March 25, 2025

Assembly Member Rebecca Bauer-Kahan
Chair, Privacy and Consumer Protection Committee
California General Assembly
1020 North Street, Room 162
Sacramento, CA 95814

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

Dear Chair Bauer-Kahan:

The NAI supports easy-to-use choice mechanisms for consumers, including the use of opt-out preference signals (OOPS). However, we are opposed to AB 566 because it does not include appropriate safeguards to ensure that the OOPS it would require browser and mobile device providers to implement will be comprehensible to consumers, 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.[1] 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 the responsible collection and use of consumer data.

The NAI has long been a leader in providing consumer choice mechanisms to opt out of the use of their data for targeted advertising. To that end, our updated Self-Regulatory Framework provides flexibility for member companies to tailor their privacy compliance efforts towards the requirements being put in place by state privacy laws like the California Consumer Privacy Act (CCPA), including the use of valid OOPS such as certain existing implementations of the Global Privacy Control (GPC) opt-out signaling specification.[2]

However, the NAI opposes AB 566 as currently drafted because it does not do enough to ensure that the OOPS it would require browsers and mobile operating systems to implement will represent authentic consumer choices to opt-out–on the contrary, default opt-out settings

[1] *See History of the NAI*, The Network Advertising Initiative, https://thenai.org/about-the-nai-2/history-of-the-nai/.
[2] Global Privacy Control Specification, Working Draft Document (Mar. 20, 2025), W3C https://w3c.github.io/gpc/.

would alter a user's expected internet experience and require potentially confusing measures to turn such a setting off. The importance of fair, valid implementations of OOPS is already contemplated by the CCPA, particularly as set forth in section 1798.185(18)(A), which 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 California Privacy Protection Agency (CPPA) have not yet implemented 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 browsers and mobile operating systems—to unfairly disadvantage other smaller businesses. Indeed, ensuring the regulations adhere to all of the CCPA's requirements is important, especially when the developers of widely-used browsers and mobile operating systems are often conflicted and may constrain or presuppose a consumer's intent in a way that significantly disadvantages smaller businesses from competing.[4]

---

[3] CCPA at § 1798.185(a)(18)

[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.

While Section 7025 of the CCPA regulations addresses opt-out preference signals, that 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]

Additionally, the CCPA did not establish a process through which the CPPA may evaluate and determine which OOPS satisfy these requirements, and as such, should be recognized by businesses as consumer choice representations under the CCPA. Absent such a requirement, businesses run the risk of a proliferation of privacy signals that do not meet the CCPA's thoughtful requirements.

While we are supportive of the use of valid OOPS and believe they hold great promise for empowering consumers to exercise their privacy rights, we also believe that requiring browsers and mobile operating systems to support OOPS without further clarifying and ensuring that the CPPA meets explicit statutory requirements to guide the implementation and use of OOPS would be premature.

Therefore, the NAI recommends the following two amendments to AB 566.

1. Reiterate the CCPA's statutory requirements highlighted above and 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 and mobile operating systems to support OOPS in AB 566 will not take effect until the CPPA completes the required rulemaking.
2. Require that the CPPA work with other states with similar requirements for OOPS to identify signals that are compliant with these requirements, as established across all other state laws that require businesses to honor consumer requests via OOPS;[6] coordinating with other states in this way will 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.

---

[5] *See* Cal. Code Regs. tit. 11 § 7025.

[6] 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).

If AB 566 is amended in these ways to ensure that OOPS represent authentic consumer choices and prevent providers of browsers and mobile operating systems from unfairly disadvantaging other controllers, the NAI could support this important effort to help empower California consumers in exercising their privacy rights online.

Sincerely,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

cc: Members of the California Assembly Privacy and Consumer Protection Committee