November 20, 2025

Tom Kemp
Executive Director
California Privacy Protection Agency
400 R Street Suite 350
Sacramento, CA 95811

RE: Development of Opt-Out Preference Signal regulations

Dear Executive Director Kemp,

I was pleased to learn from the California Privacy Protection Agency (CalPrivacy) Board meeting on November 7, that CalPrivacy has identified Opt-Out Preference Signals (OOPS) as a priority for new regulations under the California Consumer Privacy Act (CCPA). On behalf of the Network Advertising Initiative (NAI), I write to support this proposal, and to urge CalPrivacy to develop regulations to ensure that the way any OOPS is implemented is 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 enabled small businesses to thrive by promoting the highest voluntary industry standards for the responsible collection and use of consumer data for digital advertising, and the provision of consumer choice mechanisms to opt out of the use of their personal information for interest-based advertising. The NAI's approach to offering consumer choice tools has evolved recently,[2] and we currently offer 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 CCPA and other state privacy laws.[3] In developing and releasing this extension, our goals were to both provide consumers with a modern opt-out request tool, and to meet the requirements of state laws that set standards for valid OOPS.[4]

---

[1] See *History of the NAI*, https://thenai.org/about-the-nai-2/history-of-the-nai/.

[2] *See NAI Releases New Consumer Resources for Online Privacy,* https://thenai.org/the-nai-releases-new-consumer-resources-for-online-privacy-sunsets-legacy-opt-out-tools/

[3] 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/.

[4] Some states alternatively refer to universal opt-out mechanisms (UOOMs). *See, e.g.* Colo. Rev. Stat. § 6-1-1306(1)(a)(IV)

Like other states, the CCPA provides a detailed set of criteria that are necessary for a valid OOPS, and it directs CalPrivacy to develop regulations to achieve these goals. Specifically, the CCPA establishes the following requirements and specifications for OOPS to be established in regulations:[5]

- 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, while Section 7025 of the CCPA regulations addresses opt-out preference signals, the existing CCPA regulations do not fully meet the requirements from the CCPA outlined above.[6] The regulations 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 intermediary companies—such as providers of browsers and mobile operating systems—to unfairly disadvantage other smaller businesses based on how they deploy OOPS.

This is a particularly timely issue with the recent passage of the Opt Me Out Act, which will require a business that develops or maintains a web browser to include OOPS functionality.[7] Without meaningful regulations that reflect the CCPA's requirements for OOPS, those businesses could implement OOPS in a way that conflicts with the CCPA's stated goals. This is not hypothetical. The developers of widely-used browsers are often conflicted in terms of their business objectives related to the development of browsers, which are competitive with or at

---

[5] Cal. Civ. Code §1798.185 (a)(18)(A)

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

[7] A.B. 566, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB566.

odds with independent ad-supported media online. Without clear regulations consistent with the CCPA, developers may constrain or presuppose a consumer's intent in a way that disadvantages smaller businesses from competing.[8] Default-on settings for OOPS would diverge from the intent of the CCPA and alter a user's expected internet experience, without giving consumers a chance to make an affirmative decision to opt out. The business interests of browser manufacturers should not become a stand-in for consumer preferences.

Therefore, I encourage CalPrivacy to develop additional regulations to fully meet the requirements outlined above, and in particular to set the following unambiguous standards for a valid OOPS in the regulations:
- prohibit the use of default settings constraining or presupposing a consumer's intent to opt out;
- provide guidance on how businesses providing OOPS must avoid unfairly disadvantaging other businesses; and
- provide for the use of OOPS to allow consumers to limit the use of their sensitive personal information – an opt-out right that the CCPA enables for OOPS but that the current regulations do not address.

Listening to your remarks at the International Association of Privacy Professionals (IAPP) conference in October, I was pleased to hear your commitment for CalPrivacy to prioritize regulatory consistency and harmonization of CCPA regulations with respect to both California laws, and also with the laws across other jurisdictions. The NAI supports CalPrivacy working closely with other states with similar requirements for OOPS to develop regulations and guidance that will provide a consistent framework across all state laws that require businesses to honor consumer requests via OOPS.[9]

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. Without intentional

---

[8] *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.

[9] See relevant state laws containing similar requirements, chart row 20: https://docs.google.com/spreadsheets/d/1et7DQQSNB_QY9byQZ_ARcBR293zZ6I4GXqkp042lZcQ/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).

coordination with other states, disparate requirements across the U.S. is likely to lead to confusion and dysfunction of important OOPS for both consumers and businesses.

Thank you in advance for your consideration of this request. The NAI stands ready to provide additional input into the consideration of additional CCPA regulations. Please do not hesitate to contact me for more information or to discuss this issue and the NAI's efforts in greater detail.

Sincerely,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)