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