409 7th Street, NW Suite 250
Washington, DC 20004

August 23, 2022

Attn: Brian Soublet
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Dear California Privacy Protection Agency,

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide comments on the proposed regulations under the California Privacy Rights Act ("CPRA").

I. Introduction

A. Overview of the NAI

Created during the nascence of the online advertising industry in 2000, the NAI is one of the internet's longest standing and most respected industry self-regulatory programs, whose members are made up of advertising technology providers in the online advertising ecosystem. For over 20 years, the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and consumer trust. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising across all digital media.

All NAI members are required to adhere to the NAI's FIPPs-based, privacy-protective Code of Conduct (the "NAI Code"), which continues to evolve and recently underwent a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy. The NAI continues to monitor state and federal legal and regulatory changes, and our Code evolves to reflect–and in some cases exceed–those requirements. Member compliance with the NAI Code is promoted by a strong accountability program. NAI attorneys subject each NAI member to a comprehensive annual review of their businesses and data collection and use practices for adherence to the NAI Code. In addition, NAI staff advises companies on an ongoing basis about how to best comply with the Code and guidance ,and how to implement privacy-first practices. Finally, the NAI team conducts technical monitoring and review of company opt outs and privacy tools. Enforcement of the NAI Code can include penalties for material violations, and potential referral to the Federal Trade Commission (FTC). Annual reviews cover member companies' business models, privacy policies and practices, and consumer-choice mechanisms.

B. Benefits of State Law & Enforcement Harmonization

With five comprehensive state consumer privacy laws expected to become operative in the next 12 months, and many more states considering new laws, we are likely facing an inconsistent set of rules across the United States that will confuse consumers, and a disparate set of obligations that will make compliance overly difficult for businesses. We therefore urge you to seek a collaborative approach in developing implementing regulations, and specifically to work with other states to harmonize requirements to the greatest extent possible. Colorado Attorney General Phil Weiser recently committed to harmonizing his state's regulations with other states,[1] and we hope you will engage in dialogue with Colorado and other state enforcement officials to maximize consistency in the implementation of legal requirements.

This coordinated approach will greatly benefit consumers in California and across the country, in addition to businesses trying in good faith to comply with disparate laws. It will also be to the overall benefit of the California economy, and the U.S. economy more broadly, both of which are increasingly data-driven. A consistent approach across the U.S. could also help the Agency and other state regulators minimize costly legal challenges resulting from conflicting requirements.

C. Summary of NAI Recommendations

- **Opt-out Preference Signals —** The proposed regulations should be amended in accordance with the following three objectives: (1) to reflect the foundational objectives established in the CPRA that an opt-out "[c]learly represent a consumer's intent and be free of defaults constraining or presupposing that intent," and to "[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business;" (2) to establish an open and transparent review process that provides for stakeholder input to evaluate any mechanisms that propose to serve as Signals in accordance with the CPRA; and (3) to recognize that many businesses do not have the capability to recognize a consumer's opt-out request if they previously elected to use a preference signal, and that signal is disabled or does not transmit at a later date.

- **Restrictions on the Collection and Use of Personal Information —** The proposed regulations should be amended to clarify that compatible purposes, when provided with notice in compliance with the requirements of CPRA, are subject to the law's opt-out requirements, rather than creating a new opt-in requirement or a ban on compatible uses based on whether they may or may not meet an average consumer's expectation.

- **Notice at Collection of Personal Information** — The proposed regulations should be amended to clarify business may comply with the CPRA's notice requirements by providing the *types/categories* of third parties engaged in data collection, rather than having to list all of the third parties collecting personal information.

---

[1] *See* OFF. OF THE CO. ATT'Y GEN., PREPARED REMARKS: ATTORNEY GENERAL PHIL WEISER AT THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (April 12, 2022), https://coag.gov/app/uploads/2022/04/Data-Privacy-Protection-A-Colorado-Perspective.pdf (stating that through the Colorado Privacy Act ("[W]e want to make Colorado's requirements harmonious and interoperable with requirements adopted by other jurisdictions."); *See also* OFF. OF THE CO. ATT'Y GEN., PRE-RULEMAKING CONSIDERATIONS FOR THE COLORADO PRIVACY ACT (2022), https://coag.gov/app /uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy- Act.pdf. ("The rules should facilitate interoperability and help situate the CPA alongside the competing protections and obligations created by other state, national, and international frameworks.").

- **Requests to Opt Out of Sale/Sharing** — The proposed regulations should be amended to conform with the requirements of the CPRA, clarifying that businesses are not required to transmit opt-out requests to third party partners and require those partners to further pass along an opt-out request.

- **Contract Requirements for Service Providers, Contractors and Third Parties**— The proposed regulations should be amended to provide flexibility in the regulations for the use of standardized industry contracts that identify specific permitted digital advertising activities, data collection and use restrictions, data safeguards, and applicable business purposes when engaging in those activities.

- **Audits and Enforcement** — The proposed regulations should be amended to permit the use of independent, third parties for required audits. Additionally, the NAI proposes the Agency clarify audit scope and implement additional guidelines for the audit process.

II. § 7025: Opt-Out Preference Signals

The NAI has a long history of promoting consumers' ability to exercise choice with respect to how companies use their data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use choice mechanisms is a foundational element of tailored advertising that the NAI has championed for decades.[2]

To this end, the text of the CPRA provides the opportunity for businesses to honor automated "opt-out preference signals" ("Signals").[3] The NAI recognizes the substantial value Signals can provide to both consumers and businesses, particularly in an environment where expressing user preferences can be difficult and confusing for consumers due to the wide range of businesses, operating systems, software, and platforms. In fact, the NAI led industry efforts to provide a platform for consumers to express their preferences with respect to their data use for tailored advertising by creating and operating an centralized opt out page for consumer choice.

However, the industry's broad and consistent recognition of Signals that represent a clearly expressed choice by consumers ,and that relate to the choices established by the CPRA, are dependent on effective regulations that implement foundational requirements established by the statute. Unfortunately, the draft regulations are largely inconsistent with the language and the intent of the statute, and they do not adequately facilitate meaningful or active consumer choices to opt-out from the sale and sharing of their personal information. Below, we identify key areas where Sec. 7025 of the proposed regulations need to be amended to ensure that consumers are the ones making decisions about the use of their personal information, and to preserve fair competition across the digital media ecosystem.

A. Opt-Our Preference Signals Must Be User-Enabled

The CPRA requires the Agency to issue regulations that define requirements and technical specifications of the opt-out preference signal that, "clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent."[4] The statute also explicitly directs the Agency to

[2] *See* NAI Code § II.C.1; Network Advertising Inititative, Best Practices for User Choice and Transpareny (May 10, 2022), https://thenai.org/best-practices-for-user-choice-and-transparency/.
[3] *See* CAL. CIV. CODE §§ 1798.135, 1798.185(a)(19-20).
[4] CAL. CIV. CODE § 1798.185(19).

develop regulations that, "[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business."[5]

These are foundational principles governing the effective deployment of Signals across the marketplace. Similar requirements were also included in recently enacted consumer privacy laws in Colorado and Connecticut.[6] Therefore, the stated goals of the Agency to harmonize with other similar state laws would also be served by regulations that adhere to these requirements.

As currently drafted, however, the proposed regulations do not achieve these statutory objectives. Instead, the proposed regulations essentially require businesses to honor *any* opt-out signal, only provided that the Signal "is in the proper HTTP format," and that the business providing the Signal makes clear to the consumer, either through configuration or public disclosure, that it is "meant to have the effect of opting the consumer out of the sale and sharing of their personal information."[7] As a result, the proposed regulations would permit browsers – or any other technology platform providers, such as application or operating system providers – to implement Signals that automatically opt consumers out of the selling or sharing of their data, while only providing mere "public disclosure" and not a direct action by the consumer. Consumers very often rely on software and applications natively bundled with devices and operating systems without specific thought to restrictions placed on their activity across the internet, resulting in a wide range of signals that are likely to arise across the marketplace consumers are unaware they are even generating, let alone represent consumers' informed choice about their personal information.

While the NAI supports the goal of empowering consumers with easy-to-use choice mechanisms, allowing a limited number of technology intermediaries to make unilateral decisions that presume user preferences creates market imbalances by putting those companies in a position to drive business models across the digital media industry. According to a 2019 NAI survey, 60% of consumers prefer to have online content sponsored by advertising, rather than paying subscription fees for individual websites and apps.[8] The vast majority of this advertising is data-driven, utilizing various data points to show consumers more relevant and interesting ads, and making marketing decisions that provide greater value to publishers and digital service providers. Therefore, allowing Signals to be "on-by-default" is likely to dramatically curtail the predominant data-driven advertising model that promotes rich digital content today, without representing meaningful consumer choices, and to benefit certain company business models over others.

For example, while Apple's policies and technology tools are marketed as privacy-friendly, among other marketing approaches, their limits on sharing of consumers' personal information also promotes their own business model, which relies more on revenue derived from charging consumers and other businesses fees for using their services or operating on their platforms.[9] This model is in contrast to

---

[5] *Id.*

[6] The Colorado Privacy Act provides that the rules must "not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller," and that an opt-out mechanism "must be as consistent as possible" with the mechanisms required by other states. COLO. REV. STAT. § 6-1-1313(2)(a)(e). Similarly, Connecticut's Privacy Law provides that an opt-out mechanism must "not unfairly disadvantage another controller" and must "be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation[.]" CONN. GEN. STAT. § 6(e)(A)(ii).

[7] CAL. CODE REGS. tit. 11, § 7025(b)(proposed).

[8] NETWORK ADVERTISING INITIATIVE, NAI CONSUMER SURVEY ON PRIVACY AND DIGITAL ADVERTISING, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/.

[9] Apple's service business, which includes revenues from its advertising (and specifically App Store search ads) grew by 24% in the 2021 fiscal year, for a record $19.5 billion in revenue. Such growth has been possible in part because of

many other digital media businesses that rely more heavily on data-driven advertising and marketing, and it gives Apple a clear market incentive to increase revenues derived from fee-based apps and first-party advertising, rather than third-party ad-supported apps that comprise the majority of apps used by consumers today.

At the same time, Apple has also recently increased their use of first-party advertising, which allows them to bypass the same permission prompts they require of other businesses across their mobile app marketplace, while not necessarily increasing consumer privacy.[10] This is just one example of how the proposed regulations would enable a dominant technology company to usurp true user choices to their own market advantage. If the regulations are not amended to better reflect the protections required by the CPRA, the marketplace is likely to see a proliferation of other technology companies developing and deploying Signals for their own purposes, rather than as a genuine choice tool for consumers. Even if this were a goal of the Agency in developing the regulations, it does not necessarily protect consumers from harms, including privacy harms, that may result from collection of their personal information by a business with which they interact. Instead, it would merely limit that business from selling or sharing. Any first-party company, particularly a dominant technology platform such as Apple, could still collect and use a consumer's data to perform personalized, data-driven advertising across their own broad ecosystem of products and services that compete with smaller competitors who at the same time are precluded from leveraging consumer data to provide tailored advertising.

The NAI always has been, and continues to be, supportive of innovative tools and solutions that implement privacy by design. Companies should be incentivized to create competitive products and services that protect consumer data while maintaining a fair, competitive marketplace. To best achieve both consumer protection and a competitive marketplace, the Agency should not create opportunities for technology intermediaries to impose legal compliance obligations on covered businesses if these do not genuinely reflect consumers' informed decisions about the collection and use of their data.

The NAI appreciates and concurs with the Agency's goal of enabling various platforms and technology providers to develop Signals that genuinely enable consumer choices, rather than seeking to promote a singular technology standard or Signal that would be specific to the state of California and the CPRA. However, this approach is not without challenges to the marketplace. That is, digital businesses operating across different technologies and platforms quite possibly will be challenged by the need to identify and comply with a wide range of different Signals, particularly as they seek to determine which Signals genuinely reflect consumer choices, and which are merely Signals activated by the technology intermediaries. Ultimately, many businesses will challenge and reject Signals that do not reflect consumer choices, therefore unfairly disadvantaging their businesses.

The regulations can help provide clarity and fairness for businesses across the marketplace that will receive these signals—indeed, this is consistent with the direction of the statute. The best way to achieve these goals is for the Agency to establish an open and transparent review process that provides for stakeholder input to evaluate any mechanisms that propose to be recognized as Signals

---

Apple's App Tracking Transparency privacy changes, which forced advertisers running mobile app ads to recalibrate and shift spending to the App Store—where Apple can directly collect money. *See* Nina Goetzen, *Apple Ad Revenues Skyrocket Amid Its Privacy Changes*, Insider Intelligence (Jan. 31, 2022), https://www.emarketer.com/content/apple-ad-revenues-skyrocket-amid-its-privacy-changes/.

[10] *See* Samuel Axon, *Apple Ad Exec Wants to More Than Double Ad Revenue with New Ads Across iOS*, ARSTECHNICA (Aug. 15, 2022), https://arstechnica.com/gadgets/2022/08/report-apple-is-exploring-in-app-ads-for-maps-podcasts-books-and-beyond/; *see also* Sara Fischer & Scott Rosenberg, *How Apple Pushed Its Ad-vantage*, AXIOS (Aug. 21, 2022), https://www.axios.com/2022/08/21/apple-advertising-privacy-tracking-iphone.

in accordance with the CPRA. This review process should be ongoing, providing the Agency with the opportunity to periodically evaluate and test Signals deployed in the marketplace to ensure that they continue to be administered fairly. To assist in the review process, the Agency should seek input from stakeholders, particularly those businesses to which the Signals are directed.

- **NAI Recommendations:**

The proposed regulations pertaining to opt-out preference signals should be amended to achieve the CPRA's requirements to, "[c]learly represent a consumer's intent and be free of defaults constraining or presupposing that intent," and "[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business."

The proposed regulations should also be amended to establish an open and transparent review process that provides for stakeholder input to evaluate any mechanisms that propose to serve as a Signals in accordance with the CPRA. The review process should be ongoing, providing the Agency with the opportunity to periodically evaluate and test Signals deployed in the marketplace to ensure that they continue to be administered fairly. To assist in the review process, the Agency should seek input from stakeholders, particularly those businesses to which the Signals are directed.

Amend § 7025 as follows:

> (b) A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:
>
> > (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.
> >
> > (2) The platform, technology, or mechanism, ~~whether in its configuration or in disclosures to the public,~~ that sends the opt-out preference signal shall make clear to the consumer that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information in accordance with the CPRA. The configuration or disclosure does not need to be tailored only to California or to refer to California, but both the configuration and disclosure must be clear to the consumer and receiving businesses that it applies to the specific choices provided by the CPRA and activated by the consumer.
> >
> > (3) The platform, technology, or mechanism that sends the opt-out preference signal shall require the consumer to activate the signal, in accordance with (b)(2). Consumer activation of a signal can be done through the use of a clear, conspicuous and easy to use mechanism by which the consumer can exercise choice, such as a dropdown menu or main settings menu.
> >
> > (4) The signal is formally recognized by the Agency as compliant with the requirements established by the CPRA and in § 7025, in accordance with an open review process through which stakeholder review and input is solicited to evaluate the signal(s).

B. Honoring Preference Signals No Longer Present

The proposed regulation provides "[a] business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-

in to the sharing of personal information."[11] While we agree that the absence of a Signal should not be interpreted by a business to indicate that a consumer has affirmatively opted-in, the regulations should be clarified to recognize that a business cannot reasonably be expected to have the capability to recognize a consumer's opt-out if they previously elected to use a preference signal, and that signal is disabled or does not transmit at a later date.

In many instances, businesses cannot reasonably associate an opt-out signal with an individual consumer after switching browsers or devices, etc. Ultimately, if a consumer elects to deploy an opt-out preference signal, and then the signal disappears or is no longer visible to the business, the business should not be expected to maintain an opt-out for that user.

- **NAI Recommendations:**

The proposed regulations should be amended to recognize that many businesses do not have the capability to recognize a consumer's opt-out request if they previously elected to use a preference signal, and that signal is disabled or does not transmit at a later date.

Amend § 7025 as follows:

> (c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):
>
> > (5) A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information, however the business shall also not be required to process an opt-out for any consumer if the business is not able to associate the previously detected opt-out preference signal with a specific consumer, after such time as any opt-out preference signals becomes absent.

III. § 7002: Restrictions on the Collection and Use of Personal Information

In Sec. 1798.100, the CPRA provides that a business' collection, use, retention, and sharing of personal information be "*reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed*, or *for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.*"[12] The CPRA therefore provides essentially two tests for the collection, use and sharing of consumers' personal information—whether such uses are "reasonably necessary and proportionate" and whether any additional use or processing is "compatible" with the purposes for which it is collected. Related to these, the CPRA also establishes use and sharing limitations based on the disclosure obligations of the businesses that control this data collection, stating, "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes that are *incompatible with the disclosed purpose* for which the personal information was collected without providing the consumer with notice consistent with this section."[13] The emphasis throughout the statute is to provide for businesses to clearly disclose the uses of consumers' personal information at collection.

---

[11] CAL. CODE REGS. tit. 11, 7025(c)(5) (proposed).
[12] CAL. CIV. CODE § 1798.100(c) (emphasis added).
[13] CAL. CIV. CODE § 1798.100(a)(1) (emphasis added).

The NAI agrees with the statute's emphasis on clear notice requirements and we agree that businesses should not collect, use, and share personal information for purposes incompatible with these notices—this construct is at the core of the CPRA's mandate for businesses to facilitate consumer choices established by the CCPA. However, Sec. 7002 of the proposed regulations appears to deviate from the law and hinge compatibility more on the expectations of consumers, stating "[a] business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) *if they are compatible with what is reasonably expected by the average consumer*."[14]

As currently drafted, the proposed regulations rely disproportionately on the expectations of the consumer about their use of their personal information, rather than recognizing, as the statute establishes, that businesses are required to provide notice for compatible uses and provide an opt-out. The CPRA makes reference to the "average consumer" standard in multiple instances, but it does not use this test in determining what collection, uses and sharing are, or are not, compatible. As referenced above, the CPRA instead applies the concept of "compatible" to the context of collection, rather than consumer expectations, stating that the business collection can be for, "*another disclosed purpose that is compatible with the context in which the personal information was collected.*"[15]

The regulations also require opt-in consent before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information is collected or processed.[16] The NAI agrees that not all categories of personal information should be treated equally, and our Code reflects this, by requiring enhanced, explicit notice requirements beyond a privacy policy in situations involving certain categories of personal information, including precise geolocation and sensitive health information, among others.[17] While the proposed regulations are in some ways consistent with the NAI's long standing—and now widely accepted—industry standard for notice about collection and use of precise location information and other sensitive personal information, they are unclear as to how a business should apply this as established by the CPRA and Sec. 7002 as drafted, particularly with respect to the CPRA's opt-out requirement for sensitive personal information.

Data-driven advertising and marketing has been used to support the promotion and sale of products and services of all types for decades, even predating online data collection. It therefore should clearly be recognized as compatible with the collection of a consumer's personal information, as long as the data collection and use is reasonably necessary and proportionate to perform the advertising and marketing, is properly disclosed, and consumers have a right to object to this collection. However, in one of the illustrative examples, an online retailer collecting the personal information of shoppers would seemingly be prohibited from using a consumer's personal information to market other products to them without consent, even if this practice clearly disclosed at the point of collection.[18] At a minimum, the Agency should also make clear that the hypothetical online retailer would be permitted to market other businesses' products and services if such use was disclosed in the consumer notices required by the law.

[14] CAL. CODE REGS. tit. 11, 7002(a) (proposed).
[15] CAL. CIV. CODE § 1798.100(c)
[16] CAL. CODE REGS. tit. 11, 7002(a) (proposed).
[17] NAI Code § II.C.1.
[18] CAL. CODE REGS. tit. 11 § 7002(b)(4) (proposed).

- **NAI Recommendations:**

The proposed regulations should be amended to clarify that compatible purposes, when provided with notice in compliance with the requirements of 1798.100, are subject to the law's opt-out requirements, rather than creating a new opt-in requirement or a ban on compatible uses based on whether they may not meet an average consumer's expectation.

Amend Sec. 7002 as follows:

> (a) A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected. Whether a business's collection, use, retention, and/or sharing is reasonably necessary and proportionate, or compatible with the context, depends on several factors, including: the expectations of a reasonable consumer when providing their personal information; the nature and sensitivity of the personal information collected; and whether the business disclosed the use, retention, or sharing of personal information at the time it collected the personal information from the consumer. To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall obtain the consumer's explicit consent in accordance with Sec. 7004 before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that was not disclosed when the personal information was collected or is otherwise unrelated or incompatible with the purpose(s) for which the personal information was collected or processed.
>
> (b)(4) Business D is an online retailer that collects personal information from consumers who buy its products in order to process and fulfill their orders. Business D's provision of the consumer's name, address, and phone number to Business E, a delivery company, is compatible and related to the reasonable expectations of the consumer when this personal information is used for the purpose of shipping the product to the consumer. However, Business E's use of the consumer's personal information for the marketing of other businesses' products would not be necessary and proportionate, ~~nor compatible with the consumer's expectations~~ unless Business E provides appropriate notice to the consumer and provides the opportunity to opt out; such notice and subsequent use would constitute a compatible use. ~~Business E would have to obtain the consumer's explicit consent to do so.~~

IV. § 7012: Notice at Collection of Personal Information

We appreciate and concur with the regulations' explicit recognition of the third-party collection scenario, which is commonplace across the digital media industry, particularly for small publishers and other businesses that rely on third party businesses to provide tailored advertising services. However, the proposed regulations' requirements for notice at collection of personal information are unclear in instances where a first-party business engages and allows a third party to "control" the personal information of a consumer. We fear that if left as-is, the proposed regulations could be interpreted as a requirement for enhanced notice at collection of consumer data that is both unhelpful for consumers and impractical for businesses.

As currently drafted, the proposed regulations address these scenarios in two areas. First, the draft regulations direct applicable first-party businesses to include in their notices at collection "the names of all the third parties" that the first party allows to collect personal information from the consumer, *or* "[i]n the alternative, information about the third parties' business practices."[19] These alternatives are flexible and practical, providing multiple options to allow for consumers to be effectively informed regarding the collection of their data at the point of such collection, while also providing a pragmatic alternative for the business to achieve this outcome.

However, the proposed regulations create confusion by providing elsewhere that in cases where a first party allows another third-party business to control the collection, there is a choice for either the first party to "include in its notice at collection the names of all the third parties that the first party allows to collect personal information from the consumer," or in the alternative, for the third-party business controlling the collection of personal information "to provide the first party information about its business practices for the first party to include in the first party's notice at collection."[20] This provision could be interpreted to require that the choices available for businesses are for the first-party business to list *all* third parties collecting, or each and every third party to provide their own notice to the consumer, which in many cases is not practical, or even possible.

The outcome of requiring a first party to list all third parties would diverge from current practices under the CCPA and the intent of the CPRA as we understand it, and it would be cumbersome for consumers while providing limited practical value.[21] That is, it would not be substantially valuable or desirable for consumers to see a list of actual third parties, which they are not likely to know, understand, or distinguish between these companies. At the same time, such a requirement is not practical for businesses, particularly small publishers, who engage with a wide range of third-party partners and would regularly be required to update a list of each specific entity they are working with for each digital advertising partnership. Such a requirement is likely to encourage businesses to employ cookie banners and pop-up consent mechanisms that have been broadly panned by businesses and privacy advocates alike. Not only does the CPRA not embrace such an approach, there is no indication that the Agency sees this as reflecting sound policy.

- **NAI Recommendations:**

The NAI proposes the Agency clarify the alternative presented in the draft regulations (§ 7012 (g)(2)), making clear that the law's requirements can be satisfied by the first party providing the *types/categories* of third parties engaged in data collection, rather than having to list all of the third parties collecting personal information. Absent a practical interpretation for third party data collection notification, covered businesses, and particularly smaller publishers would face onerous and impractical obligations in reporting the names of all third-party data collectors, ultimately limiting choice for consumers. To accomplish this, we suggest the following amendment to the text of the implementing regulations.

Revise § 7012 as follows:

> (g)(2) A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include in its notice at collection the names of all the third parties that the first party allows to collect personal information from the consumer, or information about the types/category of third parties and their business practices. In the

[19] CAL. CODE REGS. tit. 11, § 7012(e)(6) (proposed)
[20] CAL. CODE REGS. tit. 11 § 7012(g)(2) (proposed)
[21] CAL CIV. CODE § 1798.115(a)(d).

alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection or if they have the opportunity, may elect to provide notice at collection directly to the consumer.

V. § 7026: Requests to Opt-Out of Sale/Sharing

The CPRA empowers consumers to express choices to businesses individually via a clearly labeled opt-out link directed specifically to those businesses. Additionally the CPRA provides for the opportunity for consumers to utilize Signals, which have the effect of automating opt-out requests, and therefore providing a default for all businesses with which they interact where the consumer does not provide an opt-in. However, these requests to opt out still *only* apply to the business with which the consumer is interacting, at the time, rather than extending to all of that businesses' partners.

As currently drafted, the proposed regulations threaten to extend beyond the statute, potentially also requiring businesses to send a chain of opt-out requests to other parties to which the business partners with and transfers personal information.[22] The NAI views it as inconsistent with the spirit and requirements of the CPRA for businesses to be required to notify "all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period."[23]

For example, a publisher that receives an opt-out request from a consumer can reasonably be expected to stop sharing that consumer's personal information with any partners they work with. The proposed regulations also accurately establish a first-party business' obligation to ensure that third parties who control collection of personal information on their digital property recognize and honor an opt-out or Signal. However, the regulations accidentally expand this requirement by mandating that a first-party publisher convey a consumer's opt-out choice to all of their partner businesses, and also requires those businesses to further recognize an opt-out request for that user. This could potentially also be wrongly construed to create a requirement for businesses to send opt-out requests to business that it no longer partners with, which wouldn't even be possible.

The CPRA by design enables a consumer to allow some businesses to share their personal information, while also preventing data processing or sharing by other businesses with which they have a different relationship, or specifically those who they do not trust. The proposed regulations' new flow down requirements directly contravene this.

With respect to consumer deletion requests, the CPRA takes a different approach, clearly requiring businesses to send these requests to contractors, service providers, and third parties.[24] The existence of the requirement to forward deletion requests to other parties while the same requirement is absent for opt-out requests further suggests that the CPRA does not intend to impose an opt-out flow down requirement on businesses.

---

[22] CAL. CODE REGS. tit. 11, §§ 7026(f)(2) & (3) (proposed).
[23] CAL. CODE REGS. tit. 11, §§ 7026(f) (proposed).
[24] CAL CIV. CODE § 1798.105(c)(1).

- **NAI Recommendations:**

The proposed regulations should be amended to clarify that businesses are not required to transmit opt-out requests to other parties. To accomplish this, we suggest the following amendment to the text of the implementing regulations.

Amend § 7026(f) (proposed) as follows:

> (f) A business shall comply with a request to opt-out of sale/sharing by:
>
> > (1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Providing personal information to service providers or contractors does not constitute a sale or sharing of personal information.
> >
> > (2) Ensuring that all third parties whom the business allows to control the collection of consumers' personal information on their digital property ,receive the consumer's opt-out request, and require them to honor that request and cease to sell and/or share with other third parties the consumer's personal information as soon as possible, but no later than 15 business days from the date the business receives the request.
> >
> > ~~(2) Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period.~~

VI. §§ 7051 & 7053: Contract Requirements for Service Providers, Contractors, and Third Parties

The NAI acknowledges and agrees with the objectives of the CPRA to ensure that Service Providers, Contractors, and third parties should be bound by clear contractual guidelines, including specifying the applicable "business purposes." However, we are concerned that the language in §§7051(a)(2) and 7053(a)(1) is overly prescriptive and could be interpreted in to require that businesses implement and maintain individual, customized contracts with all of their various service providers, contractors, and third party partners, for a set of business purposes that is consistent across a wide range of industry participants. This would be onerous, costly, and impractical for virtually all businesses, particularly small online publishers and advertisers that lack substantial legal and financial resources (and time) to negotiate and manage all of these contracts. This attention to creating and negotiating bespoke contracts, as a practical matter, also may come at the expense of attention to substantive compliance, which does not further the CPRA's goals.

Rather, the NAI encourages the CPPA to provide flexibility in the regulations for the use of standardized industry contracts that identify the specific permitted digital advertising activities, data use restrictions, data safeguards, and applicable business purposes when engaging in those activities. Significantly, this approach would also enable companies, and the CPPA, to more effectively perform due diligence and audits of digital advertising industry participants, rather than having to review and assess hundreds or likely thousands of individualized contracts across the industry. In short, this approach would appropriately balance the sensible goals driving the proposed rule with the practicalities of implementation.

- **NAI Recommendations:**

The proposed regulations should be amended to provide flexibility in the regulations for the use of standardized industry contracts that identify the specific permitted digital advertising activities, data use restrictions, data safeguards, and applicable business purposes when engaging in those activities.

Amend § 7051 as follows:

(a) The contract required by the CCPA for service providers shall:

(1) Prohibit the service provider or contractor from selling or sharing personal information it receives from, or on behalf of, the business.

(2) Identify the specific business purpose(s) and service(s) for which the service provider or contractor is permitted to process~~ing~~ personal information on behalf of the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. ~~The business purpose or service shall not be described in generic terms, such as referencing the entire contract generally.~~ The description shall be specific.

(3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations. ~~This section shall list the specific business purpose(s) and service(s) identified in subsection (a)(2).~~

(4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any commercial purpose other than the business purposes specified in the contract, including in the servicing of a different business, unless expressly permitted by the CCPA or these regulations.

(5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source, except for as expressly permitted by the CPRA as defined in Civil Code section 1798.140(e), or these regulations, whereby a service provider or contractor may combine personal information to perform limited business purposes.

(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to

protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(7) Grant the business or other party acting on its behalf, the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business's obligations under the CCPA and these regulations. ~~Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.~~

(8) Require the service provider or contractor to notify the business ~~no later than five business days~~ promptly after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(9) Grant the business or the party acting on its behalf, the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's or contractor's unauthorized use of personal information. ~~For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.~~

(10) Require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider or contractor to comply with the request.

(b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).

(c) A person who does not have a contract that complies with subsection (a) is not a "service provider" or a "contractor" under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with these requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.

(d) A service provider or contractor shall comply with the terms of the contract required by the CCPA and these regulations.

(e) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that does not conduct due diligence of its service providers and contractors ~~never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems~~ might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Revise § 7053 to the following:

(a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(1) Identifies the limited and specified purpose(s) for which the personal information is permitted to be sold or disclosed. ~~The purpose shall not be described in generic terms, such as referencing the entire contract generally.~~ The description shall be specific.

(2) Specifies that the business is disclosing the personal information to the third party only for the limited and specified purposes set forth within the contract and requires the third party to only use it for those limited and specified purposes set forth within the contract and requires the third party to only use it for those limited and specified purposes.

(3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses by, for example, only collecting and using personal information for purposes an average consumer would reasonably expect or other disclosed purposes compatible with the context in which it was collected, complying with a consumer's request to opt-out of sale/sharing forwarded to it by a first party business, providing the required disclosures identified in section 7010, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(4) Grants the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information that it received from, or on behalf of the business, in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest to their compliance with subsection (a)(3).

(5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. For example, the business may require the third party to provide documentation that verifies that they no longer retains or uses the personal information of consumers who have had their request to ~~opt-out of sale/sharing~~ delete their personal information forwarded to them by the first party business.

(6) Requires the third party to notify the business ~~no later than five business days~~ promptly after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(b) A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party's own purposes, shall contractually require the third party to check for and comply with a consumer's opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information.

(c) A third party that does not have a contract that complies with subsection (a) shall not collect, use, process, retain, sell, or share the personal information received from the business.

(d) A third party shall comply with the terms of the contract required by the CCPA and these regulations.

(e) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that does not conduct due diligence ~~never enforces the terms of the contract~~ might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

VII. Audits and Enforcement

While the CPRA grants broad audit authority to the Agency,[25] the proposed regulations do little to clarify the scope and process of such audits. Expanding on our CPRA Preliminary Comments[26], the NAI recommends reasonable boundaries on CPPA audit capabilities. The following recommendations would ensure predictability and practicality for businesses of all sizes operating in California, while also providing for the most efficient and streamlined use of Agency resources.

A. Use of Independent, Third-Party Auditing

The Agency should implement regulations providing that an announced or unannounced audit, pursuant to Sec. 7304 of the proposed regulations, may be conducted by independent third-party auditors. As stated in our CPRA Preliminary Comments, we again recommend that:

> *"businesses should retain the ability to either select independent third-party auditors of their choice in accordance with a set of qualifications established by the Agency or to conduct internal audits provided there are policies and other safeguards in place to ensure independence. On the latter point, California law already contemplates the ability of companies to conduct independent yet internal audits in the insurance context."* [27]

Specifically, we recommend that the agency allow for recognized third party auditors, at the election of the business that the agency seeks to audit, to conduct an audit of the business, or to submit results of a previously conducted audit voluntarily performed by the business. This approach would ensure consistency and predictability across audit types, and correspond with the annual cybersecurity audits required by the CPRA to be performed independently.[28] For businesses faced with multiple data audits per year, whether regarding cybersecurity measures or general data privacy, interfacing with the same third-party auditor would provide for familiarity, and thus a quicker and more efficient investigation overall. Furthermore, leveraging third-party independent auditors for any audit would also be less resource-intensive for the CPPA as an agency, freeing up valuable limited

[25] *See* CAL. CIV. CODE § 1798.185(a)(18).
[26] *See Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act*, NETWORK ADVERTISING INITIATIVE (2021), https://thenai.org/preliminary-comments-on-proposed-rulemaking-under-the-california-privacy-rights-act/
[27] *Id.* at 4. (citing CAL. INS. CODE §900.3 (2021))
[28] *See* CAL. CIV. CODE § 1798.185(a)(15)(a) (Providing that Agency regulations shall require cybersecurity audits "on an annual basis" and establish a process "to ensure that audits are thorough and independent.").

resources for the Agency to ensure compliance broadly, rather than getting bogged down in a lengthy, overly labor-intensive audit process.

B. Limit Audit Selection Criteria

As to the scope of the audits, the NAI recommends the Agency limit the criteria for selection only to *suspected violations of substantive provisions of the CCPA*, rather than a "history of noncompliance" with "any other privacy protection law."[29] The currently proposed language is overly broad, and may encompass privacy laws that do not generally apply to businesses within California, such as the European General Data Protection Regulation ("GDPR") or other state privacy laws in Virginia, Colorado, Utah, or Connecticut. Limiting the scope to suspected CCPA provisions will provide predictability for businesses, and also will allow the CPPA to enforce its own regulations, utilizing its expertise most effectively.

However, if a history of noncompliance with other privacy protection laws is to remain, the regulations should make clear in Sec. 7304(b) that the scope of this criteria only includes other *California* privacy laws, or federal privacy laws that give enforcement authority to California Attorney General, such as COPPA or HIPAA.[30] Without such a distinction, complying with inapplicable laws outside of California, for fear of an audit, may become impracticable for smaller businesses already struggling to compete in the digital marketing ecosystem.

C. Implement Clear, Pre- and Post-Audit Processes

The proposed regulations provide the Agency with fairly wide latitude to conduct audits on its own initiative, "announced or unannounced."[31] This potential for unannounced audits, without clear guidelines, may prove overly burdensome for both the Agency and the business being audited. The NAI thus encourages the Agency to add pre and post-audit processes to the proposed regulations, such as clarifying how the selection process might work[32] and requiring the opportunity for a "meet and confer" prior to any next steps.[33] A guaranteed "meet and confer" process, following the announcement of a formal investigation, for example, would allow for Agency personnel to further clarify the scope and next steps for the business involved. On the other side, the business personnel would also have an opportunity to resolve any uncertainties the Agency might have about its data collection practices. Altogether, this type of required process would prove conducive to an efficient and collaborative rollout of the new regulations.

When it comes to the language pertaining to the recommended measures above, the NAI again encourages the Agency to look to Federal Trade Commission regulations, and incorporate language requiring "sufficient definiteness and certainty" to any questionnaires or responses requested as part of an audit or investigation; to prescribe a reasonable deadline; and to identify an Agency or

---

[29] CAL. CODE REGS. tit. 11, § 7304(b) (proposed)
[30] 15 U.S.C. § 6504; 42 U.S.C. § 1320d-5
[31] CAL. CODE REGS. tit. 11 § 7304(c) (proposed)
[32] On its website, the U.S. Dept. of Health and Human Services made clear its audit pool sampling process for HIPAA compliance review in 2016-17. Interested parties could review the information to locate audit timelines, understand selection criteria, and fill out a pre-screening questionnaire. *See* U.S. DEPT. OF HEALTH AND HUMAN SERVICES, HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION AUDIT PROGRAM (2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html. Clarity like this would be useful for California businesses concerned about the scope of a potential CPPA Audit.
[33] *See* 16 CFR 2.7(k) (describing the required "meet and confer" process for Federal Trade Commission investigations). Businesses might already be familiar with this Federal process, and would benefit from consistency with California regulations.

independent custodian "to whom such reports or answers to questions shall be submitted."[34] In addition to the pre and post-audit processes themselves, this recommended language would make sure audits and investigations remain consistent, clear, and limited in scope, further ensuring a predictable process for all parties involved.

- **NAI Recommendations:**

The proposed regulations should be amended to permit the use of independent, third parties for required audits. Additionally, the NAI proposes the Agency clarify audit scope and implement additional guidelines for the audit process.

Revise Sec. 7304 (proposed) to the following:[35]

> (a) Scope. The Agency may require an audit of a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.
>
> (b) Performance. Audits may be performed by recognized third party auditors, at the election of the business that the Agency seeks to audit. For the purposes of this section, results from a previous audit voluntarily undertaken by the business also may be acceptable, to the extent that the audit was completed within the prior 12 months.
>
> (~~b~~c) Criteria for Selection. The Agency may ~~conduct~~ require an audit to investigate possible violations of the CCPA. Alternatively, the Agency may ~~conduct~~ require an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law~~.~~that the California Attorney General has the authority to enforce.
>
> (~~c~~d) Audits may be announced or unannounced as determined by the Agency. The Agency shall publish and maintain on its website a timeline for the audit process. The website shall also provide information about its selection process.
>
> (e) Agency demands for written responses or other material, as part of an audit, shall include sufficient definiteness and certainty as to permit such material to be fairly identified, prescribe a reasonable return date providing a reasonable period of time within which the material so demanded may be assembled and made available for inspection and copying or reproduction, and identify the Agency's custodian to whom such material shall be made available.
>
> (f) Post Audit. The Agency shall meet and confer with business staff prior to any next steps by the Agency, including enforcement and investigation proceedings, to discuss compliance and to address and attempt to resolve any issues or uncertainties that arise from the audit. The meet and confer session may be in person or virtual.
>
> (~~d~~g) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.

[34] 16 CFR 2.7(b)(3)
[35] Revisions (e) and (f) of the recommendations in this section rely heavily on existing language in 16 CFR 2.7 pertaining to Federal Trade Commission investigations.

(eh) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq.

VIII. Conclusion

Again, the NAI appreciates the opportunity to submit comments to the Agency on the proposed regulations for the CPRA. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at leigh@thenai.org, or David LeDuc, Vice President, Public Policy, at david@thenai.org.

*****

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)