

September 24, 2025

The Honorable Gavin Newsom
Governor, State of California
1021 O Street, Suite 9000
Sacramento, CA 95814

RE: Veto AB 566 – Opt-out preference signal requirements

Dear Governor Newsom:

The Network Advertising Initiative (NAI) supports easy-to-use mechanisms for consumers to exercise control of their data, including the use of opt-out preference signals (OOPS). However, we ask that you veto AB 566 because it does not include appropriate safeguards to ensure that the OOPS it would require browser providers to implement will represent authentic consumer choices and be free of anti-competitive default settings that pre-suppose consumer choices and unfairly disadvantage ad-supported businesses online.

Founded in 2000, the NAI is the leading non-profit, self-regulatory trade association for advertising technology companies. For 25 years, the NAI has promoted strong consumer privacy protections, a free and open Internet, and has enabled small businesses to thrive by promoting the highest voluntary industry standards for consumer privacy across digital advertising. The NAI recently released a Global Privacy Control (GPC) browser extension to help consumers exercise their rights to opt out of targeted advertising and sales of their personal data under the California Consumer Privacy Act (CCPA) and other state privacy laws.¹

The NAI opposes AB 566 because it does not do enough to ensure that the OOPS it would require browsers to implement will represent authentic consumer choices to opt-out. AB 566 merely requires browsers to include “functionality configurable by a consumer that enables the browser to send an opt-out preference signal.”

During the legislative session, the NAI encouraged the sponsors of AB 566, Assembly Member Lowenthal and the California Privacy Protection Agency (CPPA), to adopt amendments that accomplish the following objectives:

1. Direct the CPPA to promulgate regulations that are consistent with Cal. Civ. Code Sec. 1798.185(a)(18) and clarify that proposed requirements for browsers to support OOPS in will not take effect until the CPPA completes the required rulemaking.

¹ See, The NAI Releases New Global Privacy Control Chrome Browser Extension to Facilitate Consumer Opt-Out Requests: <https://thenai.org/the-nai-releases-new-gpc-browser-extension/>.

2. Instruct the CCPA to work with other states with similar legal requirements for OOPS to identify signals that are compliant with these requirements.² Coordinating with other states in this way will align with the objectives of other state regulators with similar legal requirements, make it easier for consumers to identify which signals they can use to effectuate their rights across states, and improve business compliance by simplifying the array of signals they may have to detect and honor.

These recommendations align with the CCPA, which recognizes the importance of fair, valid implementations of OOPS. Specifically, Section 1798.185 establishes the following requirements and specifications for OOPS to be established in regulations:³

- Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.
- Ensure that the opt-out preference 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.
- Ensure that the opt-out preference 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' 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.
- State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:
 - Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.
 - Choice to "Limit the Use of My Sensitive Personal Information."
 - Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

However, the existing CCPA regulations promulgated by the CPPA have not yet implemented the CCPA's requirements and specifications to ensure that OOPS fairly represent a consumer's intentional choice to opt out, and that these signals are not deployed in a way that enables conglomerate intermediaries—such as providers of

² See relevant state laws containing similar requirements, chart row 20: https://docs.google.com/spreadsheets/d/1et7DQQSNB_QY9byQZ_ARcBR293zZ6l4GXqkp042lZcQ/edit?usp=sharing, e.g., laws in CT, DE, MD, MN, NH, NJ, and OR (requiring OOPS to be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation; CO law (requiring that rules for universal opt-out mechanisms must adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States); MT law (requiring that a valid mechanism must be consistent with any federal or state law or regulation); and NE and TX law (providing that a controller is not required to comply with an opt-out request received through an authorized agent if it does not process similar requests from consumers for the purpose of complying with similar laws or regulations of another state).

³ CCPA at § 1798.185(a)(18)

browsers—to unfairly disadvantage other smaller businesses. Ensuring the regulations adhere to all the CCPA's requirements is important, especially when the developers of widely used browsers are often conflicted and may constrain or presuppose a consumer's intent in a way that significantly disadvantages smaller businesses from competing.⁴

While Section 7025 of the CCPA regulations addresses opt-out preference signals, this section of the regulations does not fully meet the requirements outlined above, particularly the following stipulations:


- prohibit the use of defaults constraining or presupposing a consumer's intent;
- provide guidance on how businesses providing OOPS do not unfairly disadvantage other businesses; and
- provide for the use of opt-out preference signals to allow consumers to limit the use of their sensitive personal information.⁵

The NAI is actively promoting the use of valid OOPS, as we believe these signals hold great promise for empowering consumers to exercise key privacy choices, but it would be premature to require browsers to provide OOPS without also further clarifying and ensuring that the CPPA meets explicit statutory requirements to guide the implementation and use of OOPS.

Given the absence of these important provisions, enactment of AB 566 is likely to lead to a proliferation of privacy signals that do not meet the CCPA's thoughtful requirements. The NAI therefore encourages you to veto AB 566 and direct the legislature to achieve these objectives in legislation next year.

Thank you in advance for your consideration of this request.

Sincerely,

A handwritten signature in blue ink, appearing to read "Leigh Freund", is enclosed within a thin blue rectangular border.

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

⁴ See Konrad Kollnig et al., *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels* (May 7, 2022), <https://arxiv.org/pdf/2204.03556>, ("Being the maker of the iOS ecosystem, Apple has a certain competitive advantage, by being able to collect device and user data, including hardware identifiers, that other app developers do not have access to, and use this for its own business purposes."); Latham, Steve, *Why Apple's Anti-Tracking Move Hurts Everyone ... But Apple* (Sep. 12, 2020), <https://www.flashtalking.com/blog/2020/9/12/why-apples-anti-tracking-move-hurts-everyone-but-apple>.

⁵ See Cal. Code Regs. tit. 11 § 7025.