report, Issue 6 ("Deletion of personal data in the context of back-ups"), pp. 20-22. The report notes practices ranging from complete absence of backup erasure procedures to reliance on automatic overwrite cycles.

[17] NIST SP 800-88 Rev. 2, § 3.1.2 (cryptographic erase as the only viable purge option for virtual/logical storage); ISO/IEC 27040:2024, control TC-SNTZ-R08 (four conditions: prior encryption, ≥128-bit algorithm strength, key entropy ≥ key length, all key copies sanitized).

Conclusion

The audit regulations CalPrivacy develops for DROP will set the first national standard for what "deletion" means in practice. The distinction between process compliance (did the broker have a policy?) and outcome verification (is the data actually gone?) is the most consequential design choice. I respectfully urge

CalPrivacy to require both.

The standards and techniques recommended in this comment are grounded in established NIST and ISO standards and informed by the EDPB's findings across 32 supervisory authorities. I welcome the opportunity to provide technical expertise as CalPrivacy develops these regulations.

Thank you for the opportunity to comment.

Mansoor Siddiqui
Developer, Verifiable Delete
Ephemeral Social PBC
mansoor@ephemeralsocial.com
https://verifiabledelete.dev

Catbagan, Christian@CPPA

From: Kemp, Tom@CPPA
Sent: Tuesday, April 21, 2026 9:11 AM
To: Mansoor Siddiqui
Cc: Regulations@CPPA
Subject: RE: Technical comment on DROP audit requirements + open-source verification tool

Mansoor – Thanks for providing public comments. Be sure to submit any and all additional comments to the email address on the cc: line per https://cppa.ca.gov/regulations/drop_audits.html.

The team will review all comments submitted post the submission deadline and may have followups, so we appreciate the offer.

Thanks, tom

From: Mansoor Siddiqui [redacted]
Sent: Tuesday, April 21, 2026 8:49 AM
To: Kemp, Tom@CPPA <Tom.Kemp@cppa.ca.gov>
Subject: Technical comment on DROP audit requirements + open-source verification tool

Hi Tom,

I'm Mansoor Siddiqui, a software engineer. I just submitted a preliminary comment to CalPrivacy on DROP audit requirements, and I wanted to share it with you directly.

You've said publicly that CPPA needs technologists to help build DROP and the audit function. I took that seriously. My comment proposes cryptographic verification standards for the triennial audits under Section 1798.99.86(e), grounded in NIST SP 800-88 Rev. 2 and ISO/IEC 27040:2024. The core argument: process compliance (did the broker have a deletion policy?) is not the same as outcome verification (is the data actually gone?). DROP audits should require both.

I also build Verifiable Delete, an open-source (MIT-licensed) framework that implements what the comment proposes: envelope encryption with threshold key destruction, post-deletion storage scanning across 12 database types, and tamper-evident deletion receipts (W3C Verifiable Credentials) anchored in a public Merkle transparency log.

Repo: https://github.com/ephemeral-social/verifiable-delete (263 tests)
Landing: https://verifiabledelete.dev

Comment: happy to send the full PDF

I'm available to provide technical expertise as CalPrivacy develops these regulations. Happy to brief your team in any format that's useful.

Thanks,
Mansoor Siddiqui
mansoor@ephemeralsocial.com

Catbagan, Christian@CPPA

From: Adam Wadsworth <awadsworth@ana.net>
Sent: Thursday, May 7, 2026 5:45 AM
To: Regulations@CPPA
Subject: Preliminary Comment – DROP Audits April 2026
Attachments: Ad Trade Preliminary Comments to CalPrivacy on DROP Audits.pdf

Dear California Privacy Protection Agency:

Please find attached the preliminary comments on whether to adopt regulations to clarify or further specify the audit requirement for processing deletion requests from the following advertising trade associations: **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 this letter, please feel free to reach out to Chris Oswald at coswald@ana.net.

Best Regards,
Adam Wadsworth

Adam Wadsworth
Coordinator, Law, Ethics, Govt Relations
Association of National Advertisers (ANA)
P: 202.861.2430 | C: [redacted] | ana.net | LinkedIn
2020 K Street, NW, Suite 660, Washington, DC 20006
The ANA drives growth for you, your brand, our industry, and humanity. Learn how at ana.net/membership.

May 7, 2026

Via electronic filing: regulations@cppa.ca.gov

To: California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R St., Suite 350 Sacramento, CA 95811

Re: Preliminary Comment – DROP Audits

On behalf of the advertising industry, we provide the following comments in response to the California Privacy Protection Agency's ("CalPrivacy" or "Agency") invitation for preliminary comment on potential regulations related to audit requirements for processing deletion requests through the Delete Request and Opt-Out Platform ("DROP").[1] We appreciate CalPrivacy's efforts to seek stakeholder input at an early stage to help ensure that any future requirements are workable and aligned with the California Delete Act ("Delete Act"). At the same time, we have concerns about certain topics identified for possible new rulemaking and the direction under consideration by the Agency. Below we provide comments on a non-exhaustive list of issues we have identified with the Agency's preliminary rulemaking efforts. We intend to remain engaged should the Agency move forward with formal rulemaking.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,000 companies that power the commercial Internet, which accounted for nearly 20 percent of total U.S. gross domestic product ("GDP") in 2024.[2] By one estimate, approximately 18.9% of California jobs in 2024 were related to the ad-subsidized Internet, a share projected to increase to 20.7% by 2029.[3] 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 Agency further as it reviews submitted preliminary comments and considers whether new regulations are necessary.

I. The Delete Act clearly established DROP audit requirements, and there is no record to demonstrate that regulations are necessary to facilitate compliance with this requirement.

The Delete Act established a specific audit requirement mandating that, "…[b]eginning January 1, 2028, and every three years thereafter, a data broker shall undergo an audit by an independent third party to determine compliance…" with the statute.[4] This provision reflects a targeted legislative approach: requiring audits while preserving necessary flexibility in how

[1] California Privacy Protection Agency, Invitation for Preliminary Comments, located here.
[2] S&P Global, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY, 2024-2029 at 4 (Aug. 2025), located at https://theadcoalition.com/wp-content/uploads/2025/08/TAC_SP-Global-Final-Report_August-2025.pdf.
[3] *Id.* at 15-16.
[4] Cal. Civ. Code § 1798.99.86.

businesses conduct their internal processes to process and effectuate deletion requests. The statute's audit requirement is unambiguous, and since the provision goes into effect beginning in 2028, the record does not yet demonstrate a need for additional regulation or agency involvement. Nothing in the statute requires the Agency to prescribe how companies must design, implement, or operationalize required audits. Rather, the California Legislature defined the required outputs (i.e., audit reports and related materials) without mandating the precise inputs or methodologies by which entities must achieve DROP compliance. The Agency should avoid stepping into areas that are the purview of the legislature by imposing detailed technical specifications governing audits or DROP compliance systems via regulation. If CalPrivacy promulgates regulations that impose obligations beyond those expressly set forth in the statute, the Agency would risk upsetting the balance struck by the legislature between accountability and operational flexibility, and opens the Agency to criticism of scope creep.

II. The scope of any regulations should be limited to what is necessary for DROP audit compliance.

Any implementing regulations should be narrowly tailored to what is necessary to effectuate compliance with DROP audit requirements. The Agency's role in this context is to facilitate compliance with the law and not to seek to expand the scope of underlying statutory obligations. If CalPrivacy proceeds with issuing regulations, the rules should focus on discrete procedural elements, such as clarifying the timing and method for submission of the required audit reports. Any associated recordkeeping requirements should be limited to materials that are reasonably necessary to substantiate compliance with the statute's audit provisions.

CalPrivacy should not prescribe how companies design or operationalize their deletion systems, including the technical design of databases or other proprietary infrastructure or vendors in place to process deletion requests. Any regulation with prescriptive requirements regarding DROP request implementation would risk stifling innovation and imposing unnecessary costs on businesses without corresponding compliance benefits. Similarly, the Agency should avoid creating expansive documentation requirements that extend beyond what is needed to validate deletion request processing. The statute already contemplates a targeted audit regime centered on submission of an audit report and related materials, which clearly does not give CalPrivacy any mandate to require ongoing, open-ended documentation or enterprise-wide examinations.

We are particularly concerned that certain elements of the invitation for preliminary comment include questions related to artificial intelligence ("AI") and agentic AI systems, suggesting a potential expansion of the audit framework into other areas not contemplated by the Delete Act. AI considerations are not germane to the statute's audit requirements, which are central to this pre-rulemaking exercise.

For these reasons, any implementing regulations should remain tightly aligned to the stated objective: the DROP audit process as mandated by the Legislature. The Agency should ensure any regulations on audits reinforce the statute, which allows for flexibility in the execution of an audit to verify a business's compliance with the DROP. These regulations should not serve as a vehicle for broader reach to unrelated data practices.

* * *

To the extent the Agency seeks to ensure that audits are independent and effective, it should prioritize flexibility over prescriptive mandates, support competition and cost-efficient audit measures, and promote efficiency. Above all, any regulations should remain grounded in the statute.

We intend to remain engaged and to participate in any formal notice-and-comment process should proposed regulations be issued. We welcome further opportunities to engage with the Agency to help ensure that any approach is both practicable and consistent with the Delete Act.

Thank you in advance 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
Matthew Stern, Venable LLP

Catbagan, Christian@CPPA

From: Lindsey Stewart <lindsey.stewart@zoominfo.com>
Sent: Thursday, May 7, 2026 10:57 AM
To: Regulations@CPPA
Cc: Bubba Nunnery
Subject: Preliminary Comment – DROP Audits April 2026
Attachments: ZI CPPA Comments 5.7.26.pdf

Good afternoon -

Thank you for the opportunity to submit comments for the DROP Audits (attached). Please reach out for any additional questions or for more information.

--
Lindsey Stewart, CIPP/US
Senior Director, Government and Regulatory Affairs
M: [redacted]
E: lindsey.stewart@zoominfo.com

zoominfo

330 W Columbia Way, Floor 8
Vancouver, WA 98660

866.904.9666
zoominfo.com

May, 2026

California Privacy Protection Agency
400 R Street, Suite
350 Sacramento, CA 95811

Dear California Privacy Protection Agency,

ZoomInfo is a software and data company that provides information for business-to-business sales, recruiting, and marketing. We are committed to consumer privacy and believe that well-designed audit requirements are an important tool for ensuring that data brokers are meaningfully honoring deletion requests and earning consumer trust.

We appreciate the opportunity to submit comments on the Agency's preliminary questions regarding audit requirements under the Delete Request and Opt-Out Platform (DROP), and offer the following recommendations with the goal of building a framework that is both rigorous in protecting consumers and workable in practice. Our comments correspond to each of the Agency's six questions.

1. Auditor Credentials, Certifications, and Independence Requirements

CalPrivacy should recognize existing credentialing frameworks-

A qualified, independent auditor pool is essential to meaningful consumer oversight. Rather than creating a novel DROP-specific credentialing regime, CalPrivacy should recognize existing credentialing frameworks as establishing presumptive auditor qualification. Specifically, CalPrivacy should accept firms accredited by the AICPA and certification bodies accredited by a recognized national accreditation body such as ANAB.

CalPrivacy should provide a clear definition of "independence"

CalPrivacy should also publish a clear regulatory definition of "independence" addressing structural independence, conflict-of-interest prohibitions, auditor competency, and scope integrity. Independence standards should address not only the auditor's relationship to the audited entity, but also any commercial relationships that could create misaligned incentives within the audit ecosystem. The credibility of the audit mechanism with the public rests, in part, on assurance that the oversight process itself is not shaped by commercial interests.

2. Records and Documentation Requirements for Audit Purposes

Transparency in the audit process serves consumers. We support CalPrivacy's ability to verify that deletion requests are being honored. However, certain documentation underlying a data broker's compliance processes may constitute trade secrets. Disclosure of trade secret materials outside of a controlled process—even to a government agency—can erode the legal protections those materials would otherwise carry. We recommend that CalPrivacy balance transparency with the protection of legitimate business secrets by adopting a tiered disclosure framework: auditors receive full access to documentation; CalPrivacy receives a summary audit report; and detailed technical documentation is retained by the data broker and produced to CalPrivacy only upon specific written request with appropriate confidentiality protections.

3. Audit Practices, Methods, Standards, and Technical Tools

Audit standards grounded in established, recognized frameworks will produce more consistent consumer protections than novel requirements developed in isolation. CalPrivacy should align DROP audit requirements with its existing CCPA cybersecurity audit methodology where possible, reducing duplicative burdens while reinforcing a coherent privacy compliance ecosystem. Rather than mandating specific proprietary tools—which risks inconsistency and disproportionate costs—CalPrivacy should specify functional requirements (e.g., auditors must use tools capable of verifying deletion execution at scale), giving auditors the flexibility to apply appropriate instruments while ensuring the consumer-protective outcome is verifiable.

4. Audit Requirements to Optimize Identifier Collection

Auditors should be required to report match rate by identifier type -

Effective deletion depends on accurate matching, and match accuracy ultimately determines whether DROP delivers its consumer-protective promise. Auditors should be required to report match rate data by identifier type — including the percentage of DROP requests that did and did not result in a match — so that CalPrivacy can use aggregate data to evaluate whether current identifier collection is sufficient and to inform future rulemaking. Where low match rates reflect identifier limitations rather than non-compliance, this data should guide system improvements rather than trigger penalties against data brokers acting in good faith.

Auditors should assess if consumers are provided sufficient context -

CalPrivacy should also consider whether DROP's current design adequately accounts for the distinction between a consumer's personal and professional identities. A consumer who registers for DROP to remove personal residential information from people-search platforms may not intend — or fully understand — that the same request will delete their professional profile from B2B platforms, potentially affecting

their professional visibility or business relationships. Auditors should therefore assess whether consumers are provided sufficient context at registration to make an informed, intentional choice about the scope of their deletion request. Ensuring consumers understand what they are deleting is itself a consumer protection obligation that DROP's current framework does not clearly address.

5. Materials to Be Submitted Alongside an Audit Report

To support meaningful Agency oversight without creating unnecessary disclosure risks, accompanying materials should be limited to what is necessary for CalPrivacy to evaluate the audit's scope, methodology, and findings. We recommend CalPrivacy develop a standardized audit report template specifying required submission elements — such as auditor qualifications and independence attestation, the audit period and systems reviewed, match rate data by identifier type, and a structured summary of findings and remediation actions. A standardized format would give CalPrivacy consistent, comparable information across the regulated community without requiring ad hoc disclosure of competitively sensitive technical detail. Where CalPrivacy determines that underlying technical documentation is necessary, data brokers should be permitted to designate such materials as confidential trade secrets at the time of submission.

6. Additional Considerations

An effective audit framework should reward genuine investment in privacy compliance and give regulated entities the clarity they need to meet consumer expectations. We recommend three additional measures:

Streamlined audit pathway

Data brokers holding recognized third-party certifications — such as ISO 27701 or SOC 2 Type II — should be eligible for a streamlined audit pathway. ISO 27001 establishes a comprehensive privacy information management framework that directly maps to data subject right obligations, including deletion. SOC 2 Type II reports provide independent verification of operational controls over a sustained period of time. Each of these certifications demonstrate compliance with technical and organizational controls already verified by those certifications. To the extent CalPrivacy is concerned these existing certifications may not fully encompass DROP-specific workflows, we recommend a streamlined pathway that requires data brokers to submit a scope attestation confirming that their certified control environment includes data subject deletion request processing. The proposed targeted attestation, rather than a full duplicative audit, would provide assurances while preserving the efficiency rationale of a streamlined pathway. This is not an exemption from scrutiny; it is a proportionate allocation of audit resources that directs CalPrivacy's oversight toward areas not already covered by rigorous independent review, while incentivizing

the kind of proactive compliance investment that ultimately benefits consumers.

This approach is consistent with established regulatory precedent: the FTC has recognized ISO-aligned frameworks such as NIST in enforcement contexts involving consumer privacy and data security. GDPR supervisory authorities have treated certification status as evidence of compliance with the obligations those certifications cover. For CalPrivacy to adopt the same principle would align California with this broader regulatory consensus — and establish a model for other states to follow.

Phased implementation

We recommend that first-cycle audit findings result in remediation plans with defined timelines rather than penalties, absent evidence of willful non-compliance. This approach improves consumer outcomes by driving genuine correction rather than penalizing early-stage implementation gaps in a system that is itself still maturing.

Model documentation

CalPrivacy should publish model audit scope documents and sample report templates no later than 12 months before the first audit cycle — consistent with the standardized reporting framework. Clear, published standards benefit consumers by promoting consistency in how deletion rights are verified across the regulated community, and give data brokers sufficient lead time to align their compliance infrastructure accordingly.

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

Catbagan, Christian@CPPA

From: Aodhan Downey <adowney@ccianet.org>
Sent: Thursday, May 7, 2026 1:00 PM
To: Regulations@CPPA
Subject: CCIA's Preliminary Comment – DROP Audits | CCIA Comments on CalPrivacy's Request for Comment on DROP Audit Provisions
Attachments: 2026-05-07 CCIA Comments on CA DROP Audits.pdf

Good Afternoon,

Please find attached the Computer and Communication Industry Association's comments regarding the California Privacy Protection Commission's request for comment on the DROP audit rulemaking provisions. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.

Thank you for your consideration. Should you have any questions, please don't hesitate to contact me at adowney@ccianet.org.

Thank you,
Aodhan Downey

--
Aodhan Downey
State Policy Manager, West Region
adowney@ccianet.org
o: 202-807-5284 M: [redacted]

Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.org | @CCIAnet

Before the
California Privacy Protection Agency
Sacramento, CA

In re

Preliminary Comment– DROP Audits

COMMENTS OF

THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the California Privacy Protection Agency ("CPPA")'s invitation for preliminary comments on delete request and opt-out platform audits, the Computer & Communications Industry Association ("CCIA")[1] submits the following comments.

I. What credentials, certifications, or independence requirements do you recommend third party auditors possess to ensure they are qualified and sufficiently independent?

Auditors should possess expertise in data privacy and cybersecurity, particularly the technical and operational aspects of privacy program management. CPPA guidance should list numerous professional certifications, accreditations, and other standards which will automatically qualify an auditing organization to provide the necessary evaluations. It should also list a process for reviewing and adding further certifications to this list as industry standards further develop. However, this list of automatically qualifying certifications should serve as a floor rather than a ceiling: when covered entities choose an auditor, they should have a broad list of options that are known to meet the law's requirements.

[1] CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at http://www.ccianet.org/members.

II. What records, documentation, or other evidence would demonstrate in an audit whether a data broker has properly processed consumer deletion requests?

Since each covered business will process data in unique ways, businesses' processes for ensuring that the necessary data is deleted will vary. Therefore, rather than require specific documentation, CPPA rules should allow covered entities to provide the third party auditor with any evidence they feel sufficiently demonstrates compliance with the technical requirements in Section 1798.99.86 of the California Civil Code, e.g. evidence that all verified deletion requests were adhered to within 45 days using secure methods, and evidence that all requests not adhered to were not verifiable, or that another permitted exemption applies.

The third party auditor should then assess compliance with these requirements from a technical standpoint, not a legal one. Formal audits are intended to demonstrate compliance with detailed sets of specifications rather than general legal principals. Audits are designed to evaluate questions such as whether a given set of practices meets a given standard for data security, not whether those practices constitute compliance with a law. CPPA should always make final determinations regarding legal compliance.

III. What audit practices, methods, standards, and/or technical tools should CalPrivacy consider adopting as requirements for data broker audits?

CPPA should consider established privacy frameworks, such as the deletion guidelines from NIST or ISO.[2] These standards have long played a role in evaluating compliance with the technical requirements for other privacy laws,[3] setting useful precedents for covered entities to follow. This will help businesses leverage the best existing security practices while avoiding duplicative compliance requirements that undermine efficiency.

[2] *See, e.g.*, *Guidelines for Media Sanitization*, NIST SP 800-88 Rev. 2 (Sep. 2025), *available at* https://csrc.nist.gov/pubs/sp/800/88/r2/final; Information Security, Cybersecurity and Privacy Protection — Guidelines on Personally Identifiable Information Deletion, ISO/IEC 27555:2021(en), https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27555:ed-1:v1:en.

[3] *See, e.g.*, Federal Information Security Modernization Act (FISMA), 44 U.S.C. §§ 3541-51 *et seq*. (2014); *Managing Information as a Strategic Resource*, O.M.B. Circular No. A-130 (July 28, 2016).

IV. What audit requirements would allow CalPrivacy to determine if it should be requesting different identifiers from consumers to generate the highest number of matches between the DROP data and the data broker's data?

In determining whether to request additional data from consumers, CPPA should ensure that it does not undermine privacy for the users the same users the law is designed to protect. The law's deletion requirements already require generating additional data about consumers to document compliance with their requests. While CPPA may test other identifiers for increased accuracy, the agency should only consider those that will not reveal any more than a bare minimum of personal information.

V. When CalPrivacy requests an audit report, what other materials, at minimum, do you recommend be submitted to CalPrivacy at the same time?

As noted above, covered entities will process different types of data with different sensitivities, and should therefore be able to tailor their compliance measures accordingly. CPPA should therefore consider any evidence of compliance that a covered entity wishes to submit. Guidelines should be general rather than prescriptive, requesting evidence that covered entities'deletion practices are reasonable and appropriate to the type, amount, and sensitivity of the information they process. This approach aligns with most existing laws and gives businesses the needed flexibility to institute compliance procedures specific to their operations. Prescriptive requirements to institute specific compliance documentation processes, by contrast, risk becoming obsolete as technology evolves, imposing compliance burdens without enhancing user privacy.

In evaluating such evidence, CPPA should recognize that its role is distinct from that of the third-party auditor, even when it considers the same evidence as the auditor. Again, guidance should specify that the auditor's role is to make *technical* compliance determinations, while CPPA's role is to make *legal* determinations. The auditor should evaluate only well-defined, objective questions regarding whether practices meet a technical standard, but responsibility for determining compliance with the law should remain with CPPA.

VI. What else should CalPrivacy consider in developing data broker audit regulations?

Safe harbor provisions are important for fair and effective enforcement. Safe harbors (1) provide valuable predictability to both market actors and consumers, (2) enable speedier compliance, and (3) deter vexatious, meritless litigation if in fact parties other than the federal government are authorized to enforce the statute. When CPPA alleges noncompliance with one of the listed obligations, businesses should therefore be allowed to use compliance with an established data deletion framework like the above NIST and ISO standards as an affirmative defense against such allegations. In crafting such regulations, CPPA should engage with organizations that create best practices and frameworks for their members and stakeholders to follow, such as DTSP and NIST. Covered entities should also receive advance notice of complaints and have the opportunity to cure violations before enforcement actions are brought, both to minimize costly enforcement actions and focus agency resources on large-scale and repeat offenders.

Respectfully submitted,

Jesse Lieberfeld
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
jlieberfeld@ccianet.org

May 7, 2026

Catbagan, Christian@CPPA

From: Dan Rosler <dan@resolvecompliance.com>
Sent: Thursday, May 7, 2026 1:36 PM
To: Regulations@CPPA
Subject: Preliminary Comment – DROP Audits

Greetings,
As a former board member of the NAI (Network Advertising Initiative – the AdTech industry's self-regulatory association) I concur with the comprehensive comments they are submitting for your consideration regarding DROP audits and therefore will spare you from repeating the same points.

That said, I would like to emphasize specifically a few elements:

Question 3: What audit practices, methods, etc…
An audit methodology should include the key tenants of evidenced chain of custody and comprehensive populations. Chain of custody referring to proof that the data being used to support an aspect of the audit is actually coming from the primary system of record and reflects the actual data used in production environments. This prevents substitution of alternate data or processing records that might be used to hide non-compliances. A comprehensive population is a complete dataset covering all records during the in-scope audit period from which testing samples are to be drawn. Evidence of completeness ensures that the randomly-selected samples will not be restricted to a cherry-picked population that may obfuscate time periods or data sources that may produce an unfavorable audit finding. Ensuring auditors' methodologies include evidence of working from a complete and accurate dataset from which to draw test samples will increase audit consistency and reduce the risk of bad actors manipulating data used for audits.

Second, consider also a requirement that ALL of a data broker's databases be examined/assessed for storing personal data that could potentially be matched to the DROP records to ensure there aren't any systems/sources/fields not being included in the matching/deleting procedures even if the primary systems pass audit.

Question 4: Different identifiers…
As noted in the NAI comments, IP Addresses would be a very detrimental identifier for DROP purposes. In addition to the effects of say VPNs or server gateways, whether an IP Address is assigned to a household, a multi-family structure, or a commercial/institutional location, a single IP Address could be associated with dozens or literally thousands of devices owned by potentially thousands of natural persons at any given moment. And then that same IP Address could be reassigned to completely different locations and sets of devices on other days. Therefore, IP Addresses should not be included in the DROP dataset for matching purposes.

Question 5: Additional materials…

To increase organizational accountability, a standard audit report format should include basic information for the record about the subject company's organizational structure relevant to DROP compliance, and include the names/titles of those in the company who are responsible for DROP compliance, those providing operational support, and those participating in the audit process.

Question 6: Additional considerations…

CalPrivacy should structure the timing requirements for audits to prevent a significantly skewed pattern. If all of the currently registered data brokers will be looking to get their initial audits done in a relatively short timeframe in 2028, there may be a dearth of resources available (akin to the bottleneck of privacy lawyers' capacity that happened leading up to the first GDPR enforcement date). More so, even if the resource capacity bottleneck spreads first audits out throughout 2028, then the majority of data brokers will not need another audit for three years (2031). This means that the demand for new audits during the intervening three-year lull will be limited to only new data brokers. With that "lumpiness" it may be hard for audit providers to maintain organizational readiness and staffing during the "lean" years. Smoothing out the audit demand over the first several years will help to ensure the auditor community has both the capacity and a sustainable business model to support ongoing services.

Thank you for your consideration,
Dan Rosler

Dan@ResolveCompliance.com
(925) 425-8739

Catbagan, Christian@CPPA

From: Tony Ficarrotta <tony@networkadvertising.org>
Sent: Thursday, May 7, 2026 1:35 PM
To: Regulations@CPPA
Cc: Allen, Elizabeth@CPPA; Leigh Freund; David LeDuc; Megan Cox
Subject: Preliminary Comment – DROP Audits April 2026
Attachments: NAI Preliminary DROP Audit Comments 2026.05.07_Formatted.pdf

To the California Privacy Protection Agency,

The NAI is submitting comments in response to the Agency's Invitation for Preliminary Comments on Delete Request and Opt-out Platform (DROP) audits. Please see the attached pdf for our comments. If you have any questions or would like to discuss further, please do not hesitate to reach out.

Thank you,

-Tony Ficarrotta

--
Tony Ficarrotta
Vice President, General Counsel
The NAI
409 7th Street, NW, Suite 250, Washington, DC 20004
P: 719-210-4703 | tony@thenai.org

May 7, 2026

Submitted via electronic mail to: regulations@cppa.ca.gov

California Privacy Protection Agency

Attn: Legal Division — Regulations

400 R St., Suite 350, Sacramento, CA 95811

Re: Preliminary Comment — Delete Request and Opt-Out Platform Audits

To the California Privacy Protection Agency ("CalPrivacy"):

On behalf of the NAI (Network Advertising Initiative), thank you for the opportunity to submit comments in response to CalPrivacy's Invitation for Preliminary Comments on Delete Request and Opt-Out Platform ("DROP") Audits.[1] The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. Since 2000, the NAI has promoted the highest voluntary industry standards for its member companies, which range from small startups to some of the largest companies in digital advertising, and include ad exchanges, demand side platforms, supply side platforms, and other providers of advertising technology solutions.

SECTION 1: INTRODUCTION

The NAI has engaged substantively with the Delete Act and DROP framework since CalPrivacy first initiated rulemaking in 2024. We submitted preliminary comments on the DROP mechanism's design,[2] comments on the proposed data broker registration regulations,[3] responses on behalf of NAI members to CalPrivacy's DROP Questionnaire documenting the identifier matching challenges ad-tech data brokers face,[4] and comments on the proposed DROP

[1] Cal. Priv. Prot. Agency, Invitation for Preliminary Comments: Delete Request and Opt-Out Platform Audits (Apr. 7, 2026), https://cppa.ca.gov/regulations/pdf/drop_audits.pdf [*hereinafter* CalPrivacy Invitation for Preliminary Comments].
[2] Network Advertising Initiative, Preliminary Comments on Delete Act Rulemaking (June 25, 2024), https://thenai.org/wp-content/uploads/2024/06/NAI-Preliminary-Comments-SB362-Proposed-Rulemaking-June-25-2024-copy.pdf [*hereinafter* NAI June 2024 Delete Act Comments].
[3] Network Advertising Initiative, Comments on Proposed Data Broker Registration Regulations (Aug. 20, 2024), https://thenai.org/wp-content/uploads/2024/08/NAI-Delete-Act-NPRM-Comments-8.20.2024.docx.pdf.
[4] Network Advertising Initiative, Responses to CPPA DROP Questionnaire (Apr. 11, 2025) (submitted via email to databrokers@cppa.ca.gov).

regulations addressing matched-identifier definitions, account liability, list selection, fees, and status reporting.[5] We also submitted comments on CalPrivacy's cybersecurity audit rulemaking in 2023, recommending approaches to audit requirements including auditor selection flexibility, leveraging existing frameworks, and assessment confidentiality that are directly relevant here.[6] Most recently, our April 2026 comments on Reducing Friction and Opt-Out Preference Signals addressed the application of opt-out preference signals to pseudonymous data environments, an analysis we build on below.[7] And finally, the NAI participated in the informational session at CalPrivacy's April 30, 2026, board meeting to provide information about how the California data broker registry and DROP may interact with businesses that sell Californians' personal information to government actors.[8] The NAI has undertaken these extensive engagement efforts because NAI members – which include registered data brokers – are committed to furthering practical and administrable consumer privacy protections, which we believe the audit regulations CalPrivacy is currently considering are intended to support.

A key recurring theme in these comments is that NAI member companies primarily process pseudonymous identifiers (*e.g.*, device IDs, hashed tokens, cookie-based identifiers) rather than the direct consumer identifiers (*e.g.*, names, email addresses, phone numbers) that the DROP's deletion lists primarily support. The importance of that distinction is reflected in the DROP's early operational data: of the more than 242,000 deletion requests submitted by California consumers in the first eight weeks of operation, 94% included a phone number and 91% included an email address, while pseudonymous identifiers like mobile advertising IDs were included in only 10% of requests.[9] For some NAI members, the identifiers they process (*e.g.*, proprietary cookie IDs) are not apt for submission by consumers through the DROP at all, and as discussed in Section 5 below, California law contemplates application of opt-out preference signals to certain pseudonymous data environments that the DROP's centralized matching architecture is not designed to reach. Nevertheless, these companies are required to select at least one list from the DROP, retrieve it, and run the matching process every 45 days[10] even

[5] Network Advertising Initiative, Public Comment on Accessible Deletion Mechanism (June 10, 2025), https://thenai.org/wp-content/uploads/2025/06/NAI-Comments-Accessible-Deletion-Mechanism-NPRM-June-10-2025.pdf [*hereinafter* NAI June 2025 DROP Comments].
[6] Network Advertising Initiative, Comments on the CCPA's Preliminary Rulemaking on Cybersecurity, Risk Assessments and Automated Decisionmaking (Mar. 27, 2023), https://thenai.org/wp-content/uploads/2023/03/NAI-Comments-to-CPPA-re-Cybersecurity-Audits-Risk-Assessments-Automated-Decisionmaking.pdf [*hereinafter* NAI March 2023 Cybersecurity Audit Comments].
[7] Network Advertising Initiative, Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals, at 10–11 (Apr. 6, 2026), https://thenai.org/wp-content/uploads/2026/04/NAI-Preliminary-Comments-Reducing-Friction-Opt-Out-Preference-Signals-4.6.2026_layout-version-2.pdf [*hereinafter* NAI OOPS Comments].
[8] Cal. Priv. Prot. Agency, Background Materials for Joint Board Meeting (Apr. 30 – May 1, 2026), https://cppa.ca.gov/meetings/materials/20260430_0501_background_document.
[9] Remarks of Artem Andrusov, Chief of Information Technology, Cal. Priv. Prot. Agency, at Bd. Mtg., Agenda Item 4 (DROP Update), at 40:01 (Feb. 27, 2026), https://www.youtube.com/watch?v=E4CMYnfI1uA&t=2401s (reporting that, of more than 242,000 deletion requests submitted to the DROP in the first eight weeks of operation, 99% included a ZIP code, 94% included a phone number, 91% included an email address, 24% included a vehicle identification number, 10% included a mobile advertising identifier, and 3% included a connected television identifier).
[10] Cal. Code Regs. tit. 11, § 7612(a) (requiring data brokers to access the DROP and download selected consumer deletion lists "at least once every 45 calendar days").

though some will find zero matches as a structural feature of their data environments. This is not a shortcoming of the DROP or of these companies' compliance efforts, but instead reflects a structural feature of how pseudonymous ad-tech data environments work — and it has practical consequences for every aspect of audit design ranging from what documentation brokers can produce, to what matching outcomes auditors should expect, to how compliance should be evaluated through audits.

The Delete Act requires every registered data broker to undergo an audit by an independent third party every three years, beginning January 1, 2028.[11] Consistent with that requirement, however, CalPrivacy has broad discretionary authority under the Delete Act to shape the audit framework through regulations.[12] This includes defining audit scope and depth, establishing methodology and sampling standards, specifying what records and documentation brokers must maintain, setting auditor qualifications and independence criteria, and structuring reporting requirements. These are consequential design choices. How CalPrivacy defines auditor qualifications will determine who is eligible to conduct these audits, including whether professionals with existing relationships to the regulated entity, such as designated privacy officers or outside counsel, can serve in the auditor role, and what independence standards apply. How CalPrivacy calibrates audit scope will determine whether a broker processing only pseudonymous identifiers with zero matches faces the same audit as a large consumer data aggregator processing thousands of matched deletion requests per cycle. And how CalPrivacy structures documentation and reporting will shape both the cost of compliance and the usefulness of audit findings.

Against that backdrop, the NAI urges CalPrivacy to design audit regulations around a central principle: audits should evaluate whether each broker has implemented reliable deletion processing for its actual data environment, with audit depth and documentation scaled to that environment. Our comments below apply that principle to the six questions CalPrivacy set forth in its invitation for comment, with additional first-cycle implementation considerations in a final section:

1. **Auditor qualifications and independence** — a common baseline of professional competence and independence, with technical expertise and audit scope scaled to the broker's data environment.
2. **Records and documentation** — documentation requirements calibrated to broker data architectures, resolution of the suppression-list-versus-deletion tension, and a limited-scope independent audit pathway for zero-match brokers.
3. **Audit practices, methods, standards, and tools** — a component-based, evidence-driven audit model grounded in established methodology and calibrated to the DROP's scope, without a separate AI audit overlay.

[11] Cal. Civ. Code § 1798.99.86(e)(1). The CCPA's cybersecurity audit regulations, by contrast, permit internal auditors meeting specified independence conditions and phase implementation by revenue. *See* Cal. Code Regs. tit. 11, §§ 7122(a)(2)–(3); 7121(a)(1)–(3). The Delete Act does not expressly include either accommodation.
[12] Cal. Civ. Code § 1798.99.87(a).

4. **Identifier matching and audit requirements** — what audit data can tell CalPrivacy about identifier coverage, how pseudonymous data environments are already served by opt-out preference signals, and why IP addresses are a poor candidate for identifier expansion.
5. **Materials accompanying audit reports** — a targeted reporting framework paralleling CalPrivacy's cybersecurity audit model, with presumed confidential treatment for audit materials documenting internal compliance processes.
6. **Additional considerations** — a first audit period beginning no earlier than six months after final regulations issue, phased first-cycle completion across 2028 and 2029, and coordination with the cybersecurity audit program.

SECTION 2: AUDITOR QUALIFICATIONS AND INDEPENDENCE

CalPrivacy asks: What credentials, certifications, or independence requirements should third-party auditors possess to ensure they are qualified and sufficiently independent?

A. Auditor Qualifications: A Baseline All Auditors Meet, with Technical Expertise Scaled to the Audit

To support reliable findings that are readily comparable between registered data brokers, every auditor qualified to conduct audits should be required to meet a common baseline of independence and professional competence. However, given the range of different types of registered brokers and the types of data they process, auditors should also bring technical expertise proportional to what they will examine for a given broker. CalPrivacy should structure auditor qualifications around these two layers: a baseline applicable to every DROP audit, and scalable technical expertise calibrated to the complexity of the broker's data environment and the audit components being evaluated.

Existing professional standards for auditors point to what the baseline should look like, including in existing CCPA regulations. CalPrivacy's cybersecurity audit regulations require a qualified, objective, independent professional using procedures and standards accepted in the auditing profession, referencing standards from established bodies (AICPA, PCAOB, ISACA, ISO) without prescribing specific certifications.[13] The same flexible model should be adopted for DROP audits. The ad-tech industry has adopted rigorous third-party auditing under analogous frameworks: MRC accreditation audits, for example, are conducted by independent CPAs with information-systems-audit credentialing, providing one concrete benchmark for what a qualified auditor looks like in practice.[14]

[13] Cal. Code Regs. tit. 11, § 7122(a) (setting forth standards accepted in professional auditing and requiring the auditor to "have knowledge of cybersecurity and how to audit a business's cybersecurity program").
[14] MRC (Media Rating Council) accreditation relies on annual external audits by specialized independent CPA auditors with domain expertise in media and advertising measurement. *See* Media Rating Council, Audit and Accreditation Process, https://mediaratingcouncil.org/about-mrc/audit-and-accreditation-process (last visited Apr. 28, 2026). Where TAG (Trustworthy Accountability Group) certification is obtained through independent validation, TAG guidelines contemplate use of an auditing company with a specialty in digital media audits. *See* Trustworthy Accountability Grp., TAG Certified Against Fraud Guidelines v10.1, § 2.4 (July 2025),

The technical expertise the audit requires will vary with the broker's data environment. A broker that processes direct consumer identifiers, matches thousands of deletion requests per cycle, and maintains suppression lists across multiple downstream partners presents audit subject matter that calls for deep technical and data-processing expertise. A broker whose data architecture cannot be matched against the cleartext identifiers in any available deletion list[15] presents a fundamentally different audit, one that is primarily a process verification exercise. Auditor qualifications should scale accordingly. A common baseline ensures comparability across DROP audits, while scalable expertise helps ensure that the right auditor is conducting the right engagement.

B. Audit Scope Should Be Tailored to the Broker's Data Environment

Audit scope and depth should be calibrated to the broker's data environment and processing activities, not applied uniformly across brokers with very different operations. CalPrivacy's cybersecurity audit regulations already adopt this approach: they require assessment of a program appropriate to the business's size, complexity, and the nature and scope of its processing activities,[16] and require assessment of listed components that the auditor deems applicable to the business's information system.[17] CalPrivacy should adopt a version of this combined approach for DROP audits.

The compliance elements in the DROP regulations (standardization, hashing, matching, deletion, downstream direction, suppression, and exceptions)[18] will not all apply to every broker in the same way. As noted above, a broker whose cookie-based identifiers are proprietary and ephemeral, and do not overlap with the identifier types on any available deletion list, has a markedly different set of audit considerations compared to brokers processing a variety of direct identifiers such as name, phone number, and email address. Both types of brokers are subject to the audit requirement, but professional auditors should have discretion to scope the subject matter of those audits in a way that reflects the operations and complexity each presents. We address scoping factors and audit methodology in detail in our response to CalPrivacy's question on audit practices, methods, and standards below.

C. Existing Framework Recognition

Audit regulations should recognize and leverage findings from established compliance frameworks where those frameworks already evaluate controls relevant to DROP compliance. NAI members in some cases already undergo structured third-party audits under frameworks such as SOC 2 Type II, NIST Cybersecurity Framework 2.0, and ISO 27001/27701.[19] Some also

---

https://www.tagtoday.net/hubfs/CAF/TAG%20CAF%20Guidelines%20Final.pdf. These credentialing standards demonstrate that the ad-tech industry has established benchmarks for qualified auditors that CalPrivacy could reference.

[15] Cal. Code Regs. tit. 11, § 7610(a)(3) requires every broker to select at least one consumer deletion list, and to select all lists containing consumer identifiers that match personal information in the broker's records, subject to a duplicative-list exception.

[16] *Id.* § 7123(b)(1).

[17] *Id.* § 7123(b)(2).

[18] *Id.* § 7613.

[19] *See* Nat'l Inst. of Standards & Tech., The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (Feb. 26, 2024), https://doi.org/10.6028/NIST.CSWP.29; AICPA, SOC 2® — SOC for Service

undergo ad-tech-specific audits such as MRC accreditation or TAG certification, as discussed above.

The cybersecurity audit regulations permit businesses to utilize audits, assessments, or evaluations prepared for another purpose, provided they meet all applicable requirements on their own or through supplementation.[20] The NAI recommended this approach in its March 2023 cybersecurity audit comments.[21] CalPrivacy should continue advancing this concept for DROP audits, but rather than leaving it to individual brokers and auditors to determine whether an existing audit satisfies DROP requirements, CalPrivacy has an opportunity to proactively identify which elements of established frameworks address DROP compliance obligations and deem them equivalent where applicable. This result would create efficiencies for brokers already conducting relevant audits without wasteful duplication of efforts.

For example, where "processing integrity" is included within the scope of a SOC 2 Type II examination, the criteria assess controls relevant to complete, accurate, and authorized system processing.[22] To the extent a SOC 2 report specifically tests controls over matching, processing, and output procedures relevant to integration with the DROP, those findings could inform the DROP audit rather than requiring the auditor to duplicate the evaluation. Similarly, ISO/IEC 27701 includes privacy-management controls and guidance addressing deletion, retention, disposal, and backup or archived environments where applicable.[23] Those controls may inform evaluation of deletion completeness under the DROP regulations, but should be mapped carefully against the regulation's specific requirements.

CalPrivacy should use the audit regulations to permit auditors to rely on findings from prior recognized assessments to the extent they address the DROP regulations' deletion processing requirements. This would reduce duplicative evaluation while preserving the independent review the statute requires.

Organizations: Trust Services Criteria, https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2 ; ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, https://www.iso.org/standard/27001; ISO/IEC 27701:2025, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, https://www.iso.org/standard/27701.

[20] Cal. Code Regs. tit. 11, § 7123(f) (permitting use of "a cybersecurity audit, assessment, or evaluation that [the business] has prepared for another purpose, provided that it meets all of the requirements of this Article, either on its own or through supplementation").

[21] *See* NAI March 2023 Cybersecurity Audit Comments, *supra* note 6.

[22] *See* AICPA, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP Section 100), https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022. The Processing Integrity category evaluates controls relevant to complete, valid, accurate, timely, and authorized system processing. Processing Integrity is an optional Trust Services Category; not every SOC 2 examination includes it.

[23] *See* ISO/IEC 27701:2025, *supra* note 19, Annex A (controller controls) and Annex B (processor controls) (addressing PII retention, de-identification, deletion, and disposal obligations, including guidance on assurance concerning disposal from backup or archived environments).

D. Independence

Independence standards for DROP auditors should be informed by the standards applied under established audit frameworks rather than constructed from scratch. The Delete Act requires audits to be conducted by an "independent third party."[24] The statute does not define what independence requires beyond that phrase, but the "third party" language appears to contemplate an auditor external to the broker — unlike CalPrivacy's cybersecurity audit regulations, which explicitly permit internal auditors meeting specified independence conditions.[25] Regulations should clarify how the Delete Act's "independent third party" requirement applies in practice.

The independence standard for DROP auditors will shape how the audit market develops, and regulations should promote flexibility while drawing on experience from existing frameworks. For example, SOC 2 audits require the auditor to be independent of the entity under examination, applying AICPA independence requirements that include the Independence Rule and related interpretations addressing financial interests, employment or association with attest clients, and nonattest services.[26] MRC accreditation audits require independence from the entity being accredited.[27] And CalPrivacy's own cybersecurity audit regulations reference "objectivity and independence" as auditor requirements.[28]

However, several open questions remain about how independence requirements apply in practice, and CalPrivacy should address them directly in regulations. As a baseline principle, a professional who designed, operated, or remediated the specific DROP controls under audit should not be eligible to audit those same controls. Beyond that core principle, regulations should clarify how independence applies to advisory relationships of different kinds: whether prior unrelated advisory work creates a disqualifying conflict, what safeguards and disclosure obligations should apply where prior engagements have occurred, and what cooling-off period (if any) should apply before an advisor can transition to an auditor role for the same broker. Clear regulatory guidance on these points will help both brokers and potential auditors understand the boundaries before the audit market takes shape.

---

[24] Cal. Civ. Code § 1798.99.86(e)(1). Presumably, an auditor does not have to be a "third party" as defined under CCPA. *See id*. § 1798.140(ai).
[25] Cal. Code Regs. tit. 11, § 7122(a)(2)–(3) (permitting internal auditors subject to independence conditions, including that the highest-ranking auditor report to executive management without direct cybersecurity responsibility).
[26] *See* AICPA, Code of Professional Conduct, ET § 1.200.001, 1.240, 1.275, 1.277, 1.279, 1.295, https://pub.aicpa.org/codeofconduct/ethicsresources/et-cod.pdf.
[27] *See* Media Rating Council, Minimum Standards for Media Rating Research § B.14 (Dec. 2011), https://mediaratingcouncil.org/sites/default/files/Standards/MRC%20Minimum%20Standards%20-%20December%202011.pdf (requiring the rating service to permit "such CPA firm(s) designated by the MRC for the purpose of auditing" to review or audit any procedures or operations bearing on accredited measurement); *see also* Media Rating Council, Audit and Accreditation Process, *supra* note 14 (describing audits conducted by a "specialized team of independent CPA auditors").
[28] Cal. Code Regs. tit. 11, § 7122(a).

E. Auditor Selection

Brokers should retain the ability to select their own independent third-party auditors, subject to qualifications and independence criteria established by CalPrivacy. This is consistent with CalPrivacy's existing cybersecurity audit framework, which establishes auditor qualifications without prescribing a designated-auditor mechanism or a pre-approved list.[29] CalPrivacy should not designate specific audit firms or create a pre-approved auditor list, which would risk creating bottlenecks and concentrating market power. This is particularly important given the limited pool of auditors with ad-tech data environment expertise.

SECTION 3: RECORDS AND DOCUMENTATION

CalPrivacy asks: What records, documentation, or other evidence would demonstrate in an audit whether a data broker has properly processed consumer deletion requests?

A. Documentation Requirements Must Account for the Diversity of Data Broker Architectures

A documentation standard designed for one type of data environment will not produce useful compliance evidence when applied to a different one. The DROP regulations impose a single set of processing steps on every data broker: standardize, hash, match, delete, suppress, direct downstream partners.[30] But the data environments those steps apply to are significantly different. A broker that processes consumer names and phone numbers can follow each step as written. A broker whose entire data inventory consists of proprietary cookie IDs or pre-hashed tokens cannot, because the chain is broken at the matching phase. If CalPrivacy sets documentation requirements that assume every broker holds cleartext personal information and matches it through the standard pipeline, brokers with different architectures will have no way to document compliance, not because they failed to comply, but because the documentation template does not describe what they actually do.

CalPrivacy should define documentation categories that track the required processing steps, while explicitly recognizing that not every step applies to every broker in the same way. The categories should include: how the broker standardizes personal information from its records (or why standardization is minimal or inapplicable); what hashing algorithm the broker uses (or why CalPrivacy's standard hash cannot be applied to the broker's data); access logs showing the broker retrieved deletion lists on the required schedule; match results, including zero-match outcomes with an explanation; the status reports the broker submitted back to CalPrivacy for each deletion request (record deleted, opted out of sale, exempted, or not found); evidence of deletion for each match; documentation of any delayed deletion in archived or backup systems; evidence of downstream direction to service providers and contractors; evidence of ongoing suppression list maintenance; and the basis for any exceptions invoked.[31]

---

[29] *See id.* § 7122(a) (qualifying auditors through criteria rather than agency designation).
[30] *Id.* § 7613(a)–(d).
[31] The specific regulatory provisions governing each step are found in Cal. Code Regs., tit. 11 as follows: standardization (§ 7613(a)(1)(A)(i)–(vi)); hashing (§ 7613(a)(1)(B)); matching (§ 7613(a)(1)–(2)); deletion (§ 7613(b)(1), (b)(1)(B)); archived/backup systems (§ 7613(b)(1)(C)(i)); downstream direction (§ 7613(d));

Further, three specific data architecture scenarios warrant explicit guidance in the regulations:

Zero-match scenarios. As discussed above, some ad-tech brokers process only identifier types not represented on any available deletion list, but the regulations still require them to select a list, retrieve it, and run the matching process.[32] As expected, these brokers will perform every required step and find zero matches. Without clear guidance that a documented zero-match outcome is a compliant result, these brokers face the risk of adverse audit findings for an outcome they could not have avoided. CalPrivacy should confirm that zero-match documentation satisfying each processing step constitutes compliance.

Proprietary hash scenarios. The regulations contemplate a workflow where the broker standardizes cleartext personal information and then hashes it using standard algorithms defined by regulation before comparing to the deletion list.[33] However, some ad-tech companies never possess cleartext. They receive data already hashed with proprietary salts designed to prevent re-identification. This scenario will not produce a match to cleartext if the hashes defined by regulation are applied to their data. If the audit regulations do not address this scenario, these brokers, which may be among the most privacy-protective in their data handling, have no way to know what documentation will satisfy the audit requirement.

Pass-through scenarios. The regulations require brokers to compare deletion list identifiers against personal information "maintained in the data broker's own records."[34] Some ad-tech companies collect and transmit identifiers between partners in real time without retaining them in persistent records. For these companies, there may be no stored record to compare against at the time the comparison would occur. CalPrivacy should address what documentation these brokers must maintain to demonstrate compliance when the data the audit would evaluate is no longer held.

B. The Suppression List Creates a Regulatory Tension That Auditors Need Guidance to Navigate

Brokers that comply with the Delete Act's suppression list requirement will have consumer identifiers on file after processing a deletion request.[35] An auditor without clear guidance may treat this as evidence of incomplete deletion. This is a predictable source of false noncompliance findings for ad-tech data brokers, and CalPrivacy should address it directly.

The tension arises from three provisions in the Delete Act's implementing regulations that pull in different directions. One requires brokers to save and maintain consumer deletion lists and compare newly collected records against them before sale or sharing, even for requests that did not produce a match.[36] A second defines "delete" as permanently and completely erasing

---

ongoing suppression (§ 7613(c)); status reporting (§ 7614); and exceptions (Cal. Civ. Code §§ 1798.105(d), 1798.145, 1798.146; §§ 1798.99.86(c)(2)(A)–(B)).

[32] Cal. Code Regs. tit. 11, § 7610(a)(3).

[33] *Id.* § 7613(a)(1)(A)–(B).

[34] *Id.* § 7613(a)(1).

[35] *See* Cal. Code Regs. tit. 11, § 7613(c) (requiring data brokers to save and maintain consumer deletion lists and compare newly-collected records against them).

[36] *Id.*

personal information from all systems, including archived and backup systems.[37] And a third permits retaining the minimum personal information necessary to facilitate compliance.[38]

Read together, these provisions require brokers to retain certain consumer identifiers for ongoing suppression while simultaneously requiring them to delete all personal information. The reconciliation is the "minimum necessary" exception, but that exception is undefined. NAI members maintaining suppression lists need to know whether they should retain only the hashed identifier sufficient for comparison, or whether associated metadata (such as the date of the request or the list from which the identifier originated) is permitted or required. The answer affects system design and audit outcomes: a broker that retains too little cannot effectively suppress, and a broker that retains too much risks an auditor finding it kept more than the minimum necessary.

CalPrivacy should do two things to address this tension. First, confirm that suppression list retention is not a deletion failure. These provisions must be read together, and audit standards should reflect that. Second, clarify that suppression-list retention reasonably calibrated to effectuate ongoing compliance (for example, retention of the hashed identifier, request date, source list, and comparison logs) falls within the "minimum necessary" standard under § 7613(b)(1)(B). A presumption of compliance for those data points preserves the operational flexibility that varied data architectures require while providing auditors a workable evaluation baseline.

The NAI noted aspects of this tension in its June 2025 comments on the proposed DROP regulations.[39] It now requires resolution before auditors begin evaluating broker compliance.

C. Audit Findings Should Distinguish Systemic Failures from Isolated, Remediated Exceptions

Audit findings provide the most useful compliance information when they distinguish systemic process failures from isolated, documented, and remediated exceptions. The DROP is designed to operate continuously: brokers retrieve deletion lists every 45 days, run matches, process deletions, update suppression lists, and direct service providers, then repeat the cycle.[40] A well-designed process that runs on this cycle will encounter occasional exceptions (a record that did not match on a given pass because of a transient data quality issue, a downstream partner that took an extra cycle to confirm deletion) and will identify and resolve them on subsequent passes.

Auditors should evaluate exceptions in context: whether the broker's process detected the exception, whether the exception was remediated, and whether the broker's documentation explains both. A systemic process failure is qualitatively different. A broker that never accessed the DROP, never ran matches, has no documentation of its procedures, or repeatedly fails to deliver matched records to suppression lists has not implemented the regulatory framework. Audit findings should reflect that distinction.

Regulations should facilitate auditors' evaluation of the broker's deletion processing system as a whole: whether the process is documented, whether it is followed consistently, whether it

[37] *Id.* § 7613(b)(1)(C).
[38] *Id.* § 7613(b)(1)(B).
[39] NAI June 2025 DROP Comments, *supra* note 5, at 7–8.
[40] *See* Cal. Code Regs. tit. 11, §§ 7612(a) (45-day retrieval cycle), 7613(c) (ongoing suppression obligation).

operates on the required schedule, and whether the broker detects, documents, and remediates exceptions on subsequent cycles. These questions produce findings that tell CalPrivacy what it needs to know about each broker's compliance posture, while ensuring that occasional exceptions in otherwise sound processes do not generate the same response as systemic failures.

D. A Limited-Scope Independent Audit Pathway for Zero-Match Brokers

For brokers whose data environment consistently produces zero matches, the audit's subject matter is different from a high-volume matching audit, but the audit itself remains an independent examination of evidence the data environment actually produces. The substantive audit questions reduce to five documentable elements that are testable regardless of match volume: Did the broker select the consumer deletion lists containing identifier types relevant to its records? Did it access the DROP on schedule? Did it retrieve the selected lists? Did it run its matching process consistently across cycles? And did it maintain suppression lists where required? Each element should be independently testable, for example, through list-selection records, access logs, retrieval logs, match-run output across multiple cycles, and suppression-list documentation. Where appropriate, the auditor's testing may include validating the broker's matching pipeline through test fixtures or sample inputs to confirm that a match would be detected if one existed — testing that demonstrates pipeline integrity even where the broker's data environment does not produce live matches.

The statute requires an independent third-party audit.[41] But CalPrivacy has discretion over the scope and depth of what the auditor evaluates. For brokers that can demonstrate documented zero-match outcomes over multiple cycles, CalPrivacy should establish a limited-scope independent audit pathway. The auditor still independently tests evidence (access logs, list selections, match-run records, and suppression-list maintenance), but is not required to conduct full-scope procedures designed to evaluate deletion processing that did not occur because no matches existed.

This is not self-certification. The auditor remains independent, the evidence remains independently testable, and the audit produces verifiable findings. What differs is scope. The audit examines the evidence that exists in a zero-match data environment, rather than full-scope procedures aimed at deletion outcomes the broker's data architecture did not produce. This calibrates audit depth to what the data environment warrants, complements the proportionality framework above, and serves CalPrivacy's interest in audit findings that reflect actual compliance posture rather than the absence of subject matter to evaluate.

SECTION 4: AUDIT PRACTICES, METHODS, STANDARDS, AND TOOLS

CalPrivacy asks: What audit practices, methods, standards, and/or technical tools should CalPrivacy consider adopting as requirements for data broker audits? Are there additional or different audit requirements you recommend when a data broker uses artificial intelligence (AI) or agentic AI systems?

[41] Cal. Civ. Code § 1798.99.86(e)(1).

A. Audit Methods Should Evaluate Specific Compliance Components Against Documented Evidence

An audit framework that defines what to evaluate and lets the auditor determine how deeply to evaluate it will produce more consistent and useful results than one that prescribes a single methodology for all brokers. CalPrivacy's cybersecurity audit regulations already take this approach, defining components the auditor assesses based on the business's size, complexity, and processing activities, with findings grounded in specific evidence rather than management assertions.[42]

CalPrivacy should adopt the same structure for DROP audits. The compliance components are already defined by the deletion processing requirements: standardization and hashing, matching, deletion, downstream direction, ongoing suppression, and exceptions.[43] For each component, the auditor would evaluate documented evidence (policies, procedures, access logs, match results, deletion records) and determine whether the broker's process meets the requirements. The auditor would scope which components apply based on the broker's data environment, consistent with the proportionality framework described above.

This gives auditors a clear evaluation structure while preserving flexibility. It gives brokers predictability about what the audit will examine, so they can build documentation systems in advance. And it avoids the alternative: a rigid, uniform methodology that either over-audits brokers with simple data environments or under-audits complex ones.

B. Established Audit Frameworks Offer Useful Methods, but the Scope Must Match the Task

CalPrivacy should draw on proven audit methodology rather than building procedures from scratch. SOC 2 Type II evaluates controls over a sustained period rather than at a single point in time. Banking examinations use transaction sampling and exception testing.[44] CalPrivacy's own cybersecurity audit program defines a systematic component-based approach with well over a dozen enumerated components.[45] Each offers procedural tools that could inform how DROP auditors conduct their work.

The important distinction is that these frameworks evaluate broad organizational compliance across many domains. A DROP audit evaluates a single set of deletion processing requirements.

---

[42] Cal. Code Regs. tit. 11, §§ 7123(b)(1)–(2), 7122(d) (requiring findings to rely on specific evidence including documents, sampling, testing, and interviews rather than management assertions).
[43] *See id.* § 7613.
[44] *See generally* Off. of the Comptroller of the Currency, Comptroller's Handbook: Sampling Methodologies, at 1, 5–7, 19–20 (May 2020), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/sampling-methodologies/pub-ch-sampling-methodologies.pdf (explaining that bank examiners may use sampling to analyze populations of "accounts, transactions or loans" and to identify exceptions, and describing evaluation of exceptions identified in judgmental and statistical samples); Fed. Fin. Insts. Examination Council, HMDA Examiner Transaction Testing Guidelines, Testing Procedures ¶¶ 1–7, https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/ffiec-hmda-examiner-transaction-testing-guidelines (describing examiner transaction testing through random samples, review against corresponding loan files, identification of unexplained differences as errors, staged review based on error thresholds, and corrective action or resubmission where error thresholds are met).
[45] *See* Cal. Code Regs. tit. 11, § 7123(b)–(c).

Importing applicable aspects of the methodology is valuable, but importing the scope would be excessive. Brokers should not face audit procedures designed for enterprise-wide compliance programs when the statutory task is verifying that deletion requests were processed correctly. A component-based approach with evidence testing, applied to the specific deletion processing requirements, captures the rigor of established frameworks without subjecting brokers to evaluation criteria beyond what the statute contemplates.

Ad-tech-specific frameworks may also be relevant. MRC accreditation audits, for instance, evaluate whether a measurement provider's data collection, processing, and reporting controls produce accurate outputs from verified inputs, a methodology that translates naturally to verifying whether deletion request inputs are correctly matched and processed.[46] Across these frameworks, established audit methodology already addresses foundational integrity questions such as chain of custody for audited data and completeness of the audit population, allowing auditors to verify that the data evaluated reflects the broker's production environment without selective omission. CalPrivacy need not adopt any single framework, but the procedural questions this rulemaking raises are not novel. Established methodologies already address most of them.

C. AI and Agentic Systems Do Not Change What Compliance Means

Audits should evaluate whether a broker accessed the DROP, ran its matching process, and deleted matched records. Whether the broker performed those steps through manual processes, conventional automation, or AI-powered systems should not change the outcome the auditor is evaluating. As such, CalPrivacy should not create AI-specific audit requirements within the DROP framework.

CalPrivacy has already addressed broader AI-related risks (such as bias, transparency, consumer rights) through the CCPA's automated decisionmaking technology regulations.[47] Layering additional AI requirements into the DROP audit would risk inconsistency with that framework and impose duplicative obligations.

If CalPrivacy concludes that some acknowledgment of AI use by a broker related to DROP compliance is warranted, it should be limited to disclosure: for example, requesting the broker to describe how automated systems are used in its deletion processing workflow so the auditor can evaluate whether those systems produce compliant outcomes. This fits within the evidence-based approach without requiring the auditor to evaluate the AI system itself.

Where automated systems are used in deletion processing, including AI-powered and agentic systems, the auditor's evaluation should rely on the same control evidence that applies to any high-volume automated processing pipeline: documentation of the system's role in the deletion workflow, evidence of human oversight at decision points appropriate to the system's function, reproducibility of system outputs, change management records, access controls, exception handling procedures, and audit logs. These are conventional audit subjects, and they are sufficient to evaluate whether automated deletion processing produces compliant outcomes.

---

[46] *See generally* Media Rating Council, Minimum Standards for Media Rating Research, *supra* note 27 (audit methodology for evaluating data collection, processing, and reporting controls).
[47] *See* Cal. Code Regs. tit. 11, §§ 7200, 7220–7222.

CalPrivacy does not need to define a separate AI audit regime within the DROP framework to ensure that automated systems are subject to meaningful audit scrutiny.

D. Auditors Should Choose Their Own Tools

Prescribing specific technical tools would constrain auditors without improving compliance outcomes. CalPrivacy's cybersecurity audit regulations take this approach, defining what the auditor must evaluate without specifying the software or instruments the auditor must use to do so.[48] The same principle should apply here. The audit should be judged on whether the auditor reached well-supported conclusions, not on which software produced them.

CalPrivacy could usefully identify categories of tools that may be relevant (hash verification, log analysis, database sampling) without mandating specific products. This preserves flexibility, avoids tying the audit process to technology that may become outdated, and prevents unnecessary procurement costs for brokers whose data environments do not require particular tools.

SECTION 5: IDENTIFIER MATCHING AND AUDIT REQUIREMENTS

CalPrivacy asks: What audit requirements would allow CalPrivacy to determine if it should be requesting different identifiers from consumers to generate the highest number of matches between the DROP data and the data broker's data? For example, CalPrivacy collects only zip codes from consumers, but if a full address would generate more matches — or another identifier altogether (e.g. IP address, etc.) — what evidence would demonstrate that?

A. Audit Data Can Show Where Match Rates Are Low, but CalPrivacy Should Not Infer That Different Identifiers Would Fix the Problem

Low or zero match rates do not, by themselves, indicate that consumers would benefit from CalPrivacy collecting different identifiers because in many ad-tech data environments a zero-match result would reflect effective pseudonymization that *by design* cannot be easily bridged to a consumer-provided identifier. Audit findings should help CalPrivacy distinguish that condition from cases where different consumer-provided identifiers actually would help. Audits can confirm where low or zero match rates exist, which is useful information for identifier coverage analysis. But low match rates alone do not tell CalPrivacy whether collecting different identifiers would produce better results.

The DROP compares cleartext-derived consumer-provided identifiers (names, email addresses, phone numbers) and standardized consumer-accessible identifiers (such as MAID) against a broker's records after standardization and hashing.[49] That process works well for brokers that maintain identified consumer records. It does not work for brokers whose data has been transformed through proprietary hashing, salting, encryption, or tokenization, because such data is *designed* to not be linkable to the cleartext identifiers the DROP collects. The CCPA already

[48] *See id.* § 7123(b)–(c) (defining audit components and assessment criteria without prescribing specific tools or software).
[49] *See* Cal. Code Regs. tit. 11, § 7613(a)(1)(A)–(B) (requiring data brokers to standardize personal information and apply CalPrivacy's hashing algorithm before comparing against consumer deletion lists).

contemplates this: it provides that the law shall not be construed to require a business to re-identify or link information that it does not maintain as personal information in the ordinary course of business.[50]

This means low match rates for these brokers are likely to persist regardless of which cleartext identifiers CalPrivacy adds. Adding full mailing addresses would not help a broker that processes only hashed device tokens. Adding IP addresses would not help a broker that processes only proprietary cookie identifiers. The mismatch is between the mechanism (centralized cleartext matching) and the data environment (pseudonymized, session-based, or hashed), not between one cleartext identifier and another.

Four categories of identifiers common in ad tech illustrate this. Cookies are domain-scoped and server-set under the HTTP cookie mechanism, and in programmatic advertising each platform's cookie-sync identifiers are partner-specific IDs mapped between exchanges and buyers, rather than a universal cross-company format.[51] Device-level advertising identifiers (such as Apple's IDFA and Google's Android Advertising ID) are more standardized but platform-specific, and early DROP operational data confirms that consumers include them in only 10% of deletion requests, compared with over 90% for email addresses and phone numbers.[52] Some companies receive email-derived data that has already been hashed with proprietary salts, meaning those companies cannot reverse the proprietary process to apply the standardization and hashing contemplated by the existing regulations.[53] And probabilistic identifiers based on network or device characteristics are neither consumer-accessible nor standardized.

To get useful evidence from audits about identifier coverage, CalPrivacy should try to understand three things about each broker's data environment: what identifier types the broker maintains, which of those types overlap with identifiers the DROP currently supports, and match

[50] Cal. Civ. Code § 1798.145(j)(1).
[51] *See* IETF, RFC 6265, HTTP State Management Mechanism § 4.1.2.3 (Apr. 2011), https://www.rfc-editor.org/rfc/rfc6265 (defining the Domain attribute that scopes cookies to the server that set them). Because each company's cookies use company-specific identifiers, there is no cross-company cookie format that the DROP could standardize against.
[52] *See supra* note *9*. CalPrivacy's Chief of Information Technology characterized this distribution as expected, observing that "the . . . easier an identifier to find, the more likely consumers include" it, and identifying improvements to consumer messaging on locating VINs, MAIDs, and CTV IDs as an Agency-recognized opportunity. *Id.* CalPrivacy has itself relied on NAI resources for guidance on resetting MAIDs on connected television devices. *See* Tom Kemp, Cal. Priv. Prot. Agency, *Understanding Mobile Advertising IDs and DROP* (Dec. 2, 2025), https://privacy.ca.gov/2025/12/understanding-mobile-advertising-ids-and-drop/. The NAI has separately recommended, in connection with the iOS environment where Apple does not expose the IDFA in user-facing settings, that the Agency develop a mobile application in connection with the DROP to enable consumers to surface and submit their MAID. *See* NAI June 2024 Delete Act Comments, *supra* note 2, at 11. In tandem, the NAI is currently developing a mobile application of this kind to assist consumers in identifying and submitting their MAIDs through the DROP.
[53] In April 2025, CalPrivacy's Data Broker Unit distributed a questionnaire to registered data brokers seeking information about identifier types, matching capabilities, and deletion processing practices. The questionnaire was directed to individual brokers, however, the NAI submitted a consolidated response on behalf of members addressing common technical characteristics across member data environments without disclosing any individual broker's proprietary data architecture. Letter from Tony Ficarrotta, NAI, to Cal. Priv. Prot. Agency Data Broker Unit (Apr. 11, 2025) (submitted via email to databrokers@cppa.ca.gov) [*hereinafter* NAI Questionnaire Response].

rates for the compatible subset specifically. This would allow CalPrivacy to distinguish between three different causes of low match rates: deficient processing (the broker failed to run the matching pipeline correctly), limited consumer submission (the DROP supports the identifier type but consumers rarely submit it), and non-overlap (the broker's identifiers cannot be matched against any cleartext list regardless of what CalPrivacy collects). The first warrants enforcement attention. The second may inform CalPrivacy's consumer outreach. The third tells CalPrivacy that centralized cleartext matching is not the right mechanism for that data environment, and adding more cleartext identifiers will not change the result.

B. For Data Environments the DROP Does Not Effectively Reach, Opt-Out Preference Signals Already Facilitate Consumer Choice at Scale

Opt-out preference signals (OOPS) are the mechanism designed for the pseudonymous data environments the DROP cannot effectively reach, and California law already requires those signals to extend to pseudonymous profiles. This reflects a basic difference between DROP and OOPS.

The DROP effectuates the right to deletion by matching static identifiers against stored records. That model depends on the consumer and the broker sharing a common identifier that can be compared after standardization. For pseudonymized data, no such shared identifier exists. Global Privacy Control (GPC), a recognized OOPS, operates through a different mechanism: a browser-side broadcast signal, transmitted as an HTTP header (Sec-GPC: 1) with every web request from the consumer's browser.[54] The signal does not require the consumer to submit an identifier, does not require CalPrivacy to distribute a list, and does not require the recipient to match the consumer's identity against a database.

The existing CCPA regulations already require businesses to apply opt-out preference signals not only to the browser or device on which the signal is detected, but also to "any consumer profile associated with that browser or device, including pseudonymous profiles."[55] Service-provider and contractor obligations under the same framework contemplate downstream propagation of opt-out signals through contractual chains.[56] How OOPS application extends to pseudonymous profiles in practice remains an area requiring further regulatory clarity, as the NAI has detailed in its preliminary comments on opt-out preference signals. NAI does not propose that opt-out preference signals substitute for DROP deletion where the DROP's matching mechanism can effectively reach a broker's records; rather, the two mechanisms are complementary by design. Both involve some form of matching, but the matching operates differently: DROP requires the consumer to submit static identifiers (such as a name, email, or phone number) that brokers then

[54] W3C Privacy Working Group, Global Privacy Control (GPC), W3C Working Draft (Apr. 23, 2026), https://www.w3.org/TR/gpc/ (defining the Sec-GPC HTTP header and JavaScript API for communicating consumer opt-out preferences).
[55] Cal. Code Regs. tit. 11, § 7025(c)(1); *see also* NAI OOPS Comments, *supra* note 7, at 10–11 (discussing application of OOPS to pseudonymous profiles and cross-device identifiers); Final Judgment and Permanent Injunction ¶ 26(b), *People v. Disney DTC, LLC*, No. 26STCV04425 (Cal. Super. Ct. L.A. Cnty. Feb. 11, 2026), https://oag.ca.gov/system/files/attachments/press-docs/CA_SUP_LAX_26STCV04425__Final_Judgment_and_Permanent_Injunction.pdf (requiring opt-out treatment to extend to associated "pseudonymous profiles").
[56] *See* Cal. Code Regs. tit. 11, § 7053(a)(3) (contemplating downstream third-party compliance with 'a consumer's request to opt-out of sale/sharing forwarded to it by a first-party business').

compare against identifiers stored in their own records. OOPS, by contrast, is a real-time signal transmitted from the consumer's browser to each business the consumer interacts with — the business reads the signal in-session and applies it to the browser or device that sent it, and (under existing CCPA regulations) to any pseudonymous profile the business has associated with that browser or device through its own cookie, device, or other contextual identifiers. OOPS therefore allows consumer privacy choices to reach pseudonymous profiles without requiring the consumer to submit a shared static identifier — a function the DROP's centralized list-matching architecture is not designed to perform.[57]

The DROP and OOPS provide consumers with enhanced controls over the processing of their personal information via different mechanisms, each designed for different data environments. Low or zero match rates in the DROP do not mean consumers in pseudonymous data environments lack meaningful privacy choices.

CalPrivacy's own regulatory work reinforces this. The CCPA already requires businesses to process opt-out preference signals as valid opt-out requests.[58] CalPrivacy is exploring parallel preliminary rulemaking on opt-out preference signal regulations,[59] and the legislature has passed the Opt Me Out Act to strengthen the GPC framework.[60] These efforts are specifically designed for the data environments where the DROP's cleartext matching is least effective.

C. IP Addresses Would Degrade Match Quality, Not Improve It

An identifier used for deletion matching needs to reliably identify a single individual, be verifiable by the collecting agency, and remain stable long enough for the broker to process the match. IP addresses fail all three tests.

IP addresses do not identify individuals. On residential networks, a single IP address typically serves every device in a household through the router's network address translation (NAT) function.[61] The same dynamic exists at much greater scale in commercial and institutional environments such as workplaces, schools, libraries, retail and hotel Wi-Fi networks where a single public IP address may be shared by hundreds or thousands of unrelated users at any given time.[62] On mobile networks, the problem is also severe. Mobile and broadband providers commonly use carrier-grade NAT (CGNAT) to conserve Internet Protocol version 4 (IPv4)

---

[57] *See* NAI OOPS Comments, *supra* note 7, at 10–11.
[58] Cal. Code Regs. tit. 11, § 7025.
[59] *See* Cal. Priv. Prot. Agency, *Invitation for Preliminary Comments: Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals* (Mar. 2026) https://cppa.ca.gov/regulations/pdf/pre_comments_reducing_friction_oops.pdf.
[60] *See* Cal. Civ. Code § 1798.136 (Opt Me Out Act provisions).
[61] *See generally* IETF, RFC 3022, Traditional IP Network Address Translator (Traditional NAT) (Jan. 2001), https://www.rfc-editor.org/rfc/rfc3022 (Internet Engineering Task Force technical specification defining NAT as a mechanism for mapping multiple private addresses to a single public address).
[62] *See* IETF, RFC 6269, Issues with IP Address Sharing (June 2011), https://www.rfc-editor.org/rfc/rfc6269 (IETF informational specification cataloguing technical and operational consequences of sharing single public IP among multiple users in residential, commercial, institutional, and mobile-network deployments).

address space, causing many unrelated users to share a single public IPv4 address.[63] CGNAT deployments have expanded significantly as IPv4 addresses have been exhausted, and the practice is standard in mobile networks worldwide.[64] A deletion request matched against an IP address shared through CGNAT or any other shared infrastructure could trigger deletion of records belonging to consumers who never submitted a request. Internet Protocol version 6 (IPv6), which is the newer version of the Internet Protocol that significantly expands the available address space, does not resolve these identification problems. IPv6 addresses are assigned to network interfaces (not to individual persons), and a single device may have multiple IPv6 addresses simultaneously.[65] In addition, IPv6 deployment remains incomplete, such that significant portions of consumer Internet traffic continue to traverse IPv4 networks subject to the same address-sharing and dynamic-assignment limitations.[66]

The DROP's verification framework does not extend to IP addresses. CalPrivacy's existing verification framework for email addresses and phone numbers works because those identifiers support a simple round-trip confirmation: send a message, receive a response confirming the consumer controls the identifier. IP addresses do not support an equivalent confirmation of consumer association or control. Although a website or application can observe the public IP address from which a consumer's current session originates, that observation does not establish that the consumer uniquely controls the address, will remain associated with it, or has not been sharing it with other users at the time of submission. A consumer's public IP address is assigned by their internet service provider (ISP), is typically not visible to the consumer without using a third-party lookup tool, and may change between the time the consumer looks it up and the time

[63] *See* IETF, RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space (Apr. 2012), https://www.rfc-editor.org/rfc/rfc6598 (reserving the 100.64.0.0/10 address block for use in carrier-grade NAT deployments); IETF, RFC 7021, Assessing the Impact of Carrier-Grade NAT on Network Applications (Sept. 2013), https://www.rfc-editor.org/rfc/rfc7021 (explaining that address sharing can make source IP address alone insufficient to identify the customer or endpoint responsible for a specific IPv4).

[64] *See* Livadariu et al., Inferring Carrier-Grade NAT Deployment in the Wild, IEEE INFOCOM 2018, at 2249, 2254, doi:10.1109/INFOCOM.2018.8486223, *available at* https://www.caida.org/catalog/papers/2018_inferring_carrier_grade_nat/inferring_carrier_grade_nat.pdf (finding that approximately 28.85% of inferred CGNAT deployments are located in mobile operator networks); Cloudflare, One IP Address, Many Users: Detecting CGNAT to Reduce Collateral Damage (Oct. 29, 2025), https://blog.cloudflare.com/detecting-cgn-to-reduce-collateral-damage/ (describing CGNAT as a widespread and growing source of IP address sharing and associated collateral effects when per-user assumptions are applied to shared IP addresses).

[65] *See* IETF, RFC 4291, IP Version 6 Addressing Architecture (Feb. 2006), https://www.rfc-editor.org/rfc/rfc4291 (IPv6 unicast addresses identify a single network interface, not a natural person, and an interface may be assigned multiple IPv6 addresses simultaneously).

[66] *See* APNIC Labs, Use of IPv6 for World, https://stats.labs.apnic.net/ipv6 (continuously updated 30-day measurements showing IPv6 capability remains inconsistent); *see also* Google, IPv6 Adoption Statistics, https://www.google.com/intl/en/ipv6/statistics.html.

they submit it.[67] It is not clear how CalPrivacy could confirm that a consumer submitting an IP address actually controls or is uniquely associated with that address.[68]

IP addresses are ephemeral. Many consumer ISP connections use dynamically assigned public IP addresses, which can change over time; where the Dynamic Host Configuration Protocol (DHCP) is used, the protocol assigns addresses for finite lease periods.[69] A single consumer also typically uses multiple public IP addresses across a single day as their device moves between networks (for example, a home connection, a mobile network, and a workplace or commercial Wi-Fi network). Each of those networks would provide a different public-facing IP address through that network's gateway.[70] On mobile networks using CGNAT, the association between a subscriber and a public IP address may last only for a single browsing session. The IP address a consumer submits to the DROP today may correspond to a different subscriber by the time the broker processes the deletion list 45 days later.

These problems compound. An IP-based match would produce results that neither the broker nor the auditor can evaluate with confidence: the identifier may point to the wrong person, the consumer may not have controlled it, and it may no longer correspond to the data the broker holds. CalPrivacy should not add an identifier to the DROP that increases the risk of incorrect deletions while producing match results that are unverifiable.

SECTION 6: MATERIALS ACCOMPANYING AUDIT REPORTS

CalPrivacy asks: When CalPrivacy requests an audit report, what other materials, at minimum, do you recommend be submitted to CalPrivacy at the same time?

A. Scope of Audit Reports and Supporting Materials

A well-designed audit reporting framework should give CalPrivacy reliable visibility into compliance without turning every audit into a voluminous production event. When every broker must produce a full report and supporting materials regardless of whether an audit raises concerns, brokers spend time assembling and validating production materials that may never be

[67] Consumers' public-facing IP addresses are assigned by their ISP and are not typically displayed in device settings, which commonly display the device's local network IP address allocated from the IETF's RFC 1918 private address ranges. *See* IETF, RFC 1918, Address Allocation for Private Internets (Feb. 1996), https://datatracker.ietf.org/doc/html/rfc1918 (IETF specification reserving specific IP address blocks for use within private networks rather than the public internet — these are the addresses devices typically display in their network settings). Determining one's own public IP address generally requires visiting a third-party website (e.g., whatismyip.com), which introduces the possibility of error or delay between lookup and submission.

[68] The NAI previously raised similar issues with CalPrivacy, discussing why probabilistic identifiers, including those derived from IP addresses, are poor candidates for DROP matching given that they are not directly accessible by consumers, are ephemeral due to ISP rotation and similar factors, and lack standardization. *See* NAI Questionnaire Response, *supra* note 53.

[69] *See* IETF, RFC 2131, Dynamic Host Configuration Protocol (Mar. 1997), https://www.rfc-editor.org/rfc/rfc2131 (IETF specification for the Dynamic Host Configuration Protocol used by most residential ISPs to assign IP addresses dynamically with finite lease durations).

[70] *See id.*; IETF, RFC 6269, *supra* note 61 (cataloguing network-mobility implications of shared and dynamically assigned addresses).

examined, and CalPrivacy must receive, process, and store those materials whether or not it intends to review them. Reserving full production for cases where a broker's compliance warrants closer examination focuses both parties' resources on the cases that matter.

Under the Delete Act, when CalPrivacy makes a written request, the broker must submit the audit report and any related materials within five business days, and brokers must maintain those materials for at least six years.[71] Still, CalPrivacy retains discretion to define routine submission obligations, the scope of "related materials" production when requested, and the conditions under which additional production is warranted. CalPrivacy has already built a workable model along these lines for cybersecurity audits, where businesses submit a certification of completion routinely and CalPrivacy requests the full report when a business's compliance warrants closer examination.[72] CalPrivacy should adopt a parallel targeted reporting model for DROP audits.

Within that framework, when CalPrivacy requests supporting materials in a specific case, the production should be limited to documentation that serves the audit's purpose: verifying whether the broker complied with the deletion processing requirements. Requiring materials beyond that scope does not improve CalPrivacy's ability to evaluate compliance. It converts the audit into a vehicle for collecting business information unrelated to the questions the auditor was asked to evaluate, which diverts both the broker's and CalPrivacy's resources from the compliance questions that matter. Specifically, any supporting materials should be limited to what is necessary to track the compliance components the auditor evaluated (which, as discussed above, may include standardization and hashing procedures, DROP access and processing logs, match results with explanation of zero-match outcomes, evidence of deletion and downstream direction for matched records, suppression list maintenance records, and documentation of any statutory exceptions invoked).[73] Consistent with established audit practice, the audit report itself should also identify the organizational roles responsible for the broker's deletion processing. This could include, for example, the role responsible for compliance oversight, the operational roles responsible for executing the processing steps, and the points of contact who participated in the auditor's engagement. This would also avoid needless submission of personnel lists or other individual employee information beyond what is necessary to support the auditor's findings.

B. Confidential Treatment of Audit Materials

Audit materials documenting brokers' internal compliance processes should be presumed confidential. The Delete Act already provides the public with meaningful transparency into data broker practices through consumer-facing mechanisms. Specifically, the data broker registry already provides transparency into the categories of personal information registered brokers collect and sell, the number of consumer requests they receive and process, and the other laws

[71] Cal. Civ. Code § 1798.99.86(e)(2)-(3).
[72] *See* Cal. Code Regs. tit. 11, § 7124 (requiring submission of a certification of compliance for cybersecurity audits, with the full report produced only on CalPrivacy's request).
[73] These categories correspond to the documentation framework described in Section 3, *supra*, mapped to the compliance components in Cal. Code Regs. tit. 11, § 7613(a)–(d).

that regulate their activities.[74] The CCPA separately provides consumers the right to request access to their personal information directly from data brokers.[75] These mechanisms give the public and CalPrivacy ongoing visibility into what brokers collect, how they respond to consumer requests, and whether they are participating in the system.

Audit materials serve a different function. They document the internal processes a broker uses to comply with its deletion obligations. This may often be proprietary operational information about business systems, not consumer-facing data about what a broker collects or how it responds to requests. The same audit materials that document compliance also describe the broker's matching architecture, hashing implementation, suppression-list design, and access controls in detail sufficient to evaluate them — information that, if disclosed publicly, could provide a roadmap for adversaries seeking to circumvent or exploit those controls. Because the Delete Act's transparency objectives are already served by the registry, the DROP's consumer-facing features, and CCPA rights, there should be a presumption that audit materials documenting internal compliance processes qualify for confidential treatment.[76] Where particular portions of audit materials reflect proprietary investment in matching methodology, data architecture, or processing-pipeline design, those portions may also qualify for protection under California trade-secret law.[77]

To facilitate confidential treatment of audit information, CalPrivacy should establish a designation process in the regulations allowing brokers to identify trade secret and confidential business information at the time of submission and provide a supporting justification. This allows CalPrivacy to evaluate any public records requests against the applicable statutory exemptions using a clear record, rather than forcing confidentiality to be resolved through ad hoc disputes after materials have been filed.

SECTION 7: ADDITIONAL CONSIDERATIONS

CalPrivacy asks: What else should CalPrivacy consider in developing data broker audit regulations?

A. Transition Guidance Before the First Audit Period

Reliable audits depend on documentation that was created contemporaneously with the activity being evaluated. When regulated entities know in advance what an auditor will examine, they

[74] *See* Cal. Civ. Code § 1798.99.82(b) (requiring disclosure of categories of personal information collected and sold, consumer request metrics, and other regulatory information in annual registry filings); Cal. Civ. Code § 1798.99.85(a) (requiring disclosure of consumer request metrics on the broker's website).
[75] *See id.* § 1798.110 (providing consumers the right to request that a business disclose the categories and specific pieces of personal information it has collected); *id.* § 1798.115 (providing the right to know about the sale or sharing of personal information); *id.* § 1798.130 (specifying procedures for responding to verifiable consumer requests).
[76] *See* Cal. Gov. Code § 7922.000 (Public Records Act case-specific public-interest balancing test, permitting agencies to withhold records where the public interest in nondisclosure clearly outweighs the public interest in disclosure).
[77] *See* Cal. Civ. Code § 3426.1(d) (defining trade secrets under California law, where particular portions of audit materials may independently qualify).

build systems that capture the right information as operations occur. When they do not, the auditor must work with records that were assembled after the fact and may be incomplete, inconsistent, or organized in ways that make evaluation difficult. CalPrivacy's interest in a successful first audit cycle is best served by issuing documentation guidance before DROP processing begins on August 1.

Two ambiguities in the current statutory timeline risk producing inconsistent audit outcomes if left unresolved. First, what period does the first audit cover? Deletion obligations under the DROP begin August 1, 2026, and audits are required "beginning January 1, 2028, and every three years thereafter."[78] January 1, 2028 could refer to the date the audit requirement takes effect; or it could refer to the date by which the first audit must be completed. Resolving that ambiguity will determine whether the first audit covers roughly 18 months of deletion processing (August 2026 through December 2027) or some shorter window. Without clarification, different auditors may apply different temporal scopes, producing audit results that CalPrivacy cannot meaningfully compare across brokers.

The NAI recommends that CalPrivacy define the first audit period to begin no earlier than six months after the release of final audit regulations. Companies integrated with the DROP cannot reasonably build documentation systems that conform to audit requirements until those regulations are final. If the regulations are finalized in early 2027, for example, the first audit period would begin in mid-2027 and the January 2028 audit would cover roughly six months of operations. If the regulations are finalized earlier, the audit period would be longer. This approach gives CalPrivacy control over the timeline: the earlier it finalizes regulations, the longer the first audit period. And it ensures that whatever period the first audit covers, brokers had the benefit of final guidance before that period began.

If CalPrivacy declines to define the first audit period in this manner, an alternative would be to provide that brokers are not subject to adverse audit findings for documentation gaps relating to deletion processing that occurred before the release of final audit regulations, provided the broker can demonstrate good-faith compliance with the DROP regulations in effect at the time and implements the final documentation requirements prospectively. Either approach addresses the same underlying concern, which is that audit findings should evaluate operational history that occurred under known requirements rather than retrospective documentation expectations. Second, the statute requires six-year retention of audit reports and related materials but does not address what records brokers should maintain before the first audit occurs.[79] If CalPrivacy expects auditors to evaluate deletion processing from the start of the audit period, brokers need to know what documentation to produce and retain starting from the first 45-day cycle. Standardized recordkeeping expectations established in advance ensure that auditors evaluate actual operational history rather than post-hoc reconstructions. CalPrivacy should issue guidance on minimum documentation requirements before the August 2026 operational deadline, drawing on the documentation categories described in Section 3 above.[80]

[78] Cal. Civ. Code § 1798.99.86(c); (e)(1).
[79] Cal. Civ. Code § 1798.99.86(e)(3) (requiring retention of the audit report and any related materials for six years).
[80] *See supra* Section 3 (defining documentation categories mapped to the compliance components in Cal. Code Regs. tit. 11, § 7613(a)–(d)).

B. First-Cycle Implementation of the Triennial Audit Requirement

CalPrivacy should phase first-cycle audit completion across calendar years 2028 and 2029 for brokers subject to the audit obligation as of January 1, 2028, and should adopt a defined placement rule for brokers that first become subject to registration after that date. Phasing will help protect audit quality, because independent third-party audits are only as reliable as the audit-provider market that delivers them, and concentrating every first-cycle completion into 2028 would create capacity strain that works against audit quality.

A functioning audit-provider market needs time to develop the capacity that high-quality DROP audits require. However, it is likely that compressing all first-cycle audits into a single calendar year would have two predictable effects: it would strain auditor supply when many brokers need auditors most, and it would produce uneven utilization in subsequent years as later cycles repeated the concentration. Both effects undermine audit quality.

CalPrivacy has adopted phased audit-completion schedules in its cybersecurity audit program,[81] and that program shows that staggered completion is a familiar regulatory technique for complex audit obligations. And even though the Delete Act fixes when the audit obligation begins, it nevertheless leaves the operational mechanics for CalPrivacy to specify through regulation. Specifically, every covered data broker must undergo an independent third-party audit beginning January 1, 2028, with audits recurring every three years thereafter.[82] But the statute does not specify the audit period, the deadline by which a broker must complete its audit, the method for sequencing audits across the registered population, or when audit reports must be submitted (except for the five-business-day response window after a written CalPrivacy request).[83]

Under the Agency's rulemaking authority,[84] subject to the California Administrative Procedure Act's requirement that regulations be consistent with the statute and reasonably necessary to effectuate its purpose,[85] CalPrivacy may make those implementation details specific. Doing so would not change which brokers are subject to the audit obligation, when the obligation begins, or how often it recurs. For brokers subject to the audit obligation as of January 1, 2028, audit activities (such as scoping the review and engaging a qualified third party) should commence no later than that date. The assigned audit should cover the period from commencement through the broker's assigned completion deadline, so that a later completion date affects only when the audit finishes, not the scope of conduct subject to first-cycle review. The assignment of brokers to first-cycle completion deadlines in 2028 or 2029 should use transparent, objective, and administrable criteria.

Late-registering brokers should be assigned according to the date they were required to register, not the date they actually registered. Brokers that first become subject to registration after

---

[81] *See* Cal. Code Regs. tit. 11, § 7121 (cybersecurity audit phased implementation schedule).
[82] Cal. Civ. Code § 1798.99.86(e)(1).
[83] *Id.* § 1798.99.86(e)(2) (broker must submit audit report and related materials within five business days of CalPrivacy's written request).
[84] Cal. Civ. Code § 1798.99.87(a) (authorizing CalPrivacy to "adopt regulations . . . to implement and administer this title").
[85] Cal. Gov. Code § 11342.2 (no regulation is valid unless "consistent and not in conflict with the statute" and "reasonably necessary to effectuate the purpose of the statute").

January 1, 2028 should be assigned a first-cycle completion deadline of 2030, with the assigned audit period beginning no later than the date the broker first became subject to the registration obligation. This rule places newly subject brokers at the back of the first cycle, gives them a defined placement that does not depend on Agency case-by-case discretion, and avoids extending any individual broker's first-cycle interval beyond the statutory three-year window. Subsequent cycles would commence on the statute's three-year anchor: each cycle begins on January 1 of 2031, 2034, and so on, with CalPrivacy again staggering completion deadlines within the cycle. A broker assigned to a 2028 first-cycle completion would be due no later than 2031 in the second cycle; a 2029 broker, no later than 2032; a 2030 broker, no later than 2033. This structure preserves the statute's triennial recurrence at the cycle level while distributing audit-completion demand within each cycle. The annual registration disclosure beginning January 1, 2029[86] gives CalPrivacy a mechanism to track audit status and report-submission history across the broker population, supporting administration of the phased schedule.

C. Coordination with the Cybersecurity Audit Program

Regulatory programs overseen by the same agency and evaluated during overlapping periods should be designed to avoid duplicative assessment of the same controls. The DROP audit and the cybersecurity audit are both administered by CalPrivacy. NAI urges CalPrivacy to align administration of the DROP audit program with the Audits Division's existing oversight of cybersecurity audits to enable the coordination described below. Their first cycles nearly overlap: the cybersecurity audit for businesses with annual gross revenue exceeding $100 million covers January 2027 through January 2028, with certification due April 2028; the DROP audit requirement begins January 1, 2028.[87] Many data brokers will be subject to both programs in the same year.

The two programs evaluate different requirements, but they share common ground on data security. The DROP regulations require brokers to implement and maintain reasonable security procedures for personal information provided through the DROP and to maintain secure account credentials.[88] The cybersecurity audit evaluates security controls across the business's information systems. Where the cybersecurity audit already evaluates security controls relevant to DROP data, requiring the DROP auditor to independently re-evaluate those same controls produces duplicative findings without improving the quality of CalPrivacy's oversight. CalPrivacy should permit DROP auditors to rely on cybersecurity audit findings for security controls that apply to DROP data, rather than conducting a separate evaluation of the same controls. The cybersecurity audit regulations already contemplate leveraging audits conducted for other regulatory purposes.[89] CalPrivacy should apply the same principle to coordination between the two audit programs it administers.

---

[86] Cal. Civ. Code § 1798.99.82(b)(2)(U) (annual registration disclosure of audit status and most recent year of report submission, beginning January 1, 2029).
[87] *See* Cal. Code Regs. tit. 11, § 7121 (cybersecurity audit phased implementation schedule); *id.* §§ 7122–7124 (audit thoroughness, scope, and certification requirements); Cal. Civ. Code § 1798.99.86(e)(1) (DROP audit timing).
[88] Cal. Code Regs. tit. 11, § 7616(b) (requiring reasonable security procedures for personal information provided through the DROP); *id.* § 7610(a)(1) (requiring secure account credentials and maintenance).
[89] *See id.* § 7123(f).

*****

CONCLUSION

The NAI appreciates CalPrivacy's commitment to developing a well-designed audit framework for the DROP. The decisions CalPrivacy makes in this rulemaking will shape the audit experience for every registered data broker and determine whether the process produces compliance information that is useful for CalPrivacy's oversight. The NAI stands ready to provide additional input as CalPrivacy moves from preliminary comments to formal rulemaking. We welcome the opportunity to engage further on any of the topics raised in this letter and to work constructively with the Agency to develop audit regulations that serve CalPrivacy's oversight objectives, produce reliable compliance information, and reflect the diversity of data broker data environments.

Sincerely,

Tony Ficarrotta

Vice President, General Counsel

The NAI

Catbagan, Christian@CPPA

From: Anton Van Seventer <avanseventer@SIIA.net>
Sent: Thursday, May 7, 2026 1:41 PM
To: Regulations@CPPA
Subject: Preliminary Comment – DROP Audits April 2026
Attachments: SIIA Preliminary Comment – DROP Audits April 2026.pdf

Dear CalPrivacy Team,

Please find attached the Software & Information Industry Association's (SIIA's) preliminary comments in response to the California Privacy Protection Agency's Invitation for Preliminary Comments on the Delete Request and Opt-Out Platform (DROP) Audits.

Thank you for the opportunity to provide input on this important rulemaking.

Respectfully,

Anton van Seventer
Counsel, Privacy and Data Policy
SIIA - Accelerating Innovation in Technology, Data & Media
PO Box 34340, Washington, DC 20043

avanseventer@siia.net
Telephone: +1-202-789-4471
Mobile: [redacted]
LinkedIn: https://www.linkedin.com/in/antonvanseventer

May 7, 2026

CalPrivacy Staff
California Privacy Protection Agency
Attn: Legal Division – Regulations
400 R St., Suite 350
Sacramento, CA 95811

Submitted via email to regulations@cppa.ca.gov

Re: Preliminary Comments on Proposed DROP Audit Requirements (Invitation for Preliminary Comments, May 7, 2026)

CalPrivacy Staff:

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital information industries. Our nearly 400 members include cloud service providers, developers of software — including AI systems — and platforms, as well as digital content providers and users in academic publishing, education technology, financial information, and financial services. SIIA is dedicated to fostering a healthy environment for the creation, dissemination, and productive use of information. We submit these preliminary comments because the triennial audit required by Civil Code § 1798.99.86(e) will affect SIIA members that fall within the Delete Act's scope and may serve as a template for similar efforts in other states.

SIIA appreciates CalPrivacy's decision to seek preliminary input before drafting regulatory text. Our top line recommendation is that the Agency design the audit to be workable, proportionate, and consistent with the framework finalized in September 2025 for CCPA cybersecurity audits at 11 CCR §§7120-7124. That framework establishes familiar, robust standards for auditor independence, scope, evidence, confidentiality, and leveraging prior-purpose audit work. Conforming to the same approach to audit broker's compliance with delete requests made through the Delete Request and Opt-Out Platform (DROP) will help to ensure compliance and avoid unnecessary administrative burdens on companies and the CCPA.

Summary of SIIA's Primary Recommendations

SIIA recommends that CalPrivacy:

- Accept recognized auditor credentials paired with the functional independence test of 11 CCR §7122, rather than create a bespoke DROP-only California auditor certification or narrow the qualified pool to a small set of large accounting firms.
- Define minimum audit procedures by rule, to include suppression list sampling, 45-day cycle verification, match rate integrity testing, and downstream flowdown review.
- Avoid expanding the DROP audit framework beyond the scope of the Delete Act by including AI-specific audit overlays.
- Mirror 11 CCR §7124 on certification-only submission and adopt a confidentiality posture treating the audit report and related materials as trade secret and investigatory material consistent with applicable Public Records Act exemptions.
- Expressly extend the 11 CCR §7123(d)-(f) leverage mechanism to SOC 2 Type II, ISO 27701, NIST Privacy Framework, and completed CCPA cybersecurity audits, with DROP-specific supplemental procedures defined by rule.

Auditor Qualifications (Question 1)

Civil Code § 1798.99.86(e)(1) requires an "independent third party" but does not specify credentials or organizational form. SIIA urges CalPrivacy to adopt a recognized credential plus functional independence standard consistent with 11 CCR §7122, which permits internal or external auditors with documented independence and evidence-based findings. Recognizing Certified Public Accountants, Certified Information Systems Auditors, ISO/IEC 17021-accredited certification bodies, and other qualified audit professionals — including those working in conjunction with credentialed privacy professionals such as CIPP/US or CIPM holders — would ensure a competitive market of qualified auditors. By contrast, a bespoke California-only auditor certification applicable only to assess Delete Act compliance, or eligibility rules that effectively require engagement of a small number of very large firms, would impose bottlenecks, raise costs disproportionately for mid-market registrants, and produce little commensurate consumer benefit. The statute's independence requirement should remain focused on function, not firm size.

Scope and Methodology (Questions 2 and 3)

CalPrivacy's rulemaking authority here is bounded by the deletion compliance purpose of Civil Code § 1798.99.86, not the broader rulemaking authorities under Civil Code § 1798.185(a)(14)-

(16). Regulations requiring procedures unrelated to deletion processing compliance would be difficult to sustain under the Administrative Procedure Act's "reasonably necessary" standard.

Within that scope, SIIA recommends that CalPrivacy specify minimum procedures by rule: suppression list sampling, 45-day processing cycle verification, match rate integrity testing against the DROP dataset, and review of the flowdown of deletion instructions to service providers and contractors under § 1798.99.86(c). Rule-specified procedures protect both regulated parties and the Agency. Otherwise, the regime risks inconsistent results, including contested compliance and predictable disputes over what the audit was supposed to cover.

SIIA further urges CalPrivacy not to mandate specific audit tools by regulation. Tools evolve, and rule-frozen tooling becomes outdated and creates compliance traps without improving consumer outcomes.

Finally, Question 3 raises whether agentic AI systems should trigger different audit requirements. SIIA submits that Civil Code § 1798.99.86 provides no statutory hook for AI-specific audit obligations in a deletion-compliance audit, and that grafting these kinds of obligations onto this regime without express legislative authority would likely exceed the Agency's enumerated rulemaking power. If the Agency concludes AI-specific audit obligations for data brokers are warranted, the appropriate course is to seek clarifying legislation rather than build them into DROP audit rules.

Confidentiality and Framework Reuse (Question 5)

SIIA recommends that CalPrivacy mirror 11 CCR §7124, including its protections for trade secret and investigatory material.That approach is consistent with Civil Code § 1798.99.86(e)(2), which already provides for production only on written request. SIIA further advises that CalPrivacy adopt a confidentiality posture treating the audit report and related materials as trade secret and investigatory material consistent with applicable Public Records Act exemptions, to avoid unnecessary discovery exposure of sensitive deletion pipeline details, including suppression list architecture and match algorithms whose disclosure itself raises security concerns.

We also urge CalPrivacy to extend the leverage mechanism of 11 CCR §7123(d)-(f) to this regime expressly. A registrant that has completed a SOC 2 Type II examination with the Privacy and Confidentiality Trust Services Criteria, an ISO 27701 certification, an attestation against the NIST Privacy Framework, or its CCPA cybersecurity audit under §§7120–7124, should be able to satisfy the DROP audit obligation by supplementing that prior-purpose work with DROP-specific procedures defined by the rule. SIIA conveyed this issue in our February 19, 2025 comments on

cybersecurity audit and risk-assessment rulemaking, and it applies with at least equal force here because the DROP audit is narrower in scope. Establishing such a regime, however, requires the Agency to specify the supplemental procedures in the final rule so that reuse is predictable.

Additional Considerations

First, SIIA recommends that the triennial cadence set by Civil Code § 1798.99.86(e)(1)not be supplemented with interim attestations or annual certifications. We believe doing so would exceed the Agency's enumerated rulemaking power and is not authorized by the statute.

Second, when CalPrivacy reaches formal rulemaking, we recommend that the Standardized Regulatory Impact Assessment account for the cumulative burden on regulated companies, not just the burden that is state-specific. Cumulative burden includes the $6,000 annual DROP registration fee, 45-day processing cycles, U.S. Department of Justice Data Security Program audit obligations now running for some registrants under 28 CFR Part 202, and anticipated audit regimes in New York and Vermont.

Third, because no federal data broker audit standard currently exists and California's framework will influence follow-on state regimes, SIIA recommends that CalPrivacy consider the importance of proportionate and framework-consistent design to improve compliance, increase consistency of audit processes across jurisdictions, reduce administrative burden on California, and help to minimize multi-regime compliance challenges.

SIIA appreciates the opportunity to submit these preliminary comments, and is prepared to provide additional information at the Agency's convenience if helpful.

Respectfully submitted,

Anton van Seventer
Counsel, Privacy and Data Policy
Software & Information Industry Association
avanseventer@siia.net

Catbagan, Christian@CPPA

From: Sara Geoghegan <geoghegan@epic.org>
Sent: Thursday, May 7, 2026 2:31 PM
To: Regulations@CPPA
Cc: Mayu Tobin-Miyaji; Alan Butler
Subject: Preliminary Comment – DROP Audits
Attachments: EPIC-05-07-2026 Delete and Drop Audit Comments.pdf

Hello,

On behalf of the Electronic Privacy Information Center, please find attached comments in response to the agency's April 2026 invitation for preliminary comment on the DROP audits.

Sara Geoghegan (she/her)
Director, Consumer Privacy Project & Senior Counsel
Electronic Privacy Information Center
202.483.1140 x129
https://www.epic.org/

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

3COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

California Privacy Protection Agency

on

Delete Request and Opt-Out Platform (DROP) Audits

May 7, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the invitation of the California Privacy Protection Agency ("Agency" or "CalPrivacy") for preliminary comment on data broker audit requirements for processing deletion requests, published on April 7, 2026.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has previously provided comments on the California Consumer Privacy Act (CCPA),[3] published a detailed analysis of the California Privacy Rights Act before its approval by

[1] Invitation for Preliminary Comments: Delete Request and Opt-Out Platform (DROP) Audits, Cal. Privacy Protection Agency (Apr. 7, 2026).
[2] *About Us*, EPIC, https://epic.org/about/ (2025).
[3] Comments of the Electronic Privacy Information Center (EPIC) and the Consumer Federation of America (CFA) in Response to the California Privacy Protection Agency's Proposed Rulemaking Regarding Cybersecurity, Risk Assessments, and Automated Decisionmaking Technology (Feb. 19, 2025), https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/; 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 (June 25, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/06/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agencys-Invitation-for-Preliminary-Comments-On-Proposed-Rulemaking-Under-Senate-Bill-362.pdf; Comments Of The Electronic Privacy Information Center, Center For Digital Democracy, and Consumer Federation Of America, to the California

California voters,[4] and presented oral testimony to the Agency to encourage the strongest protections for Californians.[5] Further, EPIC has advocated for best practices in algorithmic assessment requirements submitted to California regulators.[6]

EPIC commends the Agency's work to regulate data brokers, especially in light of recent evidence[7] that reports submitted by brokers are potentially unreliable or inaccurate. Robust independent third-party audit requirements are a crucial step towards oversight and limiting the harms that sale of sensitive data poses to consumers. EPIC believes that, in order to establish an effective audit process, the Agency should establish requirements and processes that ensure: (1) that auditors independently verify brokers' conclusions and should require detailed explanations of the compliance process given brokers' demonstrated inability to accurately self-report; and (2) that brokers implement additional audit requirements when they use AI systems. The Agency should also

Privacy Protection Agency (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/; Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Nov. 8, 2021), https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf.

[4] EPIC, California's Proposition 24 (2020), https://epic.org/californias-proposition-24/.

[5] EPIC Calls Out CPPA as Board Votes to Adopt Weak Risk Assessment, ADMT, and Cybersecurity Regulations, EPIC (July 24, 2025), https://epic.org/cppa-votes-to-adopt-weak-cybersecurity-risk-assessments-and-admt-regulations/.

[6] Mayu Tobin-Miyaji, et al., *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments*, EPIC at 37-38 (June 2025), https://epic.org/wp-content/uploads/2025/06/Assessing-the-Assessments-Report.pdf.

[7] Justin Sherman, *The Data Brokers Selling US Data to Foreign Actors, According to California*, EPIC (Mar. 25, 2026), http://epic.org/the-33-data-brokers-selling-us-data-to-foreign-actors-according-to-california/; *Privacy Policy: California Data Broker Registry Reveals Dozens of Brokers Selling Consumers' Data to Foreign Actors, Law Enforcement, Federal Government*, Capitol Forum (Apr. 1, 2026), https://thecapitolforum.com/privacy-policy-california-data-broker-registry-reveals-dozens-of-brokers-selling-consumers-data-to-foreign-actors-law-enforcement-federal-government/.

consider the experiences and lessons learned from the technical framework from Europe's GDPR right to be forgotten.

Audit requirements should prevent auditors from rubber stamping or accepting as true conclusions from brokers. A robust audit process requires independent verification of the claims being submitted by data brokers. It is not sufficient to take these data broker submissions at face value.[8] Independent testing and inspection by an auditor is necessary to ensure accuracy in the registry data. CalPrivacy should require each broker to provide a detailed explanation of the compliance process it followed when self-reporting information for the registry. Brokers cannot reliably represent that they've deleted all applicable data if they have not at least gone through the de minimis data mapping required by the registry process. Accordingly, this information should be made available to auditors for inspection.

EPIC suggests that when a data broker uses AI or agentic AI systems that there should be additional audit requirements to review those AI systems. Data brokers should be required to submit the factors and logic of any algorithm used, the kinds of data that the AI system collects or processes, the source of the training data in the underlying model of the system, the processing context for such data, and the results of testing for bias, inaccuracy, reliability, disparate impact, and data security.[9] Brokers that use AI systems should also submit evidence about the how the quality of the input is maintained and how the system will be free from inaccuracy, unreliability, bias, or disparate impact in the future, including by providing metrics to measure the system's performance and its known limitations.[10]

---

[8] *Id*.
[9] *See* Mayu Tobin-Miyaji, et al., *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments*, EPIC at 37-38 (June 2025), https://epic.org/wp-content/uploads/2025/06/Assessing-the-Assessments-Report.pdf.
[10] *Id.*

EPIC suggests that the Agency consider the technical infrastructure requirements needed to execute erasure effects under the European Union General Data Protection Regulation's right to be forgotten. These include requiring entities to build technical infrastructure for: data mapping to know where personal information resides across platforms; search capabilities to location individuals' personal information; mechanisms for deletion that can remove information without disrupting system integrity; and audit trails to document erasure actions.[11] Importantly, building this technical infrastructure also requires building the technical ability to remove personal information while retaining it in backup archives with sufficient safeguards to protect against reintroduction.[12] The Agency should implement similar requirements to protect against reintroduction, particularly when partial deletion is appropriate.

EPIC appreciates CalPrivacy's attention to this important issue. Regulators play a pivotal role in reigning in the harmful practices of data brokers. Robust enforcement requires accurate and complete information in order to be effective. But as we have seen, the data broker industry repeatedly evades regulation, including by failing to accurately and completely provide relevant information to regulators. The Agency should consider this pattern of regulatory evasion when establishing audit requirements and enact stringent requirements to ensure effective audits. We thank CalPrivacy for the opportunity to provide preliminary comment on this topic, and we look forward to working with the Agency in the future to protect the privacy of all Californians.

Respectfully Submitted,

/s/ Sara Geoghegan
Sara Geoghegan
Director, Consumer Privacy Program & Senior Counsel
geoghegan@epic.org

[11] Kevin Yun, *Right to be Forgotten: Deleting Your Digital Past*, ComplyDog (May 17, 2025), https://complydog.com/blog/right-to-be-forgotten#practical-steps-for-data-controllers.
[12] *Id.*

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

Catbagan, Christian@CPPA

From: Ben Isaacson <ben@inhouseprivacy.com>
Sent: Thursday, May 7, 2026 3:45 PM
To: Regulations@CPPA
Subject: Preliminary Comment – DROP Audits
Attachments: In-House Privacy, Inc. Preliminary Comments to CPPA Re_ DROP Audits 5.7.26.pdf

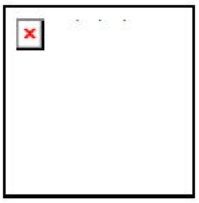
Greetings,

On behalf of In-House Privacy Inc, I am submitting the following written comments. I welcome any feedback or the opportunity to further clarify these comments at any time.

Best regards,

--Ben Isaacson

--



Ben Isaacson **Principal | In-House Privacy, Inc.** CIPP/US, CIPP/E **m.** [redacted] **w.** **www.inhouseprivacy.com** **e.** **ben@inhouseprivacy.com**

May 7, 2026

California Privacy Protection Agency
Attn: Legal Division - Regulations
400 R Street, Suite 350
Sacramento, CA 95811

Submitted electronically to: regulations@cppa.ca.gov

Re: Preliminary Comments - Delete Request and Opt-Out Platform (DROP) Audits

In-House Privacy, Inc. ("IHP") is a law firm that serves numerous businesses subject to the California Delete Act. IHP submits these comments on its own behalf.

Questions for Preliminary Comment

1. **What credentials, certifications, or independence requirements do you recommend third party auditors possess to ensure they are qualified and sufficiently independent?**

    A. **Audit experience.** The third party auditors should be practiced in audits (e.g., already do SOC 2 Type II audits, ISO 27001, ISO 27701 or the like) or they should be established privacy consultants who regularly review policies and practices for data governance. CalPrivacy could implement an approved vendor initiative akin to the Federal Trade Commission's COPPA Safe Harbor Program.

    B. Legal review. Auditors will need legal analysis to review the scope of the audit to determine where the Delete Act/DROP is applicable to the data broker data processing activities, and where legal exceptions may apply. The Delete Act requires that data brokers limit the deletion and/or suppression from the DROP to data that is 'sold', but many data brokers also provide data-related services that are exempt from Delete Act/DROP application. In order for an audit to be effective, the auditor must align with legal reviewers in order to determine where exceptions to DROP application may apply based on specific use cases and document the rationale for those exceptions.

    C. Data governance technical expertise. As the DROP requires various technical integrations and applications, including cryptography, the auditor must be knowledgeable about how companies govern all aspects of data processing, including key cryptographic matching methods used by data brokers to ensure the DROP the specifications are accurately applied. The International Association of Privacy Professionals maintains certifications for individuals who are 'technologists' (CIPT) which could be expanded upon to include CalPrivacy DROP audit requirements for future certifications that would enable more individual consulting opportunities and cost effective audits vs requiring data brokers to rely upon traditional auditor firms.

2. **What records, documentation, or other evidence would demonstrate in an audit whether a data broker has properly processed consumer deletion requests?**

   For example, what documentation should a data broker be required to maintain for audit purposes that evidences: how they have standardized and hashed their data; their method for matching their data to that from CalPrivacy; whether they are deleting information when finding a match while only retaining allowable data; and how they are using the deletion list(s) they maintain solely to compare with any new records (also known as a "suppression list")?

   Data brokers already maintain a record of the number of data subject requests they've received from Californian Consumers, whether these requests were honored in whole or in part, whether they were denied in whole or in part, and the median and mean number of days to respond. Data brokers also commonly create and apply suppression lists that extend beyond strict compliance requirements, which often include processes and procedures to create and maintain record-keeping logs of all suppression processing activities. These processes and procedures, as well as the record-keeping logs, could be available on-demand to auditors in addition to the DROP application verifications.

   It is also recommended for the CPPA to provision auditor-specific DROP accounts in order for auditors to access and verify data broker activities and reporting metrics independently of relying on data broker access records alone.

   Given data broker requirements to direct service providers and contractors to delete all personal information in its possession related to a consumer associated with a matched identifier in DROP, the data broker should provide to the third party auditor the records associated with all 'downstream' deletion and/or suppression file management activities.

   As noted, auditors will be required to have data governance expertise that includes a complete understanding of methodologies related to cryptographic hash-matching, and deletion policies and protocols including those related to passive data storage. It is expected for data brokers to maintain and produce robust data retention policies that incorporate all possible maintenance of data following DROP applications.

   An important note is that many data brokers maintain proprietary 'identity resolution' methods that should remain confidential during an audit, while enabling an auditor to determine that the methodology satisfies the Delete Act/DROP requirements. Again, some of these reviews may require legal support in order to determine where the scope of the DROP specifications may exempt certain data matching assets or methods.

3. **What audit practices, methods, standards, and/or technical tools should CalPrivacy consider adopting as requirements for data broker audits? Are there additional or different audit requirements you recommend when a data broker uses artificial intelligence (AI) or agentic AI systems?**

For example, should CalPrivacy consider audit practices used in the cybersecurity or banking sectors, and should auditors be required to use certain tools, such as data analytics or code-review software?

Many data brokers implement 'probabilistic' matching methods to create inferences or identity graphing across disparate data sets, some of which may be deployed using machine learning programs. An auditor should be familiar with these methods in order to enable a data broker to distinguish between a required DROP identity application and potentially exempt identifiers that are a low accuracy 'probabilistic match' against the DROP data. Again, legal analysis may be helpful in determining these distinctions.

4. **What audit requirements would allow CalPrivacy to determine if it should be requesting different identifiers from consumers to generate the highest number of matches between the DROP data and the data broker's data?**

   For example, CalPrivacy collects only zip codes from consumers, but if a full address would generate more matches—or another identifier altogether (e.g. IP address, etc.)—what evidence would demonstrate that?

   CalPrivacy should be verifying the consumer's postal address at the time of registration, and a validated residential postal address would be a reasonable addition to the other data points requested during registration.

   While some commenters may indicate that the collection of IP addresses would enable a very high match rate, this commenter strongly advises against expanding the scope to include IP addresses. The IP address provisioning system was not designed for identity resolution, and many data brokers who process such data are knowingly doing so based on a fundamental understanding that it is 'probabilistic' when matched to other potential identity records.

   An important point is that the 'match rate' is more aligned with the data retention policies of the data broker than the scope in which a data broker processes multiple identifiers. If a data broker serves as a transient intermediary between data sources and data recipients, they may only process data for less than the 45 day period in which the DROP may be applied resulting in a negligible match rate.

5. **When CalPrivacy requests an audit report, what other materials, at minimum, do you recommend be submitted to CalPrivacy at the same time?**

   A statement should be provided alongside a DROP audit that includes any notable exceptions to the DROP applicability. This statement should include any legal analysis,

product-specific data descriptions or data flows, and operational controls that exempt data sets from being applicable to DROP synchronization.

An auditor may also want to provide any descriptions and data broker justifications for situations where the DROP was not applied, such as where the data broker maintains a limited data retention policy and where the DROP access timing resulted in a low, or negligible, data match. The goal for such a statement is to avoid unnecessary CalPrivacy investigations of data brokers that do not produce high match rates with the DROP.

Auditors should also align with the CPPA on the methodology and reporting of anomalies and errors. This commenter has previously requested that CalPrivacy consider a 'safe harbor' for data brokers who regularly apply the DROP and where an audit report may indicate that an error took place 'in good faith' that does not result in a statutory penalty. A common example may be applicability of archival backups to the DROP and missing a mirroring backup system, or where a vendor does not delete such a backup by mistake.

6. What else should CalPrivacy consider in developing data broker audit regulations?

The definitional intersection of 'business' and 'data broker' under the CCPA and Delete Act does not require a $25mm annual revenue threshold,many small businesses are registered as California data brokers. As a result, CalPrivacy should advise small businesses on how to make these audits cost effective. Data brokers should not be deterred from completing a comprehensive audit due to the cost of compliance. (In addition to the $6000 registration fee and DROP integration costs, which are material costs for many small businesses.) Further, many data brokers will seek outside legal counsel to advise them in advance of, and during an audit, which will add to the cost of compliance with the audit.

Finally, to re-iterate, CalPrivacy should consider a safe harbor program for 'good faith' errors made by data brokers and/or a 'grace period' of at least the initial year of the audit period to ensure accurate compliance with risk of statutory penalties during the audit period.