May 20, 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 — Notices & Disclosures and Employee Data

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

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to submit comments in response to CalPrivacy's Invitation for Preliminary Comments on Notices & Disclosures and Employee Data.[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 voluntary industry standards for its member companies, which range from small startups to some of the largest companies in digital advertising, including ad exchanges, demand-side platforms, supply-side platforms, and other providers of advertising-technology solutions.

I. Introduction

The California Consumer Privacy Act's ("CCPA") builds consumer rights on a foundation of business disclosures. When those disclosures are clear, consistent, and comprehensible, consumers are better able to exercise their rights. However, due to the complexity of both the CCPA's disclosure requirements and how consumer personal information is used in today's digital economy, businesses face real challenges when balancing fidelity to the CCPA's requirements and their business practices against clarity and comprehensibility for consumers.

The NAI has worked with its member companies to help them achieve that balance for 25 years. Each year, NAI staff reviews, among other things, every member company's privacy notices through the NAI's Privacy Review Program.[2] The NAI's general observations from last year's Privacy Review cycle are documented in the NAI's 2025 Annual Report.[3] That hands-on review work helps the NAI develop a perspective on best practices for consumer-facing disclosures. The recommendations and illustrative examples included in our comments are based in part on the NAI's experience conducting the 2025 Privacy Review cycle.

---

[1] Cal. Priv. Prot. Agency, Invitation for Preliminary Comments: Notices & Disclosures and Employee Data (May 2026), https://cppa.ca.gov/regulations/pdf/notices_disclosures_employee_data.pdf [hereinafter "*CalPrivacy Invitation for Preliminary Comments*"].
[2] *See* NAI's Principles & Self-Regulatory Framework, Appendix A, § 1(a)–(d) (Accountability Requirements for Principle 1 – Transparency), (Mar. 2025), https://www.thenai.org/wp-content/uploads/2025/03/NAI-Framework_March-2025.pdf [hereinafter "*NAI Framework*"]. Member companies are required to undergo an annual review of their transparency disclosures and privacy notices under the NAI Framework.
[3] *See* NAI's 2025 Annual Report, Section III — Privacy Review Program, at 17, https://thenai.org/wp-content/uploads/2026/05/The-NAIs-Annual-Report_2025.pdf [hereinafter "*Annual Report*"].

The NAI believes that today's disclosure environment can be improved, and we hope that in providing these comments we can support regulations that promote disclosures that are both clear, comprehensible, and useful to consumers and easy to implement for businesses.

Below, we list each question posed by CalPrivacy, and provide substantive responses to many of them. In summary, our recommendations are as follows. CalPrivacy should:

1. Issue a voluntary model Notice at Collection as a regulatory safe harbor for the form of the disclosure.
2. Add illustrative examples to the regulations covering disclosure scenarios where the operational gap between principle and disclosure is widest, including (a) categories of third parties in programmatic advertising, (b) retention periods and criteria, and (c) opt-out preference signal display and probabilistic linkage scenarios.
3. Issue an illustrative example on the website / services two-policy disclosure structure common on business-to-business advertising technology websites.
4. Add a nonexclusive regulatory example for notice on interfaces that do not support traditional webpage-based notices, including connected televisions, over-the-top streaming services, and gaming consoles.
5. Clarify in regulation that businesses should not present additional links, referrals, or other disclosures in a manner reasonably likely to confuse or mislead consumers about how to exercise their CCPA rights.
6. Establish a voluntary Alternative Notice Link modeled on the existing Alternative Opt-out Link.
7. Recognize IP-based location estimation as a permissible basis for delivering state-tailored privacy notices at initial notice presentation.
8. Take a risk-based approach on vendor oversight in the employee data context.

II. Notices and Disclosures

Q1. ***When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?***

N/A

Q2. ***What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?***

See our response to Question 3 below, which addresses recurring drafting issues observed across the 2025 Privacy Review cycle and the regulatory tools that may be able to address them.

Q3. ***What challenges do businesses experience when describing information practices in a privacy policy or other disclosures to consumers? How can the regulations address this issue?***

Two structural challenges shape how digital-advertising businesses approach the disclosures the CCPA requires. The first is translating operationally complex practices, including the use of pseudonymous identifiers, data flows involved in cross-context behavioral advertising, and data retention periods that sometimes involves technical elements into: (1) language that is both

technically accurate and accessible to an ordinary consumer; and (2) a format short enough to be useful at the point of collection. The result is wide variance and inconsistent translation of similar practices across notices. This sometimes leads to inefficiency for businesses charged with providing these disclosures, and it may hamper consumer understanding of similar practices across different businesses. Below, the NAI provides recommendations for how CalPrivacy can use regulations to help address these issues.

A. CalPrivacy should issue a voluntary model Notice at Collection that businesses can adopt as a regulatory safe harbor for the form of the disclosure

Among the existing California disclosure obligations, the Notice at Collection is the best-suited candidate for a voluntary model form. Every covered business that collects personal information must provide one at or before each point of collection.[4] The Notice at Collection regulations specify six content elements, and those elements lend themselves to a tabular layout that maps each statutory element to a standardized column.[5]

There is strong precedent for issuing a voluntary model form. Federal regulators have used voluntary model forms with documented results in adjacent privacy contexts. The closest precedent is the Model Privacy Form under the Gramm-Leach-Bliley Act, issued through a joint interagency rulemaking in 2009[6] following formal consumer-comprehension research.[7] The rulemaking record summarizing those studies found that the model form materially outperformed alternative formats on consumer comprehension, the ability to compare practices across institutions, and the ability to make informed choices.[8] However, adoption of the Model Privacy Form is voluntary; a financial institution that uses the model form consistent with the regulators' instructions is in a safe harbor on the form-of-disclosure obligation.[9]

The Notice at Collection presents a similar design opportunity for CalPrivacy. The NAI's 2025 Privacy Review observed variation across different notices at collection with respect to categorization vocabulary, retention formulations, and sale-and-sharing presentation among the businesses we reviewed.[10] To promote normalization of those disclosures, the NAI recommends that CalPrivacy issue a voluntary model Notice at Collection, with safe-harbor treatment for the

[4] Cal. Civ. Code § 1798.100(a); Cal. Code Regs. tit. 11, § 7012(a), (d).
[5] Cal. Code Regs. tit. 11, § 7012(e)(1)–(6).
[6] *Final Model Privacy Form Under the Gramm-Leach-Bliley Act*, 74 Fed. Reg. 62890 (Oct. 1, 2009), https://www.federalregister.gov/documents/2009/12/01/E9-27882/final-model-privacy-form-under-the-gramm-leach-bliley-act (joint adoption by the OCC, the Federal Reserve, the FDIC, the Office of Thrift Supervision, the NCUA, the FTC, the CFTC, and the SEC) [*hereinafter* "*Final Model Privacy Form*"].
[7] Alan Levy & Manoj Hastak, *Consumer Comprehension of Financial Privacy Notices* (2008), https://www.ftc.gov/system/files/documents/reports/quantitative-research-levy-hastak-report/quantitative_research_-_levy-hastak_report.pdf; Kleimann Communication Grp., *Financial Privacy Notice: A Report on Validation Testing Results* (Feb. 12, 2009), https://www.ftc.gov/system/files/documents/reports/financial-privacy-notice-report-validation-testing-results-kleimann-validation-report/financial_privacy_notice_a_report_on_validation_testing_results_kleimann_validation_report.pdf.
[8] *Final Model Privacy Form*, *supra* note 6, at 62894–98.
[9] 17 C.F.R. § 248.2; *Final Model Privacy Form*, *supra* note 6, at 62890.
[10] *Annual Report*, supra note 3, §§ III.a.i–iv, at 20–24.

form and presentation of the notice, conditional on accurate completion of the model fields and on compliance with the CCPA readability standard.[11]

A model form drawn along these lines could be structured substantially as illustrated in Appendix A. Any model form, however, should accommodate a variety of business models, including digital advertising and related services. For example:

- An ad-technology business that processes pseudonymous identifiers. A business that collects information through cookies, mobile advertising IDs, or hashed values rather than direct identifiers can populate the Identifiers row with the operative pseudonymous identifier types and the purposes for which they are used. A sample row for a publisher whose advertising-technology partners process such identifiers is populated in the example form provided in Appendix A.
- A business operating under the third-party-collection rule. Where a first-party publisher allows a third-party ad-tech business to control collection of certain personal information on the publisher's site, both businesses have Notice at Collection obligations, and the regulations permit them to provide a single joint notice describing their collective information practices.[12] Any model form should accommodate this scenario by allowing the publisher to incorporate the relevant practices of third-party businesses into its own notice. In many cases, ad-tech companies have no direct contact with the consumer because the publisher controls the consumer-facing surface entirely. In those scenarios, publisher-delivered Notice at Collection is the only realistic mechanism through which these businesses can satisfy their obligation. CalPrivacy guidance can help reinforce that the publisher's joint notice or equivalent upstream delivery is sufficient. An example illustrating an approach to this type of scenario is provided in Appendix A.

B. CalPrivacy should add illustrative examples in the regulations for digital-advertising disclosure scenarios where the operational gap between principle and disclosure is widest

Beyond the Notice at Collection, the broader privacy-policy disclosure obligations cover a wider range of substantive material that varies across business models. A single model form would likely struggle to capture that breadth. A more apt regulatory tool is the illustrative example, which CalPrivacy already employs extensively in existing regulations. The Notice at Collection regulations already use multiple illustrative examples covering where to make the notice "readily available," how to handle third-party collection, and how to apply the notice in physical-premises contexts.[13] The NAI identifies three candidates from the 2025 Privacy Review where additional illustrative examples would likely help guide businesses in meeting CalPrivacy's expectations and improve efficiency for businesses.

1. Categories of third parties in programmatic advertising anchored to the "meaningful understanding" standard.

The "meaningful understanding" standard for third-party-category disclosures requires within-category granularity that the current regulations do not yet illustrate for the digital-advertising recipient ecosystem. Section 7011(e)(1)(E) requires the privacy policy to describe categories of

[11] Cal. Code Regs. tit. 11, § 7003(a)–(b); *see also id.* § 7012(b).
[12] *Id.* § 7012(g)(1).
[13] *Id.* § 7012(c) (five examples on availability); *id.* § 7012(g)(3) (three examples on third-party collection).

third parties to whom personal information is sold or shared "in a manner that provides consumers a meaningful understanding of the parties to whom the information is sold or shared."[14] The existing definitions in the regulation define "categories of third parties" with generic examples that include "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."[15] What that definitional baseline does not provide, and what the "meaningful understanding" standard does not yet illustrate, is the level of within-category granularity that the digital-advertising recipient ecosystem requires for the standard to be operative for consumers. Within the regulation's broad category of "advertising networks" alone, several functionally distinct types of recipients operate, and publishers, advertisers, and ad-tech companies face choices of how, or whether, to disaggregate them in their privacy policy disclosures. Their choices in this regard may impact consumer understanding, including disclosures that are too general but also too specific, as industry sub-categories or terms of art may not aid consumer understanding or be material to their decisions about whether to exercise their privacy rights. CalPrivacy can help guide companies and enhance consumer understanding by providing illustrative examples using categories of third parties. An illustrative example could read substantially as follows:

> *A publisher that displays advertising sold through programmatic real-time bidding could describe the categories of third parties to whom it sells or shares identifiers and internet-activity information for advertising as follows, where each category applies: (i)* ***Advertising marketplace and ad-delivery providers*** *— companies that operate the platforms used to request, bid on, select, deliver, and report on ads (industry terms: supply-side platforms, demand-side platforms, and ad exchanges); (ii)* ***Identity and matching providers*** *— companies that maintain advertising identifiers and link consumer activity across browsers and devices for advertising-targeting and measurement purposes; (iii)* ***Measurement, analytics, and attribution providers*** *— companies that measure ad delivery, performance, reach, frequency, and attribution; (iv)* ***Ad verification, fraud-prevention, and brand-safety providers*** *— companies that detect invalid traffic, protect against fraud and security threats, and assess whether ads appear in appropriate contexts; and (v)* ***Audience and data providers*** *— companies that provide, receive, or help create audience segments used for targeting or measurement.*

An example like this (or with another level of granularity that CalPrivacy assesses as appropriate) would tell a consumer in plain language what each category of recipient does, while preserving an opportunity to provide more detailed terminology in parentheticals for precision. It would also resolve the design tension between overly generic disclosures (e.g., "our advertising partners") and overly granular disclosures (an enumeration of every counterparty in a real-time bidding flow).

The example provided above represents one approach to striking a balance that maximes consumer comprehension while providing meaningful guidance to businesses. However, a business may still meet the "meaningful understanding" standard through different categorizations that accurately reflect its specific data flows. The same plain-language discipline applies to how businesses describe the purposes for which they collect and use personal information. A purpose described in concrete operational terms (for example, limiting the number of times an ad is shown (frequency capping), ad performance measurement, or geographically

[14] *Id.* § 7011(e)(1)(E).
[15] *Id.* § 7001(g).

relevant advertising) gives the consumer more usable information than a generic formulation such as "business purposes" or "advertising."

2. Retention periods or criteria.

Retention disclosure is a recurring drafting challenge: general formulations like "as long as necessary for the purposes described" may satisfy the CCPA's approach in form but provide limited information for consumer comprehension. The statute and the implementing regulation require businesses to disclose, for each category of personal information, either the period for which the business intends to retain that category or the criteria the business uses to determine that period.[16] An illustrative example would distinguish three retention patterns commonly used in digital-advertising disclosures:

> *A business may disclose retention for each category of personal information using the pattern that fits the underlying data: (i)* ***Identifier expiry or refresh-based retention*** *— for identifiers such as cookies or session tokens that expire or are refreshed by consumer interaction: "Browser cookies are retained for [defined period] from collection or until the cookie expires or is reset by the consumer's next interaction with the business, whichever occurs first." (ii)* ***Relationship-based retention*** *— for information retained while a consumer maintains an active relationship with the business: "Information tied to an active consumer account is retained for the duration of the account plus a defined period thereafter for routine account-closure processing." (iii)* ***Policy-based retention*** *— for information retained under a defined business-purpose schedule: "Information retained for audit, fraud-prevention, dispute-resolution, or legal-compliance purposes is retained for [defined period] from collection consistent with the business's documented retention schedule, after which the data is deleted, aggregated, or de-identified."*

The three patterns are not mutually exclusive (a single business will commonly use all three), but illustrating them separately could help close the gap between general criterion formulations and consumer-operative disclosure.

3. Opt-out preference signal display, and signal-scope clarification in identity-graph linkage scenarios.

The existing regulations covering opt-out preference signals (OOPS) already provide substantial guidance, including five illustrative examples, descriptions for how a business should display whether it has processed the consumer's OOPS, and how a business should treat an OOPS as a valid request to opt-out of sale/sharing for the consumer's "browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles."[17] However, two adjacent disclosure issues on OOPS are not yet illustrated in the regulations, and the NAI's 2025 Privacy Review surfaced both as areas where guidance would help businesses and consumers.

The first is **the placement and persistence of the opt-out display in preference-center environments**: guidance on where the display should appear, how persistent the display must be across navigation and sessions, and whether the display should describe the scope of processing affected by the signal beyond stating "Opt-Out Request Honored." The existing examples illustrate the general fact of display but not other considerations that will help determine whether

[16] Cal. Civ. Code § 1798.100(a)(3); Cal. Code Regs. tit. 11, § 7012(e)(4).
[17] Cal. Code Regs. tit. 11, § 7025(c)(1), (c)(6), (c)(7)(A)–(E); *id.* § 7026(g).

the display is usefully visible to consumers in practice, or what opt-out requests have been honored, or in what way.

The second is **signal scope in identity-graph linkage scenarios**: a business may maintain linkages associating a browser with other browsers, devices, or pseudonymous profiles in the ordinary course of its business, but those associations are made without relying on an account login. This distinction can be critical, as these linkages are *probabilistic*, whereas account logins are *deterministic*, and thus extending an opt out across probabilistic linkages will often yield imprecise results. The existing examples illustrate scenarios in which such association either exists through a logged-in account or does not exist at all; the intermediate case is left for businesses and consumers to navigate without a guiding example.[18] An additional illustrative example in the regulations would help clarify how the opt-out should apply to probabilistically linked browsers or devices, and how the business should describe the scope to the consumer.[19] Any such example should apply only to linkages a business maintains in the ordinary course and should not require businesses to create or expand identity-graph linkages for the purpose of opt-out propagation.

Currently, the regulations also require businesses to explain how an OOPS will be processed, including whether the signal applies to the device, browser, consumer account, and/or offline sales.[20] Similarly, due to the probabilistic (and imprecise) nature of certain linkages, properly describing how an OOPS will be processed in this context invites risk of describing the scope of the opt out in a way that will be unclear to a consumer. As the requirement to properly disclose and explain how an OOPS will be processed for the consumer has been an enforcement priority for CalPrivacy, the intermediate probabilistic linkage example is precisely where that explanation is hardest to operationalize.[21]

C. CalPrivacy should issue an illustrative example on the website privacy policy / services privacy policy structure that is common in business-to-business ad-tech

California-resident visitors to a business-to-business ad-tech provider's marketing website are consumers under the CCPA, regardless of professional capacity. The CCPA defines a "consumer" as "a natural person who is a California resident … however identified, including by any unique

---

[18] Notably, example D addresses how an OOPS should be processed when a consumer is sharing online browsing habits through the use of a pseudonymous cookie. *See id.* § 7025(c)(7)(D). However, this example does not address whether or how the scope of an OOPS should be extended to an identity graph relying on probabilistic linkages between cookie identifiers.

[19] *Cf.* Network Advertising Initiative, *Guidance for NAI Members: Cross-Device Linking* § II.C, at 5 (May 2017), https://thenai.org/wp-content/uploads/2021/07/NAI_Cross_Device_Guidance.pdf [hereinafter *NAI Cross-Device Guidance*]. When a consumer opts out on one browser or device, the *NAI Cross-Device Guidance* suggests preventing personalized advertising from being served on that browser or device; as well as preventing data collected from that browser or device from being used on other browsers or devices for personalized advertising. The NAI's recommendation here is not that opt-out preference signals automatically propagate across all probabilistic linkages, but that the regulations should provide a guiding example for businesses operating in the intermediate scenario. The *NAI Cross-Device Guidance* provides a proven model for how to do so.

[20] *See* Cal. Code Regs. tit. 11, § 7011(e)(3)(F).

[21] CalPrivacy cited this disclosure requirement in *In re Tractor Supply Co.*, Stipulated Final Order ¶ 43 (Cal. Priv. Prot. Agency Sept. 26, 2025), https://cppa.ca.gov/pdf/20250930_tractor_supply_bd_sfo.pdf; *cf. Complaint, People v. Disney DTC, LLC*, No. 26STCV04425 ¶ 15 (Cal. Super. Ct., L.A. Cnty., filed 2026), https://oag.ca.gov/system/files/attachments/press-docs/1%20-%20Complaint%20(Disney).pdf (framing failure to honor opt-out preference signals as a form of deception).

identifier."[22] The former business-to-business exemption, which carved out personal information collected from natural persons acting on behalf of a business in a business-to-business transaction, sunset on January 1, 2023 and is no longer operative.[23] When a covered business collects personal information from a California-resident visitor to its marketing website, the visitor's professional capacity does not exempt the interaction from the CCPA, and the disclosure obligations under the statute and the implementing regulations apply to that collection.

It is common industry practice for business-to-business ad-tech providers to adopt a two-policy structure for marketing-website disclosure: a **website privacy policy** addressed to visitors to the provider's marketing website, and a **services privacy policy** addressed to the end users whose personal information the provider processes through its ad-tech services on other digital properties. The NAI supports this structure because it reflects the fact that the provider operates in two distinct relationships, one with marketing-site visitors and one with end users of the provider's customers' services, each involving different information practices governed by the same CCPA framework.

However, the two-policy structure raises a disclosure-design question that an illustrative example could help resolve. A California-resident visitor to the provider's marketing website is entitled to a comprehensive description of the business's information practices under the privacy-policy regulations. The website privacy policy will ordinarily be the operative disclosure for the consumer's interaction with the marketing website. The services privacy policy describes information practices that may not apply to the marketing-website visitor, but may apply in some scenarios, including where the same provider's advertising technology operates on the marketing website itself. From the consumer's perspective, the question is which policy applies to the marketing-website interaction and how to navigate between them; from the business's perspective, the question is how the two-policy structure satisfies the comprehensive-description requirement for the website-visitor consumer.

The NAI recommends that CalPrivacy issue an illustrative example clarifying how the two-policy structure can give the marketing-website consumer a comprehensible path through the relevant disclosures. An illustrative example could provide that:

> *Business Q is an advertising-technology provider that operates a marketing website for its customers and prospective customers on its own domain; and provides separate services that process personal information in connection with its customers' websites and applications. Business Q maintains two privacy policies: a website privacy policy that applies to the marketing website, and a services privacy policy that applies to Business Q's services as deployed by its customers. On the marketing website, Business Q provides a Notice at Collection at or before the point of collection, including by posting a conspicuous link to the notice on its homepage(s), on webpages where personal information is collected, and in close proximity to webform input fields. The Notice at Collection contains the information required by subsection (e) and includes a link that takes the consumer directly to the relevant section of Business Q's website privacy policy. The website privacy policy describes the information practices applicable to the marketing-website interaction. Where Business Q's services also operate on the marketing website, the website privacy policy either describes those practices*

[22] Cal. Civ. Code § 1798.140(i).
[23] *See id.* § 1798.145(n)(3) ("This subdivision shall become inoperative on January 1, 2023."). Subdivision (n) — the former business-to-business exemption — remains in the statute text but is inoperative by its own terms; the legislature did not extend or replace it.

or provides a conspicuous link that takes the consumer directly to the relevant section of the services privacy policy. This example addresses only Business Q's marketing website and does not determine Business Q's role or notice obligations in any customer's deployment of Business Q's services.

This kind of example would address a recurring drafting question NAI's members have surfaced through the 2025 Privacy Review, while preserving the flexibility for businesses to address two distinct audiences through purpose-appropriate disclosures.

Q4. *What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights? For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?*

The CCPA's notice principles are device-agnostic: disclosures must be easy to read and understandable, and methods for submitting requests and obtaining consent must be easy to understand, symmetric in choice, free of confusing or impairing architecture, and easy to execute.[24] The illustrative examples that accompany those principles, however, address websites, mobile applications, offline forms, telephone, and in-person interactions; the only non-webpage examples in the Notice at Collection regulation concern Wi-Fi captive portals and in-vehicle signage.[25] That leaves real implementation uncertainty on connected televisions ("CTV"), over-the-top ("OTT") streaming services, and gaming consoles. The requirement that a business not operating a website "shall make the privacy policy conspicuously available to consumers"[26] could be clearer as applied to businesses collecting personal information through those platforms.

The NAI recommends that CalPrivacy add a nonexclusive regulatory example confirming that, for interfaces that do not support traditional webpage-based notices, a business may provide notice through a surface-appropriate mechanism (including on-device settings entries, QR codes, short URLs, or paired-application handoffs), provided the mechanism is conspicuous, available at or before the point of collection, routes the consumer directly to the relevant notice or rights mechanism, and complies with the device-agnostic notice principles. The example should not mandate any single user-experience design pattern, should not require long-form notice presentation on constrained interfaces, and should not restrict businesses from offering companion-device handoffs as a primary path where on-surface input mechanisms are cumbersome.

Q5. *What challenges do businesses face when providing notices, including opt-out links, across different devices or platforms? How can the regulations address this issue?*

NAI's substantive positions relevant to this question are developed elsewhere. On cross-device opt-out propagation, including the application of opt-out preference signals to pseudonymous data environments, see NAI's Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals (April 6, 2026).[27] On notice mechanisms for

[24] *See generally* Cal. Code Regs. tit. 11, §§ 7003, 7004.
[25] *See id.* § 7012(c)(1)–(5); *id.* § 7012(g)(3)(B)-(C).
[26] *Id.* § 7011(d).
[27] Network Advertising Initiative, *Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals* (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.

interfaces that do not support traditional webpage-based notices, including CTV, OTT, and gaming surfaces, see our response to Question 4 above.

Q6. Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.

Each year, NAI's Privacy Review program conducts hands-on review of member companies' privacy notices, choice mechanisms, governance programs, and other items. NAI staff test member implementations through direct website testing, in-product submission of access and deletion requests, privacy-inbox testing, and A/B comparison of browser sessions with and without Global Privacy Control enabled. The 2025 review cycle generated cross-ecosystem observations of design choices that function at the moment of consumer interaction.[28] These observations arise in the context of member adherence to the NAI Self-Regulatory Framework, not controlled consumer-comprehension testing.[29]

The effective practices described below are drawn from that review process and include design patterns NAI staff identified as effective because they provide clarity and ease of use.

A. **Surfacing relevant identifiers in context.** Identifiers that ad-tech companies rely on are not always easy for consumers to locate, particularly when they are accessible only through technical device settings. In some cases, effective rights workflows can address this discoverability problem by reading and displaying the relevant identifier in context, or providing clear, device-specific instructions for locating it. One effective implementation NAI staff observed that addressed this issue starts with a template DSR submission form that cannot natively surface the business's pseudonymous identifier. However, the implementer reads the consumer's device ID from the browser using an iframe, and then displays the relevant identifier and prompts the consumer to copy it into the form.
B. **Jurisdiction-tailored rights presentation.** As state privacy laws have proliferated, effective rights-disclosure architectures present the rights, processes, and statutory language applicable to the consumer's state through clearly indexed state-specific sections or dedicated jurisdiction-tailored pages. The alternative (conditional "you may have rights" or "if your state has a data privacy law" phrasing) has been flagged by privacy enforcement authorities in Delaware, Connecticut, and Oregon as inadequate.[30]
C. **Cookie-consent banners reflecting symmetry-in-choice principles.** Where a banner presents an "Accept All" path for advertising-related cookies or tracking, the most effective implementations we observe provide an equally prominent reject affordance, granular per-purpose toggles that are clearly described, a notice on the banner itself that Global Privacy Control has been detected and honored where applicable, and a clear display of the consumer's current consent state. The statutory footer-link approach remains a separate compliant path;[31] these design choices describe one effective implementation using banners as a primary disclosure surface, not a California requirement to replace the footer-link approach. The combination reflects the symmetry-in-choice principle articulated in CalPrivacy's enforcement action in the *Honda* matter: that the path for a consumer to exercise a more privacy-protective option cannot be longer, more difficult, or more time-consuming than the path to exercise a less privacy-

[28] *See Annual Report*, *supra* note 3, §§ III, III.b.i, at 17, 25.
[29] *See NAI Framework*, *supra* note 2.
[30] *See Annual Report*, *supra* note 3, § III.a.ii — Declarative Rights, at 20.
[31] *See generally* Cal. Civ. Code § 1798.135.

protective option.[32] The on-banner GPC notice in particular closes a longstanding consumer-comprehension gap, since consumers using GPC otherwise have no contemporaneous confirmation that their preference signal was received.

D. **Privacy policies with dedicated authorized-agent and appeals sections.** State-by-state fragmentation has produced procedural complexity in two specific areas, authorized-agent intake and (where applicable) consumer appeals, that consumers otherwise must navigate by emailing generic privacy contact addresses. Effective privacy policies surface these procedures directly: a dedicated authorized-agent section setting out who may submit, what documentation is required (and not required) for verification, where to direct the submission, the applicable timeline, and the expected response; and, where applicable, a dedicated appeals section setting out the appeal process and decision points. This pattern converts opaque downstream processes into foreseeable consumer-facing ones, reducing the response-time and effort burdens that otherwise fall on consumers.
E. **Device- and platform-specific opt-out guidance in CTV contexts.** In the CTV context, effective consumer-facing disclosures provide device- and platform-specific opt-out instructions rather than relying on browser-centric privacy language. Such disclosures may appropriately link to supplementary resources, including NAI's device-specific consumer guidance updated in late 2025 to span web browsers, mobile devices, CTV, and streaming devices,[33] where those resources function as a supplement to the business's own statutory choice mechanisms rather than a substitute. CTV consumers otherwise face a notice environment built for browsers, with limited access to choice resources tailored to the device they are using.
F. **Privacy policy navigability**. Effective privacy notices are mindful of the consumer's path through the privacy policy itself, where the 2025 Privacy Review surfaced practical navigability factors that materially affect whether a consumer reaches the disclosure that applies: descriptive section headings, a functioning table of contents, a current "last updated" date, working in-policy hyperlinks, and content organization that does not require the consumer to scroll past extensive content that may be less relevant to reach, *e.g.*, rights and choice mechanisms.

These examples are illustrative rather than exhaustive. NAI's 2025 Privacy Review cycle has surfaced additional implementations across the ecosystem, and the NAI would welcome the opportunity to share further detail at the agency's request.

Q7. ***What else should CalPrivacy consider regarding CCPA notice and disclosure requirements?***

Consumer notice fatigue can arise from too many notices, particularly when they are presented or linked to in the same place. This is a risk when companies present many disclosure links in the website footnote even where each individual disclosure link is compliant. This is challenging because businesses today face a growing array of those obligations: the CCPA, the consumer-privacy laws of many other states, industry opt-out tool referrals, cookie-consent notices, sensitive-data-use disclosures, and state-specific consumer-rights content within the privacy policy itself. The corresponding links and sections often serve similar purposes under different

[32] *In re Am. Honda Motor Co.*, Stipulated Final Order ¶ 60 (Cal. Priv. Prot. Agency Mar. 7, 2025), https://cppa.ca.gov/regulations/pdf/20250307_hmc_order.pdf; *see also* Annual Report, *supra note 3*, § III.b.ii — Symmetry in Choice & Design, at 26.
[33] *See* Network Advertising Initiative, *How to Opt Out*, https://thenai.org/how-to-opt-out/ (last visited May 20, 2026) (providing device-specific opt-out instructions spanning web browsers, mobile devices, and TVs & streaming devices).

headings: "Your Privacy Choices" and "Your Ad Choices"; "Notice at Collection" and "Privacy Notice"; "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information"; California-rights language alongside parallel content for other states. NAI has previously urged CalPrivacy to apply a streamlining principle to overlapping notice architectures in adjacent CalPrivacy rulemaking, including in NAI's 2025 comments on the Automated Decisionmaking Technology (ADMT) regulations;[34] the same principle remains relevant for the notice-architecture concerns considered here.

The NAI offers three recommendations to reduce the risk notice fatigue without weakening any substantive disclosure obligation, each explained in more detail below:

- Clarify that businesses should not present additional links, referrals, or other disclosures likely to mislead or confuse consumers about how to exercise their CCPA rights.
- Establish a voluntary "Alternative Notice Link" modeled on the existing Alternative Opt-out Link, consolidating the Notice at Collection and the privacy-policy access path at the point of collection.
- Recognize IP-based location as a permissible basis for delivering state-tailored privacy notices at initial notice presentation, without prescribing detailed implementation rules.

A. CalPrivacy should clarify that businesses should not present additional links, referrals, or other disclosures likely to mislead or confuse consumers about how to exercise their CCPA rights

The CCPA's prominence requirements for homepage links set a standard for the consumer's initial routing to disclosures at the moment at which the consumer decides which link to click to begin exercising a CCPA right.[35]

However, the prominence of CCPA-required links may be degraded when the homepage footer (or other consumer-facing surface) presents too many additional links, referrals, or disclosures alongside the operative CCPA links in ways that may confuse consumers about which link delivers the CCPA-required functionality. The consumer may select a link that does not deliver the desired

[34] *See* Network Advertising Initiative, *Comments on CCPA Updates* (June 2, 2025), at 2, https://thenai.org/wp-content/uploads/2025/06/NAI-Comment-on-CCPA-Updates-6.2.2025.docx.pdf [hereinafter *NAI ADMT Comments*].
[35] *See* Cal. Civ. Code § 1798.135(a); Cal. Code Regs. tit. 11, § 7011(d); *id.* § 7013(c).

result and walk away believing the right has been exercised when it has not. Recent CalPrivacy and California Attorney General enforcement reflects the risk.[36] [37]

To address this risk, the NAI recommends that CalPrivacy adopt the following standard directly in regulation:

> *A business shall not present additional links, referrals, or other disclosures in a manner reasonably likely to confuse or mislead consumers into believing they have exercised a CCPA right or have been provided with a CCPA-required disclosure when they have not been.*

Adopting this language in regulation would clarify a principle articulated through enforcement and promote a more uniform standard businesses can implement, reducing reliance on case-by-case enforcement to address the same recurring design risk. It would also benefit consumers by requiring businesses to consider whether too many additional links may confuse or mislead consumers.

B. CalPrivacy should establish a voluntary "Alternative Notice Link" modeled on the existing Alternative Opt-out Link

The CCPA already recognizes that closely related disclosure links can be consolidated into a single, clearly-labeled link or mechanism. The existing Alternative Opt-out Link implements this for choice: a business may, in lieu of posting separate Notice of Right to Opt-out and Notice of Right to Limit links, post a single Alternative Opt-out Link titled "Your Privacy Choices" or "Your California Privacy Choices," paired with a standardized icon.[38] The Alternative Opt-out Link is voluntary; adopting businesses gain an approved form of consolidated link presentation, and consumers gain a consistent, recognizable point of entry. CalPrivacy has applied the same consolidation principle in the Automated Decisionmaking Technology ("ADMT") context, accepting that the ADMT pre-use notice may be presented as part of the existing Notice at Collection.[39] The same concept can be applied to the disclosures consumers encounter at the point of collection.

---

[36] *In re 2080 Media, Inc. d/b/a PlayOn Sports*, Stipulated Final Order ¶ 47 (Cal. Priv. Prot. Agency Feb. 27, 2026), https://privacy.ca.gov/wp-content/uploads/sites/357/2026/03/Order-of-Decision_PlayOn_Enforcement.pdf (concluding that a business "failed in its responsibility to provide a method for opting out of the Sale/Sharing of Personal Information by certain Tracking Technologies and instead stated in its privacy policy that Consumers should opt-out directly with third parties via the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA)"). The NAI publicly recognized the principle the *PlayOn* order applies shortly after the order was announced, *see* NAI, *Statement from NAI President & CEO Leigh Freund on the CalPrivacy Settlement with PlayOn Sports* (Mar. 3, 2026), https://thenai.org/press/statement-from-nai-president-ceo-leigh-freund-on-the-calprivacy-settlement-with-playon-sports-decision/. Well before *PlayOn* was announced in September 2025, the NAI had sunset its legacy industry opt-out infrastructure to align its consumer-facing resources with the CCPA's business-level opt-out architecture.

[37] *People v. The Walt Disney Co.*, Final Judgment and Permanent Injunction ¶¶ 26(e), 29 (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 (¶ 29 enjoining "language and choice architecture likely to confuse or deceive CONSUMERS"; ¶ 26(e) requiring opt-out notices not require consumers to "unnecessarily search or scroll through text" or use "hard-to-find-links, unlabeled carets, arrows, or other hidden menu icons").

[38] Cal. Code Regs. tit. 11, § 7015(a)–(b).

[39] *Id.* § 7220(a); *NAI ADMT Comments*, *supra* note 34.

The existing Notice at Collection regulations already permit a business to satisfy the obligation by linking directly to the section of the privacy policy that contains the required content.[40] In practice, businesses using that deep-link approach often still present a second, adjacent privacy-policy link at the same collection interface, because the existing regulations do not address the relationship between using deep-linking to present the notice at collection and the general privacy-policy accessibility requirement.[41] The result in those cases is a consumer being presented with two links to reach the same disclosure: the same structural concern the Alternative Opt-out Link already addresses on the choice side.

To address this issue, the NAI recommends that CalPrivacy establish a voluntary Alternative Notice Link, modeled on the existing Alternative Opt-out Link, as follows:

> *A business may, in lieu of posting separate links to a Notice at Collection and to the business's privacy policy, post a single, clearlylabeled link that directs the consumer to the section of the business's privacy policy containing the required Notice at Collection content. The linked section must include a conspicuous same-page control, persistent navigation element, or immediately adjacent link allowing the consumer to access the full privacy policy. The single link shall use a standardized title (for example, "Notice at Collection & Privacy Policy") and may be paired with a standardized icon, in a form CalPrivacy may specify. Where a business uses the Alternative Notice Link consistent with this section, no separate general privacy-policy link is required.*

The recommendation does not reduce the substantive content of CCPA disclosures; the required Notice at Collection content elements all remain. It addresses only the link architecture by which the consumer reaches those elements.

C. CalPrivacy should recognize IP-based location for delivering state-tailored privacy notices at initial notice presentation

State-tailored notice presentation can streamline a consumer's path to the operative rights without changing the substantive disclosures. In many cases, privacy policies have grown into long, structurally complex documents that combine general descriptions of a business's information practices with discrete sections tailored to the California consumer-privacy regime and, increasingly, to those of other states. A consumer reaching the policy through a single conspicuous link encounters substantial content that may not apply to the consumer's actual state of residence, lengthening the document and increasing the cognitive load of identifying the operative rights. Some businesses, in response, deliver state-tailored privacy notices keyed to the state associated with the consumer's current connection, a positive streamlining response to a real consumer burden observed across the NAI's 2025 Privacy Review.

However, state-tailored delivery or privacy disclosures requires a workable way to estimate the state associated with the consumer's current location. One practical mechanism is reference to the state associated with the site visitor's current IP address. While imperfect, use of IP address to estimate general location is an accepted industry practice, and has also been recognized as a valid approach in some circumstances by Minnesota. Minnesota's Consumer Data Privacy Act provides

[40] Cal. Code Regs. tit. 11, § 7012(f).
[41] *See id.* § 7011(d).

that "use of an Internet protocol address to estimate the consumer's location is sufficient to determine the consumer's residence."[42]

The NAI recommends that CalPrivacy establish a presumption (or a comparable form of recognition) that a business may use IP-based location estimation to estimate the state associated with the consumer's current connection for the purpose of selecting which state-tailored privacy notice to present at initial notice presentation. This presumption should anticipate and account for businesses accommodating consumers whose IP location does not correspond to their actual state of residence (for example, VPN users or consumers traveling), so long as those businesses make routing to other state disclosures available to the consumer as needed.

III. Employee Data

Scoping note: The NAI's Privacy Review Program focuses on consumer-facing practices in the digital advertising ecosystem. The NAI does not review member companies' HR practices. The NAI provides a response to Q6 (service-provider and contractor oversight) below because that question has broader applicability and draws directly on NAI's adtech-vendor-oversight experience.

Q1. ***Expectations or concerns about why businesses collect, use, disclose, or retain personal information as a job applicant or employee?***

N/A

Q2. ***Have you received a copy of a business's privacy policy, Notice at Collection, or CCPA rights' notices as a job applicant or employee?***

N/A

Q3. ***What challenges do businesses experience when providing a privacy policy, Notice at Collection, or CCPA rights' notices to job applicants and employees?***

N/A

Q4. ***Have you exercised your CCPA rights as a job applicant or employee?***

N/A

Q5. ***What challenges do businesses experience when providing job applicants and employees with the ability to exercise their privacy rights?***

N/A

Q6. ***What steps do businesses take to oversee their service providers' and contractors' CCPA compliance, and what challenges do businesses face when doing so? For example, do businesses conduct audits of these entities or test the service provider's or contractor's systems? How effective are these audits and tests to assess a service provider's or contractor's CCPA compliance?***

NAI's Privacy Review program does not examine member companies' HR practices, and we leave most of this question to commenters with HR-vendor administration expertise. We offer two observations.

[42] Minn. Stat. § 325M.14, subd. 3(a)(5) (2025).

A. **Vendor oversight under the CCPA is risk-based by design.**

The CCPA service-provider regulation requires the contract to grant the business the right to take "reasonable and appropriate steps" to ensure CCPA-consistent use of personal information, and identifies a permissive, non-exhaustive menu (manual reviews, automated scans, internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months) among the steps those rights "may include."[43] What is reasonable and appropriate depends on the sensitivity of the data, the processing role, the controls already in place at the vendor, and the scalability of testing across different kinds of vendors.

B. **The employee-data context is particularly sensitive and is not representative.**

Employee-data processing implicates workplace power asymmetries and decisions affecting employment opportunities, compensation, benefits, discipline, and termination. Vendor-oversight calibration appropriate to that context may not reflect what "reasonable and appropriate" oversight requires across other CCPA contexts, including the ad-tech ecosystem, where processing roles, data sensitivity, contractual controls, and technical access points differ materially.

The NAI encourages CalPrivacy to consider these distinctions when considering regulations applicable to the employee data context and address vendor-oversight standards of general application separately.

Q7. What else should CalPrivacy consider regarding CCPA requirements for job applicants and workers in the employment lifecycle?

N/A

IV. Conclusion

The NAI appreciates the opportunity to engage with CalPrivacy on these questions. Our recommendations are offered in service of notices and disclosures that are clear, comprehensible, and useful to consumers, supported by clear and reasonable expectations of businesses delivered through regulation, model notices, and examples in the regulations. The NAI stands ready to provide additional information and to continue engaging with CalPrivacy on the regulatory landscape under the CCPA.

Respectfully submitted,

Tony Ficarrotta

Vice President, General Counsel

The NAI

tony@networkadvertising.org

[43] Cal. Code Regs. tit. 11, § 7051(a)(6).

Appendix A: Sample Form Notice at Collection*

NOTICE AT COLLECTION · CALIFORNIA CONSUMER PRIVACY ACT

Notice at Collection of Personal Information

[Business Name] · Effective [date] · 11 Cal. Code Regs. § 7012

California law requires us to tell you, **at or before we collect your personal information**, what we collect, why, whether we sell or share it, and how long we keep it. The table below covers each category of personal information we collect about California consumers.

§ 7012(G) This notice describes collection by **[Business Name]** and, where applicable, by third parties that control collection on this site or app. Where provided jointly with another business, it describes their collective practices.

Look across each row to see what we collect, why we use it, whether we sell or share it, and how long we keep it.

Categories of Personal Information *types we collect about you* § 7012(e)(1)	**Purposes of Use** *why we collect & how we use it* § 7012(e)(2)	**Do we sell this category?** *for money or other valuable consideration* § 7012(e)(3)	**Do we share this category for cross-context behavioral advertising?** *shared for ads*	**Retention** *how long we keep it* § 7012(e)(4)
Identifiers Browser cookies; mobile advertising IDs (IDFA / AAID); hashed user identifiers.	• Ad delivery • Performance measurement • Cross-context behavioral advertising • Fraud prevention & security • Legal compliance	[Yes / No]	[Yes / No]	**Cookies:** [period] or until reset by consumer **IDFA/AAID:** [period] or until reset by consumer **Hashed IDs:** [period] from collection
Internet or other electronic network activity URLs visited; ad interactions; device signals.	• [Purposes specific to this category]	[Yes / No]	[Yes / No]	[Period or criteria]
Sensitive personal information *(if collected)* List each SPI category collected — e.g., precise geolocation; account log-in credentials; contents of communications; government identifiers; racial or ethnic origin; health information; biometric information.	• [Business's actual purposes for collecting and using this SPI]	[Yes / No]	[Yes / No]	[Period or criteria]

Your choices under the CCPA		
Opt out of sale and sharing § 1798.120 / § 1798.135	*Include if any category is sold or shared*	[Link to Notice of Right to Opt-Out]
Limit use of sensitive personal information § 7027 Applies only when our purposes for SPI go beyond those permitted by § 7027(m).	*Include if SPI is used or disclosed beyond § 7027(m)*	[Link to Notice of Right to Limit]
Read our full privacy policy § 7011	Always include	[Link to Privacy Policy]
Questions? Contact us at [email] or [postal address].		

[Business Name] Notice at Collection 11 Cal. Code Regs. § 7012(e), (g) Page 1 of 1

* Produced with assistance from generative AI tools.