# NAI Comments in Response to CalPrivacy Invitation for Preliminary Comments: Reducing Friction & Opt-Out Preference Signals

April 6, 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 – Reducing Friction in the Exercise of Privacy Rights & Opt-Out Preference Signals

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 Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals ("OOPS").[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. In March 2025, the NAI published its updated Self-Regulatory Framework, which establishes comprehensive privacy and data governance standards that NAI member companies commit to uphold.[2]

The NAI appreciates CalPrivacy's decision to seek stakeholder input before initiating formal rulemaking on these important topics, and always welcomes the opportunity to engage in the rulemaking process. Last year, we wrote to CalPrivacy to express our support for prioritizing rulemaking on OOPS and to offer recommendations for what those regulations should address.[3]

Below, we build on those recommendations in this preliminary comment period.

[1] 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 [*hereinafter* "CalPrivacy Invitation for Preliminary Comments"].

[2] *See* Network Advertising Initiative, *NAI Self-Regulatory Framework* (Mar. 2025), https://www.thenai.org/wp-content/uploads/2025/03/NAI-Framework_March-2025.pdf.

[3] NAI Letter to CalPrivacy RE: Development of Opt-Out Preference Signal Regulations (Nov. 20, 2025), https://thenai.org/the-nai-sends-letter-to-calprivacy-supporting-new-regulations-under-ccpa/.

## Introduction

The California Consumer Privacy Act (CCPA)[4] balances protecting consumer privacy with promoting California's data- and technology-driven economy. It does so by embracing an opt-out model for consumer privacy rights, which empowers consumers to limit how businesses use their personal information without stifling innovation. In line with this key feature of the CCPA, we are encouraged by statements from CalPrivacy's staff recognizing the need for a balance between strong consumer protections with practical, operationalizable requirements for businesses, and by the agency's openness to stakeholder input as it considers new regulations on opt-out preference signals.[5] Those statements align with the NAI's position that the strongest privacy frameworks are ones that businesses can implement effectively, with clarity, and at scale. However, the CCPA's opt-out approach only succeeds if the mechanisms available for consumers to exercise their opt-out rights are easy-to-use and effective.

The NAI has championed a similarly balanced approach for over 25 years through voluntary self-regulation that promotes strong consumer privacy standards while working to keep the ad-supported internet accessible to consumers and viable for businesses of all sizes. But the landscape is changing rapidly. After the passage of the Opt Me Out Act (AB 566) web browsers will be required to provide native support for opt-out preference signals beginning January 1, 2027.[6] Further, the Delete Request and Opt-Out Platform ("DROP") is now available for California consumers to submit deletion requests to registered data brokers.[7] And following California's lead, eleven additional states have enacted laws supporting consumers' exercise of their opt-out rights using opt-out preference signals or similar mechanisms.[8] The question is no longer whether scalable consumer choice tools will be part of the privacy landscape. It is whether they can be implemented effectively, consistently, and in a way that reflects genuine consumer requests to opt out.

The NAI believes they can be. That is why we proactively sunset our legacy third-party opt-out tools in 2025 and launched a Global Privacy Control ("GPC") browser extension designed to conform with the legal requirements for valid opt-out preference signals across multiple states.[9] This decision reflects the NAI's conviction that opt-out preference signals recognized by law are the future of scalable consumer choice online.

Further, while the NAI recognizes the important role that enforcement plays in effectuating compliance with the CCPA's opt-out requirements, we also believe regulation is the proper venue for providing detailed implementation guidance for businesses to address the challenges

---

[4] Cal. Civ. Code § 1798.100 *et seq*.
[5] *See, e.g.*, Remarks of Executive Director Tom Kemp, The Monopoly Report Podcast (Jan. 2026), https://youtu.be/YBc5itessTE; Remarks of Executive Director Tom Kemp, Privado Bridge Summit Keynote (2026), https://youtu.be/uPRCiShe5UQ.
[6] Opt Me Out Act, Assemb. B. 566, 2025–2026 Reg. Sess. (Cal. 2025) (codified at Cal. Civ. Code § 1798.136) [*hereinafter* "Opt Me Out Act"].
[7] Cal. Priv. Prot. Agency, Delete Request and Opt-Out Platform (DROP), https://privacy.ca.gov/drop/ (last visited Apr. 6, 2026).
[8] *See* Colo. Rev. Stat. § 6-1-1306(1)(a)(IV); Conn. Gen. Stat. § 42-520(e)(1)(A)(ii); Del. Code Ann. tit. 6, § 12D-106(e)(1)(a)(2); Md. Code Ann., Com. Law § 14-4707(f)(3)(ii); Minn. Stat. § 325M.14, subd. 3; Mont. Code Ann. § 30-14-2809(3)(b); Neb. Rev. Stat. § 87-1111(5); N.H. Rev. Stat. Ann. § 507-H:6(V)(a)(1)(B); N.J. Stat. Ann. § 56:8-166.11(8)(b); Or. Rev. Stat. § 646A.578(5)(c); Tex. Bus. & Com. Code § 541.055(e).
[9] *See* Network Advertising Initiative, *The NAI Releases New Global Privacy Control Chrome Browser Extension to Facilitate Consumer Opt-Out Requests* (2025), https://thenai.org/the-nai-releases-new-gpc-browser-extension/.

they face when operationalizing consumers' opt-out choices. Regulatory clarity promotes uniform compliance more effectively than interpretation of enforcement actions can.

Our comments below are organized in two parts, following the structure of CalPrivacy's invitation for comments:

- In Part I, we address challenges businesses face in facilitating the exercise of consumer privacy rights, including recommendations to:
    - Enhance authorized-agent transparency and consistently apply the CCPA's data minimization requirements to authorized agents in order to protect consumers and reduce friction for businesses;
    - Develop safe harbors based on recommended standard consumer-facing disclosures and forms, rather than developing a one-size-fits-all model requirement for businesses; and
    - Coordinate with other states to promote consistent, uniform compliance.
- In Part II, we address challenges in the processing and scope of OOPS, including recommendations to:
    - Close the gap between the CCPA's statutory directives and the existing implementing regulations by requiring that opt-out preference signal implementations reflect affirmative consumer choice and prohibit default-on settings that presuppose consumer intent;
    - Clarify the provenance and scope requirements for valid OOPS;
    - Clarify how OOPS apply to pseudonymous profiles and across devices.

We focus these preliminary comments on the areas where regulatory guidance is most needed and look forward to addressing additional topics during the formal rulemaking process.

# PART I: REDUCING FRICTION IN THE EXERCISE OF PRIVACY RIGHTS

## A. Challenges Businesses Experience in Responding to Consumer Rights Requests

The CCPA's consumer choice framework depends on effective mechanisms for consumers to exercise their rights. When those mechanisms work well, consumers can easily opt out of certain processing, request deletion of their data, and otherwise limit how businesses use personal information about them. Authorized agents are one such mechanism: the CCPA allows consumers to designate an agent to act on their behalf in exercising privacy rights, including through opt-out preference signals.[10] Ideally, authorized agent services would reduce friction for consumers and businesses alike. In practice, however, some authorized agent service providers are creating friction in their attempts to exercise rights on behalf of consumers.

The NAI has observed these issues through our members' experience receiving authorized agent requests.[11] Other state regulators have noted similar concerns. Oregon's Department of Justice, in its first-year enforcement report on the Oregon Consumer Privacy Act ("OCPA"), flagged that authorized agents are overpromising rights they are not empowered to exercise under Oregon law and cautioned that agents "should be careful in how they represent their services to consumers, and particularly should avoid using misleading language to engage consumers in subscription models."[12] CalPrivacy has an opportunity to address these problems proactively through rulemaking, and the NAI urges the Agency to do so.

### 1. Authorized agents should not share more consumer personal information with businesses than is needed to facilitate a consumer rights request

When businesses process consumer privacy requests under the CCPA, they are expected to collect only the minimum personal information necessary to verify the consumer and process the request.[13] The same standard should apply to authorized agents submitting those requests on a consumer's behalf. This is important to address now because the volume of authorized agent requests is only expected to grow.[14]

Some authorized agents include far more personal information in their requests than the receiving business needs, or could even use, to fulfill those requests. Some agents include the consumer's full name, physical address, dates of birth, and even sensitive personal information such as photographs of government-issued identification, regardless of whether the receiving business possesses or can match that information to the identifiers in its systems. But many advertising technology companies process only pseudonymous identifiers such as device IDs, cookie IDs, or hashed values. As such, agents in those circumstances are sending excessive consumer personal information to those ad-tech companies that they cannot use to facilitate a

[10] *See* Cal. Civ. Code §§ 1798.135(e); 1798.140(ak).
[11] *See* Tony Ficarrotta, *Some Authorized Agent Providers Are Selling Privacy Snake Oil and Why It Needs to Stop*, IAPP (Feb. 13, 2025), https://iapp.org/news/a/some-authorized-agent-providers-are-selling-privacy-snake-oil-and-why-it-needs-to-stop.
[12] Or. Dep't of Justice, *Enforcement Report: The Oregon Consumer Privacy Act, The First Year*, at 6 (Aug. 2025), https://www.doj.state.or.us/wp-content/uploads/2025/08/OCPA-One-Year-Enforcement-Report-2025.pdf.
[13] *See generally* Cal. Priv. Prot. Agency, Enforcement Advisory No. 2024-01, Applying Data Minimization to Consumer Requests (Apr. 2, 2024), https://cppa.ca.gov/pdf/enfadvisory202401.pdf.
[14] *See generally* Kate Dedenbach & Mark Gravador, *2026 Will Be the Year of the Authorized Agent*, Fisher Phillips (2026), https://www.fisherphillips.com/en/insights/insights/2026-will-be-the-year-of-the-authorized-agent.

consumer rights request, and that they would not otherwise collect. The result is increased friction for many businesses and unnecessary privacy risks for the consumers the agent is supposed to be helping.

The CCPA regulations already require authorized agents to implement and maintain reasonable security procedures and include certain purpose limitations on how agents use consumer personal information.[15] But the regulations do not specifically address the volume and scope of personal information agents include in their requests.

**To address this gap, the NAI recommends that CalPrivacy promulgate regulations requiring authorized agents to limit the personal information they include in requests to what is reasonably necessary to enable the receiving business to identify the consumer and fulfill the request.**

This change would be consistent with CalPrivacy's approach to data minimization in the context of processing consumer requests,[16] as well as the data minimization requirements CalPrivacy holds itself to for the DROP.[17] Aligning the practices of authorized agents with established data minimization standards in other contexts would help reduce friction for businesses responding to those requests while promoting the privacy of consumers for whom agents are submitting requests.

2. **Authorized agents should be transparent with consumers about the scope and effect of their services, including which businesses will receive consumer information**

Consumers who designate an authorized agent are often paying for a service they expect will effectively and safely exercise their privacy rights. But consumers may lack critical information about what the agent is actually doing on their behalf—including which businesses are being contacted, what information is being shared, and whether the requests being submitted are ones the agent is legally empowered to make.

The Oregon Department of Justice's experience illustrates the risk of agents acting outside of, or at least overstating, their legal scope. Under Oregon law, authorized agents are empowered to submit opt-out requests, but not deletion requests.[18] Oregon has accordingly warned that some paid authorized-agent services may be overstating what they can deliver, particularly by suggesting they can exercise deletion rights the law does not empower them to make.[19] While California supports a broader set of authorized agent rights, the underlying concern remains: consumers must not be misled about what an agent can and will do on their behalf.

This transparency becomes critical when an agent submits requests to hundreds of businesses on a consumer's behalf. Under California law, the agency relationship is fiduciary, and an agent is charged with the "duty of fullest disclosure of all material facts concerning the transaction that

[15] *See* Cal. Code Regs. tit. 11, § 7063.
[16] *See* Cal. Priv. Prot. Agency, Enforcement Advisory No. 2024-01, Applying Data Minimization to Consumer Requests (Apr. 2, 2024), https://cppa.ca.gov/pdf/enfadvisory202401.pdf.
[17] *See* Cal. Code Regs. tit. 11, §§ 7610(a)(3)(A)–(B) (requiring data brokers to select only consumer deletion lists containing identifiers that match to personal information in the broker's records); 7616(a) (prohibiting data brokers from using consumer personal information received through the DROP for any purpose other than compliance).
[18] *See* Or. Rev. Stat. § 646A.576(4).
[19] *See* Or. Dep't of Justice, *supra* note 12, at 6–7.

might affect the principal's decision."[20] Which businesses an agent will submit requests to bears directly on both the scope of authority the consumer is conferring and the practical consequences of the agent's actions. This is especially true for deletion requests, which may have permanent and irreversible effects: deleting an account or associated data may terminate access to a service, erase purchase history, extinguish loyalty benefits, or stop requested communications. Because those consequences depend on **which businesses** receive the request, the identity of those businesses is material to the consumer's decision whether, and how broadly, to authorize the agent to proceed.

California regulators have already recognized, in an adjacent context, the importance of transparency and control tied to deletion requests. Under the DROP, consumers can view the list of active registered data brokers implicated by the request and can exclude particular brokers before submission. That framework does not directly govern private authorized agents, but it reflects a sound policy judgment: where a deletion request may have significant consequences, consumers are better served when they can see which businesses are implicated and make selective choices rather than *only* be able to send blind, blanket requests.

**The NAI recommends that CalPrivacy address authorized-agent transparency through rulemaking in two ways:**

- **First, regulations should require authorized agents to clearly identify to the consumer, before any requests are sent, the businesses to which they will submit requests, so that the consumer can define the agent's scope of authority with meaningful specificity.**
- **Second, regulations should require agents to accurately and not misleadingly represent which rights they are empowered to exercise, and the practical limits on those rights, under applicable California law, preventing agents from overpromising the scope or effectiveness of their services.**

3. **CalPrivacy should clarify that correction requests may be treated as deletion requests where correction cannot be meaningfully effectuated.**

The CCPA provides consumers with a right to request correction of inaccurate personal information.[21] For businesses that collect and process data through automated means (including many advertising technology companies that process only pseudonymous identifiers) "correction" of a data point may not be meaningful in the way the statute envisions. A business cannot "correct" a cookie ID, a hashed device identifier, or an inferred interest category in the same way that a retailer can correct a misspelled name or an outdated mailing address. In many cases, the only practical response to a correction request for this type of data is to delete it.

To address this, CalPrivacy should clarify in its regulations that where a business processes personal information collected through automated means and correction cannot be technically effectuated in a meaningful way, the business may satisfy a correction request by deleting the challenged data. This approach serves the consumer's underlying interests by ensuring that inaccurate data is not used through an effective remedy of deletion; while reducing friction for businesses that receive correction requests they cannot act on except to delete.

[20] *Batson v. Strehlow*, 68 Cal. 2d 662, 675 (1968). *Batson* did not arise in the privacy context, but its principle supports treating the identity of the businesses an agent intends to contact as a material fact.
[21] Cal. Civ. Code § 1798.106.

## B. Standardization and Uniformity

CalPrivacy asks whether a lack of standardization or uniformity in how businesses handle consumers' privacy-rights requests is a challenge, and how the Agency should address it. The NAI recommends that CalPrivacy address this through safe harbors rather than mandates.

Prescriptive, one-size-fits-all requirements for how businesses communicate privacy choices to consumers or accept their consumer rights requests can be counterproductive. When consumers encounter rigid, identical disclosures across different contexts, the result is often notice fatigue rather than comprehension. Businesses need flexibility to provide layered, context-appropriate information that meets consumers where they are. In addition, overly-prescriptive regulations often stifle innovation by locking businesses and consumers into outdated standards that fail to account for future technological breakthroughs. Safe harbors solve both problems: they give businesses confidence that their approach will satisfy regulatory expectations while leaving room to tailor disclosures to the contexts in which they operate; and they encourage innovative advances in technology that improve privacy mechanisms for consumers.

The "Your Privacy Choices" link is a case study in how this kind of approach can work. CalPrivacy established a standardized link icon that businesses could adopt as an alternative to posting separate opt-out and limit-use links.[22] Many companies adopted it voluntarily because doing so gave them confidence that their approach would satisfy regulatory expectations. The result was rapid, organic standardization that benefits consumers (who see a consistent label across websites and apps) and businesses (who gain compliance certainty) without requiring a one-size-fits-all mandate.

**The NAI recommends that CalPrivacy develop similar safe harbor approaches in two areas relevant to this rulemaking.**

1. **Model forms must account for pseudonymous data to avoid forcing unnecessary data collection.**

Businesses and consumers alike would benefit from voluntary model forms that establish a safe harbor for CCPA compliance. However, a one-size-fits-all model form that does not account for pseudonymous personal information is unlikely to gain broad adoption in practice.

While consumer-facing brands process direct identifiers like names and emails, some advertising technology companies primarily process pseudonymous personal information, such as device IDs, cookie IDs, or hashed values. If regulators issue a single, traditional model form that requires, for example, a name and email address only, businesses that rely on pseudonymous personal information will be unable to use it.

To ensure these forms are usable across the digital ecosystem, the NAI recommends that CalPrivacy develop distinct model forms specifically designed for pseudonymous environments. These specialized forms should allow consumers to submit the specific identifiers needed to effectuate the request (*e.g.*, a MAID) without requiring the submission of unhelpful, off-device identifiers. The DROP already provides a model for how to do this.[23] As with all model forms, their use should remain voluntary.

---

[22] *See* Cal. Code Regs. tit. 11, § 7015.

[23] *See* Cal. Priv. Prot. Agency, Delete Request and Opt-Out Platform: Unique Identifiers, https://privacy.ca.gov/drop/unique-identifiers/ (last visited Apr. 6, 2026) (explaining mobile advertising IDs; consumer may also submit mobile advertising IDs through a specific field provided in the DROP registration flow).

### 2. Safe harbor language for communicating how the business processes opt-out preference signals.

The existing regulations already require businesses to communicate to consumers how they process opt-out preference signals. Businesses are required to display on their website whether they have processed a consumer's opt-out preference signal as a valid request to opt out of sale and sharing and provide an example display stating "Opt-Out Request Honored."[24] Separately, businesses that process opt-out preference signals in a frictionless manner must include in their privacy policy a description of the consumer's right to opt out, a statement that the business processes opt-out preference signals, information on how consumers can implement such signals, and instructions for other available opt-out methods.[25]

These requirements tell businesses what to communicate but not how. As a result, the messaging consumers encounter may vary widely from business to business, such as different language describing what rights are honored, different levels of detail, and different placement. CalPrivacy could significantly reduce this inconsistency by developing safe harbor language for each of these disclosures. Businesses that adopt the safe harbor messaging would have confidence that their disclosures meet regulatory expectations. Consumers would encounter more consistent and comprehensible descriptions of how their choices are being honored. As opt-out preference signal adoption accelerates under the Opt Me Out Act (which will require major browsers to include native OOPS functionality beginning January 1, 2027),[26] this kind of clarity will become increasingly important.

## C. What Else CalPrivacy Should Consider

The NAI is pleased to offer additional comments in response to CalPrivacy's invitation to identify other areas that could reduce friction in consumers' exercise of their privacy rights.

### 1. The Fragmented Choice Ecosystem

The consumer choice ecosystem today includes multiple, overlapping opt-out methods: opt-out preference signals like Global Privacy Control ("GPC"),[27] legacy industry opt-out tools, consent management platform interfaces, and businesses' own direct opt-out mechanisms. This fragmentation is itself a source of friction for consumers. Consumers may not understand the relationship between these tools, may not know which ones are effective vehicles for exercising their legal rights as distinct from self-regulatory opt-out programs, and may assume that using one tool has resulted in exercising their California privacy rights across the board when it has not.

A recent enforcement action taken by CalPrivacy underscores this problem. In its settlement with PlayOn Sports, CalPrivacy concluded that a business's reliance on links to third-party opt-out tools in lieu of offering its own compliant opt-out mechanism did not satisfy the CCPA's requirements.[28] In anticipation of challenges like this, the NAI transitioned its self-regulatory

[24] Cal. Code Regs. tit. 11 § 7025(c)(6).
[25] *Id.* § 7025(g)(2).
[26] Opt Me Out Act, *supra* note 6.
[27] Global Privacy Control Specification, W3C Working Draft, https://w3c.github.io/gpc/.
[28] *See* In re 2080 Media, Inc. d/b/a PlayOn Sports, Stipulated Final Order, Cal. Priv. Prot. Agency (adopted Feb. 27, 2026; announced Mar. 3, 2026) ($1.1 million fine), https://privacy.ca.gov/wp-

program and consumer choice tools to align with new legal requirements. In 2025, the NAI sunset its legacy third-party opt-out tools substantially to avoid this problem. At that time the NAI began promoting use of GPC signals, including by developing and releasing to the public GPC browser extension for Chrome designed to meet the legal requirements for valid opt-out preference signals.[29]

Opt-out preference signals that meet the requirements of the CCPA and comparable state laws represent a promising path forward for scalable, legally compliant consumer choice. CalPrivacy should consider how its regulations can be amended to provide greater clarity to businesses regarding what types of third-party opt-out tools can be used to comply with requirements for providing consumer opt-out choices at scale.

### 2. Cross-State Interoperability

CalPrivacy's regulations on OOPS should be developed with an eye toward alignment with the requirements in other states, particularly around default settings, verification, and technical specifications. There is a high degree of statutory convergence across states on the key requirements for valid opt-out preference signals and universal opt-out mechanisms. Beyond California, all eleven other states that have enacted laws addressing these signals require that the manufacturer of a platform, browser, or device providing such a signal cannot unfairly disadvantage another business.[30] Similarly, all eleven require that the signal reflect affirmative, freely given consumer choice and not use default settings that presuppose the consumer's choice.[31] And all eleven speak to consistency and interaction with other states' requirements.[32]

California's absence from the consistency requirement is notable. CalPrivacy has an opportunity to lead on this issue by developing regulations that are compatible with the approaches taken by other states, particularly on requirements around default settings, signal provenance, and verification.

---

content/uploads/sites/357/2026/03/Order-of-Decision_PlayOn_Enforcement.pdf. The NAI also issued a statement recognizing this important distinction. Network Advertising Initiative, 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/.

[29] *See* Network Advertising Initiative, *The NAI Releases New Global Privacy Control Chrome Browser Extension* (2025), https://thenai.org/the-nai-releases-new-gpc-browser-extension/; Network Advertising Initiative, *The NAI Releases New Consumer Resources for Online Privacy, Sunsets Legacy Opt-Out Tools* (2025), https://thenai.org/the-nai-releases-new-consumer-resources-for-online-privacy-sunsets-legacy-opt-out-tools/.

[30] *See* Colo. Rev. Stat. § 6-1-1313(2)(a); Conn. Gen. Stat. § 42-520(e)(1)(A)(ii)(I); Del. Code Ann. tit. 6, § 12D-106(e)(1)(a)(2)(A); Md. Code Ann., Com. Law § 14-4707(f)(5)(i); Minn. Stat. § 325M.14, subd. 3(a)(1); Mont. Code Ann. § 30-14-2809(3)(b)(i); Neb. Rev. Stat. § 87-1111(6)(a); N.H. Rev. Stat. Ann. § 507-H:6(V)(a)(1)(B)(i); N.J. Stat. Ann. § 56:8-166.11(8)(b)(2)(a); Or. Rev. Stat. § 646A.578(5)(c)(A); Tex. Bus. & Com. Code § 541.055(f)(1).

[31] *See* Colo. Rev. Stat. § 6-1-1313(2)(c); Conn. Gen. Stat. § 42-520(e)(1)(A)(ii)(II); Del. Code Ann. tit. 6, § 12D-106(e)(1)(a)(2)(B); Md. Code Ann., Com. Law §§ 14-4707(f)(4)(v), (f)(5)(ii); Minn. Stat. § 325M.14, subd. 3(a)(2); Mont. Code Ann. § 30-14-2809(3)(b)(ii); Neb. Rev. Stat. § 87-1111(6)(b); N.H. Rev. Stat. Ann. § 507-H:6(V)(a)(1)(B)(ii); N.J. Stat. Ann. § 56:8-166.11(8)(b)(2)(b); Or. Rev. Stat. § 646A.578(5)(c)(B); Tex. Bus. & Com. Code § 541.055(f)(2).

[32] *See* Colo. Rev. Stat. § 6-1-1313(2)(e); Conn. Gen. Stat. § 42-520(e)(1)(A)(ii)(IV); Del. Code Ann. tit. 6, § 12D-106(e)(1)(a)(2)(D); Md. Code Ann., Com. Law § 14-4707(f)(4)(iii); Minn. Stat. § 325M.14, subd. 3(a)(4); Mont. Code Ann. § 30-14-2809(3)(b)(iv); Neb. Rev. Stat. § 87-1111(5)(d); N.H. Rev. Stat. Ann. § 507-H:6(V)(a)(1)(B)(iv); N.J. Stat. Ann. § 56:8-166.11(8)(b)(2)(d); Or. Rev. Stat. § 646A.578(5)(c)(D); Tex. Bus. & Com. Code § 541.055(e)(4).

# PART II: OPT-OUT PREFERENCE SIGNALS

## A. Challenges Businesses Face in Processing Opt-Out Preference Signals

CalPrivacy asks what challenges businesses face in processing opt-out preference signals like GPC, and how businesses are applying the signal to known consumers, pseudonymous profiles, and across different browsers, devices, or identifiers.[33]

### 1. CalPrivacy should provide regulatory clarity on the application of opt-out preference signals to pseudonymous profiles and across devices.

The existing CCPA regulations establish that when a business receives an OOPS, it must treat the signal as a valid opt-out request for the browser or device on which it is detected, and for "any consumer profile associated with that browser or device, including pseudonymous profiles."[34] If the consumer is known to the business, the opt-out extends to that consumer.[35]

Recent enforcement activity underscores the significance of this requirement. California's settlement with Disney includes a statement that if a business links devices for advertising purposes, it should be prepared to link those same devices for opt-out purposes as well.[36] This principle is intuitive, and the NAI does not take issue with it. Businesses that associate consumer data across devices and identifiers to deliver advertising should apply opt-out signals with corresponding breadth.

However, one aspect of the current regulation warrants additional clarity. The term "pseudonymous profiles" is not defined in the CCPA or the existing regulations. In digital advertising, pseudonymous consumer profiles or device linkages are often built through probabilistic identity resolution, which infers associations between devices based on shared signals such as IP addresses, user agent strings, timestamps, and device characteristics, achieving broader reach than deterministic methods anchored to authenticated logins but with less precision and less persistence.[37] The FTC has recognized that while this methodology enhances competition by enabling companies without first-party login data to compete with the few large platforms that have it, it also creates challenges for honoring consumer opt-outs.[38] CalPrivacy's

---

[33] Cal. Priv. Prot. Agency, Invitation for Preliminary Comments: Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals, at 2 (Mar. 2026), https://cppa.ca.gov/regulations/pdf/pre_comments_reducing_friction_oops.pdf.

[34] Cal. Code Regs. tit. 11 § 7025(c)(1).

[35] *Id.*

[36] *See* Compl., People v. The Walt Disney Co., No. 26STCV04425 at 3 (Cal. Super. Ct., L.A. Cnty., filed Feb. 11, 2026), https://oag.ca.gov/system/files/attachments/press-docs/1%20-%20Complaint%20%28Disney%29.pdf; *see also* Proposed Final Judgment and Permanent Injunction, *id.* ($2.75M settlement), https://oag.ca.gov/system/files/attachments/press-docs/CA_SUP_LAX_26STCV04425__Final_Judgment_and_Permanent_Injunction.pdf.

[37] *See* IAB Tech Lab, *Identity Solutions Guidance* at 15–16 (2023), https://iabtechlab.com/wp-content/uploads/2024/05/Identity-Solutions-Guidance-FINAL.pdf (describing probabilistic identity methods that rely on IP addresses, user agent strings, timestamps, and device characteristics to infer associations between devices, and distinguishing these from deterministic methods based on authenticated identifiers such as email addresses and phone numbers).

[38] *See* Fed. Trade Comm'n, *Cross-Device Tracking: An FTC Staff Report* at 6, 15 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (finding at 6 that cross-device tracking technology "may enhance competition in the advertising arena" by enabling companies without deterministic data to compete with

own regulatory examples illustrate this dynamic: the scenarios accompanying § 7025 describe a consumer who clears cookies and revisits a website, at which point the business can no longer recognize the consumer and must process the opt-out anew.[39]

CalPrivacy should provide definitional clarity for "pseudonymous profiles," and guidance on the scope of association, to promote uniform compliance across the range of business models and data practices in the digital advertising ecosystem. In doing so, CalPrivacy should account for the practical realities of probabilistic identity resolution, including that linkages between identifiers may be severed over time and through routine processes such as cookie expiration, identifier resets, and IP address rotation. The NAI's cross-device guidance, which states that when a consumer opts out on a given browser or device, members should cease collection and use of data for personalized advertising on that browser or device and should not use data from the opted-out device for personalized advertising on other linked devices, offers a workable and tested model for how regulations can balance effective consumer choice with these technical limitations.[40]

**2. CalPrivacy should clarify that a valid opt-out preference signal must originate from the consumer, the consumer's device, or the consumer's user agent.**

A valid opt-out preference signal should originate from the consumer or from a mechanism the consumer has configured to send it. This follows from several provisions of the CCPA, read together.

Section 1798.135(e) provides that a consumer may authorize another person to opt out on the consumer's behalf "including through an opt-out preference signal . . . indicating the consumer's intent to opt out." Section 1798.135(b)(1) provides that a business may satisfy its opt-out obligations by honoring an OOPS "sent with the consumer's consent by a platform, technology, or mechanism." And the Opt Me Out Act requires browsers to include "functionality configurable by a consumer that enables the browser to send an opt-out preference signal."[41] The common thread across these provisions is that the signal is consumer-initiated.

The practical reality reinforces this reading. When a consumer enables GPC in a browser or browser extension, the consumer is making a choice by configuring a tool to communicate their opt-out request to the websites they visit. That is what an opt-out preference signal is designed to do, and it is consistent with the CCPA's objective: translate a consumer's configured preference into a technical signal that businesses can detect and honor.

A flag populated by a downstream intermediary in a programmatic bid protocol is fundamentally different in kind. That flag may reflect the intermediary's operational decision (*e.g.*, a publisher's choice about how to characterize the inventory it makes available) rather than anything the consumer configured or consented to. This does not mean that a consumer's opt-out choice

---

platforms that have large login-based user bases; concluding at 15 that "current limitations make it difficult to effectuate a single opt-out" across linked devices).

[39] *See* Cal. Code Regs. tit. 11, § 7025(c)(7), Example (E).

[40] *See* 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 (requiring members to cease collection and use of data for personalized advertising on the opted-out browser or device, and prohibiting the use of data from the opted-out device for personalized advertising on other linked devices, while not requiring that other linked devices be independently opted out absent a separate consumer choice on each device).

[41] Cal Civ. Code § 1798.136(a)(1).

(including when expressed via OOPS) loses its validity when it is later relayed through an intermediary. A consumer's authentic choice remains valid regardless of how it is transmitted. Rather, the distinction is between a consumer's choice expressed via OOPS and flags that are populated by intermediaries based on their own operational decisions without that consumer-configured origin. The CCPA does not clearly distinguish between these scenarios, and the existing regulations do not address signal provenance at all.

Intermediary-generated signals serve an important compliance purpose in facilitating consumer choice information between businesses. However, under the CCPA, they do not carry the same legal weight as a signal that originates from a consumer's configured browser or device, because they do not necessarily reflect the consumer's own choice in the way that the statute contemplates. This is also why business-to-business-contractual controls are often necessary for the proper functioning of these other signals.[42] As the OOPS ecosystem grows more complex and particularly as the Opt Me Out Act[43] brings additional browsers into play, the distinction between a consumer-configured signal and an intermediary-populated flag will become increasingly important.

CalPrivacy should clarify in its regulations that a valid OOPS is one that originates from the consumer's configured browser, device, platform, or user agent acting on the consumer's choice. This would promote trust in OOPS as a mechanism that genuinely reflects consumer choice.

## B. The Statute–Regulation Gap

CalPrivacy asks whether there is anything that requires additional clarity or guidance in the form of a regulation relating to OOPS.[44] There is, and this comment period presents an important opportunity for CalPrivacy to fulfill the CCPA's statutory vision for OOPS.

### 1. The Statutory Framework

The CCPA directs that regulations be adopted to further the purposes of the statute,[45] including a specific direction to address OOPS by defining the requirements and technical specifications for opt-out preference signals. The statute goes further, expressing legislative intent that those regulations should:[46]

- Ensure that the manufacturer of a platform, browser, or device that sends the signal cannot unfairly disadvantage another business;
- Ensure that the signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary;
- Clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent;

---

[42] *See* Michael Hahn & Rowena Lam, *Multi-State Privacy Agreement and Global Privacy Platform Update*, Interactive Advertising Bureau (May 14, 2024), https://www.iab.com/blog/multi-state-privacy-agreement-and-global-privacy-platform-update/.
[43] Opt Me Out Act, *supra* note 6.
[44] CalPrivacy Invitation for Preliminary Comments, *supra* note 1.
[45] Cal. Civ. Code § 1798.185(a), as originally enacted, directed the Attorney General to adopt regulations. Proposition 24 (2020) transferred this rulemaking authority to the California Privacy Protection Agency. *See id*. § 1798.185(d).
[46] *See id*. § 1798.185(a)(18)(A).

- Ensure that the signal does not conflict with other commonly used privacy settings or tools that consumers may employ;
- Provide a mechanism for the consumer to selectively consent to a business's sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the signal globally; and
- Specify that in the case of a page or setting view that the consumer accesses to set the signal, the consumer should see up to three choices, including a global opt-out from sale and sharing, a choice to limit the use of sensitive personal information, and a choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

In addition, the CCPA addresses how businesses honoring OOPS should respond to those signals, and provides that those regulations should promote competition and consumer choice, be technology neutral, and curb coercive or deceptive practices without unduly restricting good-faith compliance.[47]

The CCPA's direction is clear for the Agency to both develop regulations and define the specific requirements and technical specifications for OOPS. The NAI has previously encouraged the Agency to further develop these regulations in accordance with the CCPA, and we therefore appreciate this process to assess necessary updates to the existing regulations in this area.

### 2. The Current Regulations Do Not Address the Statute's Priorities

The existing CCPA regulations address OOPS in part.[48] The regulations establish that businesses must treat a valid OOPS as a consumer request to opt out of sale and sharing, and that the signal applies to the browser or device and any consumer profile associated with it, including pseudonymous profiles.[49]

However, the current regulations *do not*:

- define technical specifications for applications intended to serve as OOPS;
- address whether or how platform, browser, or device manufacturers may unfairly disadvantage other businesses through their implementation of OOPS;
- require that signals reflect a consumer's genuine, affirmative choice rather than a preset default;
- address conflicts between OOPS and other commonly used privacy settings or tools; or
- provide a mechanism for selective consent.

The gap between the statute's vision and the current regulations is significant and calls for further rulemaking. The NAI raised this issue in its November 2025 letter to CalPrivacy, and we welcome the opportunity to continue engaging with the Agency during formal rulemaking to address the gap.[50]

[47] *See* Cal. Civ. Code § 1798.185(a)(19)(A)-(D).
[48] *See* Cal. Code Regs. tit. 11 § 7025.
[49] *Id.* § 7025(b), (b)(1).
[50] *See* NAI Letter to CalPrivacy, *supra* note 3.

### 3. Recommendations

The NAI offers the following recommendations on the areas where additional regulation is most needed.

#### a. Default-on implementations must be addressed before AB 566 takes effect.

The CCPA provides that OOPS should "clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent."[51] This provision reflects a core principle of the CCPA's opt-out model whereby the consumer is empowered to decide. However, a signal that is activated by default without any affirmative decision by the consumer does not represent a consumer's choice. Instead, it represents a decision by the business operating the browser about what privacy settings its users should have.

This concern is not hypothetical. The Brave browser implemented GPC as a default-on setting and has done so since it first implemented the specification in 2020. Brave's own documentation states that it "does not require users to change anything to start using the GPC" because Brave treats a consumer's decision to download its browser as itself "an unambiguous expression that they do not want their data to be sold or shared online."[52] That reasoning conflates a consumer's choice of browser with a decision to opt out of all businesses they encounter online. Those are meaningfully different decisions, and the latter presupposes the consumer's intent in exactly the way the statute cautions against.

This is also particularly important in the case of Brave, because a consumer using Brave who did not intend to send GPC has no straightforward way to stop it. On desktop and Android, the only way to disable GPC is to navigate to a hidden developer page (brave://flags) that is not accessible through Brave's standard settings interface.[53] A proposal to add a standard user-facing toggle has been formally deprioritized in Brave's own engineering tracker.[54]

Brave is also instructive because it is not a disinterested intermediary. Brave blocks third-party advertising by default while operating its own competing advertising products, including display ads on the browser's new tab page, push notification ads, and search ads served through its own search engine.[55] In a March 2026 interview, Brave's Chief of Ads confirmed the company's advertising business model.[56] A browser that sends GPC by default, while simultaneously blocking the ads of other businesses and selling its own advertising to fill the resulting space, is not facilitating consumer choice. Brave appears to be using privacy controls to advance its own

---

[51] Cal. Civ. Code § 1798.185(a)(18)(A).
[52] Brave Software, *Global Privacy Control, a New Privacy Standard Proposal*, https://brave.com/web-standards-at-brave/4-global-privacy-control/ (last updated Sept. 8, 2023).
[53] *See* Brave Help Center, *How Do I Change My Privacy Settings?*, https://support.brave.app/hc/en-us/articles/360017989132-How-do-I-change-my-Privacy-Settings ("To toggle Global Privacy Control (GPC) on desktop and Android, go to brave://flags/#brave-global-privacy-control-enabled. GPC is enabled by default on Desktop and Android.").
[54] *See* Brave Browser, GitHub Issue #40561 (filed Aug. 20, 2024), https://github.com/brave/brave-browser/issues/40561, (proposing migration of GPC toggle to standard settings; classified as Priority P5: not scheduled).
[55] *See* Brave Software, *Brave Launches Self-Serve Ads Program*, (last updated Mar. 30, 2026), https://brave.com/blog/self-serve-ads/; Brave Software, Brave Search Ads Report Massive 1500% Growth (Feb. 2025), https://brave.com/blog/2025-search-ads-update/.
[56] *See* Jean-Paul Schmetz, Chief of Ads, Brave Software, interview with AdExchanger (Mar. 24, 2026), https://www.adexchanger.com/platforms/why-ad-blocking-browser-brave-introduced-its-own-ads/.

competing advertising model, one which disadvantages many other businesses across the digital media industry.

This matters because even a valid OOPS does not block advertising. A consumer whose browser sends a valid GPC signal will continue to see ads on the websites they visit. However, those ads become less relevant because the businesses that would otherwise use the consumer's information to tailor advertising can no longer do so. Less relevant advertising generates significantly less revenue for the publishers and content creators who depend on it to keep their content free. This tradeoff, between personalized advertising that supports free content and less relevant advertising that does not, is one that an informed consumer is better suited to choose, rather than being determined by a browser's default setting.

The urgency increases with the Opt Me Out Act, which will require all major browsers to include native OOPS functionality by January 1, 2027.[57] Without regulations addressing defaults before that date, additional browser manufacturers will make their own implementation decisions without clear standards to guide them. CalPrivacy has an opportunity and a responsibility under the CCPA to act now to establish clear rules of the road before the field expands.

There is strong consensus on this point across state lines. Every other state that has enacted OOPS or related requirements has also included protections against default settings that presuppose a consumer's intent. Across the other eleven states with OOPS provisions, all eleven require, in substance, that opt-out signals reflect affirmative, freely given, and unambiguous consumer choice rather than preset defaults.[58] California is the only state with OOPS provisions that require regulations to further effectuate these consistent legal requirements; but to date the regulations have not done so.

CalPrivacy should address this by promulgating regulations that require OOPS implementations to reflect a consumer's affirmative, informed choice, and that prohibit default-on settings that constrain or presuppose a consumer's intent to opt out. Regulations should also provide for periodic review of OOPS implementations to ensure that they continue to meet these standards as the ecosystem evolves. This would bring California's regulations into alignment with both the CCPA's own statutory framework and the approaches taken in other states. To help provide a model for how GPC implementations can both be easy-to-use for consumers and meet state law requirements for valid OOPS, the NAI developed and released its own GPC browser extension in 2025, designed to meet the requirements of state laws that set standards for valid OOPS.[59] Its settings do not presuppose the consumer's intent, and it is available as a free download that does not condition its use on participation in any advertising program.

[57] *See* Opt Me Out Act, *supra* note 6.
[58] *See, e.g.*, Del. Code Ann. tit. 6 § 12D-106(e)(1)(a)(2)(B); Conn. Gen. Stat. § 42-520(e)(1)(A)(ii)(II); and other states cited *supra* notes 30-32.
[59] *See* Network Advertising Initiative, *NAI Releases New Global Privacy Control Chrome Browser Extension to Facilitate Consumer Opt-Out Requests* (2025), https://thenai.org/the-nai-releases-new-gpc-browser-extension/; NAI Global Privacy Control Signal, Chrome Web Store, https://chromewebstore.google.com/detail/nai-global-privacy-contro/ecmgoeapljejplncpocmgnpdemidoffo.

### b. Unfair disadvantage and competition require regulatory attention.

The statute provides that regulations should ensure that the manufacturer of a platform, browser, or device "cannot unfairly disadvantage another business."[60] Separately, the statute provides that regulations governing business responses to OOPS should "promote competition and consumer choice and be technology neutral."[61] The current regulations are silent on these points.

The concern is structural. The companies that manufacture the most widely used browsers and mobile operating systems are not always neutral intermediaries standing outside the digital advertising ecosystem. Instead, they are major participants in it, with their own advertising businesses and privileged access to first-party consumer data. When those companies implement privacy mechanisms in ways that impose stricter requirements on third parties than on their own operations, the effect can be to raise rivals' costs, preserve first-party data advantages, and shift competitive value toward their own ecosystems — all under the banner of consumer privacy, but not necessarily to the privacy benefit of consumers.

This is not a theoretical risk. It has played out in practice with Apple's App Tracking Transparency ("ATT") framework, which provides a directly relevant precedent for the OOPS context. ATT required third-party apps to obtain explicit user consent before "tracking." However, Apple's own advertising operations, including personalized ads, continue to operate under a materially different choice architecture.

The competition effects have been significant and well-documented. France's competition authority found that ATT's objective was not problematic, but that its implementation was disproportionate, artificially complicated third-party app use, and caused economic harm to publishers and advertising service providers — particularly smaller publishers that depend more heavily on third-party data.[62] Competition authorities in Germany and the United Kingdom have expressed similar concerns,[63] and empirical research has corroborated these findings, documenting reduced ad effectiveness and revenue declines disproportionately borne by smaller firms.[64]

The lesson from ATT is directly applicable to OOPS. As the Opt Me Out Act brings additional browser manufacturers into the OOPS ecosystem — including companies with their own advertising businesses — the risk that privacy mechanisms will be implemented in ways that asymmetrically burden competitors is real and well-documented. The NAI fully agrees that

---

[60] Cal. Civ. Code § 1798.185(a)(18)(A).
[61] *Id.* § 1798.185(a)(19)(A).
[62] *See* Autorité de la concurrence [Fr.], Decision No. 25-D-02 (Mar. 31, 2025) (€150 million fine), https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-autorite-de-la-concurrence-imposes-fine-eu150000000-apple.
[63] *See* Bundeskartellamt [Ger.], *Bundeskartellamt Has Concerns About the Current Form of Apple's App Tracking Transparency Framework (ATTF)*, Preliminary Assessment (Feb. 13, 2025), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2025/02_13_2025_ATTF.html; UK Competition & Mkts. Auth., *Mobile Ecosystems Market Study, Appendix I: Considering the Impacts of Apple's ATT* (Dec. 2021), https://assets.publishing.service.gov.uk/media/61b86aeb8fa8f5037778c3b8/Appendix_I_-_Considering_the_impacts_of_Apples_ATT.pdf.
[64] *See* Konrad Kollnig et al., *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels*, FAccT '22 (2022), https://doi.org/10.1145/3531146.3533116; Guy Aridor et al., Evaluating the Impact of Privacy Regulation on E-Commerce Firms: Evidence from Apple's App Tracking Transparency, Management Science 0(0) (2025), https://doi.org/10.1287/mnsc.2024.06600.

implementation of OOPS at the browser level is a key feature for consumers to effectuate their choices. However, when a platform owner that also sells advertising designs those implementations so that third parties face stricter prompts, more friction, or weaker defaults than the platform's own advertising operations, the result is not consumer protection but, instead, competitive distortion.

To address these issues, CalPrivacy should develop regulations that:

- define what constitutes unfair disadvantage in the implementation of OOPS;
- require that platform, browser, and device manufacturers that implement OOPS apply materially comparable treatment to their own advertising operations and those of third parties; and
- provide for periodic review of OOPS implementations to ensure ongoing compliance with these standards.

These regulations would be consistent with the statute's directive to promote competition and technology neutrality.

**c. The GPC specification does not cover the full scope of what the statute envisions for OOPS.**

The statute provides that OOPS should serve as a mechanism for consumers to limit the use of their sensitive personal information, and that consumers should be able to selectively consent to a specific business's processing without disabling the signal globally.[65] The current regulations do not address either capability.

GPC is by its own terms limited to signaling a consumer's request that their data not be sold or shared with third parties and not be used for cross-context targeted advertising. The specification is explicit about its limitations: it "is not designed to exercise every possible privacy right, nor even every right to opt out of advertising or ad targeting."[66] GPC does not signal a request to limit the use of sensitive personal information, which is a distinct consumer right under § 1798.121 of the CCPA.

This creates a gap. The statute envisions OOPS as a vehicle for exercising the right to limit sensitive personal information processing. The only signal specification currently in use does not support that function. Regulations could address this by encouraging the development of signal specifications that support SPI-related signaling, or by clarifying how businesses should interpret and respond to OOPS in the context of SPI rights that the current signal does not cover. Notably, this is the only opt-out right under the CCPA that applies to a business's first party use of data, further implicating the competition issues posed by how privacy controls are implemented.

On selective consent: the statute provides that a consumer should be able to "selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally."[67] A consumer may wish to opt out generally while permitting a specific business to continue

[65] Cal. Civ. Code §§ 1798.185(a)(18)(A)(v)-(vi).
[66] *See* Global Privacy Control Specification, W3C Working Draft, https://w3c.github.io/gpc/.
[67] Cal. Civ. Code § 1798.185(a)(18)(A)(v).

processing. Under the current framework, the only way to make such an exception is to disable the signal entirely, which defeats its purpose. Regulations should provide for selective consent mechanisms consistent with the statute.

### C. Interstate Coordination

Finally, the NAI encourages CalPrivacy to coordinate with other states that have enacted OOPS requirements. An important distinction here is between OOPS as a legal concept and GPC as a technical specification. GPC is the signaling specification recognized in California, Colorado, Connecticut, and other states.[68] But the legal requirements for what makes an OOPS valid vary by state, even though the underlying technical signal is the same.

Eleven of twelve states with OOPS or similar provisions speak to consistency and interaction with other states' requirements, with California as the outlier.[69]

Businesses that honor OOPS do so across state lines. Consumers who activate GPC do so regardless of which state's law applies. Divergent regulatory frameworks for the same technical signal create confusion for consumers and undermine the ability of businesses to trust the signals they receive as genuine expressions of consumer intent. CalPrivacy can reduce that friction by coordinating with other states to develop a consistent regulatory framework, so that a signal that is valid in one state is valid in all. This would also align with the stated goals of CalPrivacy staff to harmonize the CCPA's requirements with those of other states' privacy laws.[70]

********

[68] *See, e.g.*, People v. Sephora USA, Inc., Stipulated Final Judgment and Permanent Injunction (Cal. Super. Ct. 2022), https://oag.ca.gov/system/files/media/pea-sephora-filed-judgment.pdf (California AG enforcement recognizing GPC as valid opt-out preference signal); Colo. Dep't of Law, Universal Opt-Out Mechanism Shortlist (July 2024), https://coag.gov/opt-out/ (designating GPC as a recognized universal opt-out mechanism); Conn. Office of the Attorney General, Joint Investigative Privacy Sweep with California and Colorado (2025), https://portal.ct.gov/ag/press-releases/2025-press-releases/connecticut-california-and-colorado-announce-joint-investigative-privacy-sweep.

[69] *See, e.g.*, Conn. Gen. Stat. § 42-520(e)(1)(A)(ii)(IV); Del. Code Ann. tit. 6 § 12D-106(e)(1)(a)(2)(D); Colo. Rev. Stat. § 6-1-1313(2)(e).

[70] *See, e.g.*, *Behind the Curtain With Tom Kemp: New CCPA Rules, Enforcements, and What's Next*, Red Clover Advisors, YouTube, https://youtu.be/rAyd25gu6_Y ("It's important for us to . . . ensure that we're harmonized with other states in terms of the enforcement of our laws[.]"); *How CalPrivacy Balances Enforcement, Transparency, and Innovation with Tom Kemp of the California Privacy Protection Agency*, The Privacy Insider Podcast, Ep. 23, Osano, YouTube (Feb. 16, 2026), https://www.youtube.com/watch?v=I_67D9Qw4wQ ("We are required . . . to work with not only state legislators here in California and other governmental bodies but also across jurisdictions . . . that will provide harmonization of our laws with other laws that are out there will make it easier for consumers and businesses.").

## Conclusion

The NAI appreciates CalPrivacy's commitment to developing a regulatory framework for opt-out preference signals that reflects the CCPA's statutory vision and serves consumers, businesses, and the digital advertising ecosystem. 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 regulations that promote effective consumer choice, fair competition, and clear expectations for businesses.

Sincerely,

**Tony Ficarrotta**

Vice President, General Counsel

The NAI