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

**RE: Cross-Industry Advertising Trade Association Comments on the Modified Text of Proposed Regulations to Implement the California Privacy Rights Act of 2020 – CPPA Public Comment**

Dear Privacy Regulations Coordinator:

On behalf of the thousands of brands, publishers, agencies and ad technology companies in our membership that represent the advertising industry, we provide the following comments in response to the California Privacy Protection Agency's ("CPPA" or "Agency") November 3, 2022 request for public comment on the modified text of proposed regulations to implement the California Privacy Rights Act of 2020 ("CPRA").[1] We and the companies we represent, many of which do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We appreciate the Agency's incorporation of certain input we provided during the 45-day comment period into the modified text of proposed rules. In this comment letter, we provide the Agency with further input and suggested changes to discrete proposed regulatory provisions to help ensure implementing regulations are consistent with the law and protect consumers while remaining workable for the business community.

We remain concerned that several provisions in the proposed regulations contravene the clear text of the CPRA. We addressed some of those concerns in our response to the Agency's initial request for comment on the proposed regulations. We renew several of those concerns—particularly with respect to the quickly approaching CPRA enforcement start date in the absence of finalized regulations; Section 7050; and the proposed opt-out icon—in **Appendix A**. Additionally, in October 2022, we sent a letter to the Agency detailing some of our concerns related to opt-out preference signals and necessary and proportionate data processing requirements in the proposed rules. We advocated that the CPPA not advance those controversial regulatory provisions through an abridged or accelerated "consent agenda" process. That letter is attached hereto as **Appendix B**. We discuss the points made therein, as well as an additional issue related to legal defenses under Section 7051(c), in more detail in the sections that follow below.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country ranging from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.[2] Our group has more than a decade's worth of hands-on experience regarding matters related to consumer privacy and controls. We welcome the opportunity to engage with you in this process to develop practical regulations to implement the CPRA.

---

[1] California Privacy Protection Agency, *Notice of Modifications to Text of Proposed Regulations* (Nov. 3, 2022), located here. *See also* California Privacy Rights Act of 2020, located here (hereinafter, "CPRA").
[2] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located here (hereinafter, "Deighton & Kornfeld 2021").

## I. The Modified Proposed Regulations' "Necessary and Proportionate" Requirements Should Be Amended To Align with the CPRA's Text.

The "necessary and proportionate" data processing requirements in Section 7002 of the modified text of proposed regulations contradict the CPRA's text. Section 7002 should be revised to implement the statute's plain language and intent.

The modified proposed rules would completely eliminate the important, intended, and statutorily prescribed role of consumer notice within the CPRA framework. Instead of permitting businesses' disclosures to consumers to determine necessary and proportionate data use as set forth in the CPRA, the modified proposed rules would require businesses to engage in a convoluted multi-factor analysis to determine whether certain data processing activities are permissible.[3] If a proposed processing purpose does not adequately satisfy the factors, a business would be required to obtain consumer consent for data processing. In direct contrast to this rule, the CPRA itself sets forth an opt-out approach to *certain* data processing activities and does not mandate consumer consent for all data processing. And yet, Section 7002 suggests that the statutory opt-out approach could be converted to an opt-in requirement with all of the concomitant challenges associated with such a regime, such as the consent fatigue and anti-competitive concerns associated with the EU's General Data Protection Regulation ("GDPR").[4] Section 7002 of the modified proposed rules thus turns the CPRA's approach on its head, is contrary to the law's text, and diametrically opposes the privacy framework that California voters directly approved when they approved the CPRA ballot initiative.

### A. Section 7002 Should Be Modified to Permit Data Processing Described in Consumer Disclosures Instead of Requiring a Subjective Multi-Factor Analysis.

In addition to several other factors, the modified proposed rules would require businesses to consider the "reasonable expectation of the consumer" to determine whether data processing is permitted. The modified proposed rules then provide examples of activities that would or would not meet this standard without referencing any basis for those conclusions, such as consumer testing or research, or even real-world observations of actual consumer behavior. This "reasonable expectation of the consumer" consideration, along with the other factors articulated in the modified proposed rules, would require businesses to make similar amorphous and highly subjective determinations about allowed processing activity. It also vests in the Agency a high level of subjectivity which is likely not to have been contemplated by the voters or by the California APA. In contrast, the CPRA itself provides clear standards for permissible data processing tied to consumer notice. The CPRA specifically allows businesses to process data for uses described in their privacy notices, including uses that are consistent and compatible with the businesses' disclosures.[5] The CPRA explicitly articulates highly specific standards for consumer disclosures related to the type of personal information processed, the purpose(s) for processing, the categories of entities to which personal information is sold or shared, and the sources of personal information. These specific disclosure requirements were included in the law to ensure businesses act in furtherance of the CPRA's stated purposes of helping consumers "become more informed counterparties in the data economy, and promot[ing] competition."[6] The modified proposed regulations ignore the important and statutorily provided role of consumer notice plays in the law and substitute the Agency's views of how the CPRA text *should* read rather than honoring and furthering the letter of the law itself.

---

[3] Cal. Code Regs. tit. 11, § 7002 (proposed).
[4] *See* Kate Fazzini, *Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators* (May 5, 2019) located here.
[5] CPRA, Cal. Civ. Code § 1798.100(c) (effective Jan. 1, 2023).
[6] *Id.* at § 2(G).

The modified proposed regulations run counter to the CPRA's text and purpose by requiring businesses to engage in a highly subjective analysis in order to proceed with data processing that has already been disclosed to consumers according to the CPRA's notice requirements.[7] Such an approach would stifle innovation by subjecting product and service innovation to consent, which is not workable. The factor-based test would also require businesses to presuppose preferences according to each consumer's perceived "reasonable expectations," resulting in diminished choice and autonomy for consumers. The CPRA does not envision this sort of framework, but instead strives to leverage consumer disclosures to educate consumers so they can make meaningful choices about how personal information is processed.[8]

Instead of issuing regulations that plainly contradict the CPRA, the Agency should permit controllers to process personal data in line with the specified processing purposes disclosed to consumers.[9] Only when a controller wishes to process personal data for purposes that are undisclosed should the business be required to consider a series of factors to determine if such processing is permissible.[10] This approach provides much more clarity to businesses and consumers alike, as it relies on bright line, clear consumer disclosures to define the permissible purposes for data processing. Additionally, such an approach would align with the CPRA, which permits data processing if the processing is adequately disclosed to the consumer and provides an opt-out structure for certain processing activities rather than requiring consumer consent.

### B. Amending Section 7002 To Permit Processing In Line With Disclosures Would Prevent Converting the CPRA's Opt-Out Structure Into an Opt-In Framework.

The CPRA clearly permits data processing that aligns with businesses' disclosures to consumers. It also allows for consumers to opt out of certain data processing activities. The law itself does not require businesses to engage in subjective, multi-factor analyses to determine if they may process data in certain ways. The CPRA also sets forth an opt-out structure for certain data processing and does not require consumer consent. Section 7002's consent requirements would consequently completely convert the fundamental opt-out structure of the CPRA into an opt-in law; this would not further the intent and purpose of the statute. Moreover, by requiring businesses to make decisions about data processing that would be "necessary and proportionate" according to each consumer's "reasonable expectations," the modified proposed regulations inject an unnecessary and unhelpful level of ambiguity into businesses' ability to determine whether certain data processing is permissible. The CPRA itself puts autonomy in the hands of consumers by placing the responsibility on businesses to inform and educate, not gate-keep by eliminating consumer choices altogether. The modified proposed regulations should be revised to ensure businesses can process personal information in line with CPRA-compliant consumer disclosures without requiring an unnecessarily chilling and uncertain multi-factor analysis to determine permissible data processing. Accordingly, Section 7002 of the modified regulations should be updated to align with the CPRA and avoid reaching beyond its mandates.

## II. The Modified Regulations Should Follow the CPRA by Clarifying That Opt-Out Preference Signals Are Optional, Implementing Statutorily Required Safeguards to Authenticate Signals, and Providing Technical Specifications for Signals.

The CPPA should align the regulatory text surrounding opt-out preference signals with the CPRA itself. Prior to finalizing the regulations, the Agency should also take steps to promulgate rules

[7] Cal. Code Regs. tit. 11, §§ 7002(b), (c) (proposed).
[8] *See* CPRA, § 2(G) (effective Jan. 1, 2023)..
[9] Colo. Regs. 6.08A, located here (proposed).
[10] *Id.* at 6.08(C).

to further several key safeguards for such signals, as well as to define technical specifications for the signals so businesses know how to recognize and implement the opt-out signals they may receive, as discussed in **Appendix B**. The CPPA should also take steps to help standardize opt-out preference signal tools so businesses and consumers understand which tools meet the requirements of law. As presently drafted, the regulatory text directly contravenes the CPRA by making adherence to opt-out preference signals mandatory, and it ignores clear requirements for the Agency to promulgate specific regulations addressing safeguards and technical specifications for opt-out preference signals.

### A. The CPRA Makes Opt-Out Preference Signals Optional.

The CPRA clearly states that businesses "may elect" to comply with opt-out preference signals or include a clearly labeled opt-out link in the footer of their websites.[11] The modified proposed rules contradict this statutory language by stating that processing such signals is mandatory.[12] The modified proposed regulations ignore clear language in the law that makes opt-out preference signals optional. Instead, the modified proposed rules suggest that a business is mandated to honor opt-out preference signals in either a "frictionless" or "non-frictionless manner," terms that are not in the text of the CPRA itself.[13] The modified regulations' "frictionless" standard is extra-legal, as it is not supported by the text of the CPRA; it directly contravenes the law, which clearly makes adherence to opt-out preference signals optional.

To support making adherence to opt-out preference signals mandatory, the Agency's Initial Statement of Reasons ("ISOR") for the proposed rules cites the regulatory authority given to the Agency in Section 1798.185(a)(20) of the CPRA.[14] According to the ISOR, adherence to opt-out preference signals is mandatory because the statute gives the Agency authority to issue rules governing how a business may provide consumers with an opportunity to subsequently consent to sales or sharing of personal information.[15] This reasoning does not describe why the Agency has gone beyond the plain text of the law by instituting a mandatory standard instead of the clear, optional choice the CPRA envisions with respect to such signals. Moreover, it entirely ignores the fact that the regulatory directive in Section 1785.185(a)(20) itself even acknowledges that adherence to opt-out preference signals is optional. According to that section, the Agency must issue "regulations to govern how a business ***that has elected*** to comply with subdivision (b) of Section 1798.135," the subdivision that describes opt-out preference signals, "responds to the opt-out preference signal."[16] By making adherence to opt-out preference signals mandatory, the Agency has ignored the clear text of the CPRA. The Agency should rewrite its opt-out preference signal regulations to reflect the CPRA's provisions, which explicitly give businesses a choice to process such signals ***or*** offer a clearly labeled opt-out link in the footers of their websites.

### B. The CPRA Requires the Agency to Address Key Safeguards and Technical Specifications for Opt-Out Preference Signals.

The Agency's proposed opt-out preference signal rules fail to implement key provisions of the CPRA that require the CPPA to set guardrails around the development of optional opt-out preference signals and provide technical standards for such signals to clarify developers' design obligations. The CPRA specifically tasks the Agency with "issuing regulations to define the requirements and *technical*

[11] CPRA, Cal. Civ. Code § 1798.135(b)(3) (effective Jan. 1, 2023).
[12] Cal. Code Regs. tit. 11, §§ 7025(b), (e) (proposed).
[13] *Id.* at § 7025(e).
[14] California Privacy Protection Agency, *Initial Statement of Reasons* at 34-35, located here.
[15] *Id.*
[16] CPRA, Cal. Civ. Code § 1798.185(a)(20) (effective Jan. 1, 2023) (emphasis added).

*specifications* for an opt-out preference signal," which would ensure the signal meets several safeguards: the signal (1) cannot unfairly disadvantage certain businesses in the ecosystem; (2) must be clearly described; (3) must clearly represent a consumer's intent and be free of defaults presupposing such intent; (4) must not conflict with commonly-used privacy settings consumers may employ; (5) must provide a mechanism for consumers to consent to sales or sharing without affecting their preferences with respect to other businesses; and (6) must provide granular opt-out options for consumers.[17] Not one of these key safeguards—which are explicitly in the text of the CPRA and which the Agency is instructed to effectuate via regulations—is addressed in the proposed rules, nor are there any proposed rules that would define technical standards for opt-out preference signals. These safeguards and technical specifications are necessary to clarify how developers must construct opt-out preference signal tools.

As written, the modified proposed regulations would create widespread confusion, because they do not clarify how opt-out preference signals can meet the safeguards requirements that are set forth in law, and they do not clarify how businesses can technically implement the ability to receive opt-out preference signals. Moreover, the modified proposed rules inject additional uncertainty into the opt-out preference signal requirements by adding an unnecessary reference to "pseudonymous profiles." This is new term that is not defined by the CPRA or the proposed regulations.[18] In this way and others, the modified proposed regulations do not set forth clear directives related to opt-out preference signals, call for any standardization of such signals, or specify how businesses are to know which opt-out signals are valid under the statute. Effectuating new signals will be a development project for many organizations, which requires months of lead time. Without sufficient lead time and specificity regarding which signals are to be respected, organizations will be left guessing or subject to security risks or consumer dissatisfaction when the mechanism does not work or is not seamlessly integrated into the online experience, thus opening up well-intentioned efforts to unnecessary liability.

### C. The Agency Should Maintain a List of Approved Opt-Out Preference Tools to Reduce Consumer and Business Confusion.

To help clarify which in-market opt-out preference tools meet the requirements of the CPRA (*i.e.*, are not set by default, do not disadvantage certain businesses or models of others, etc.), the Agency should maintain a public list of recognized mechanisms that have met legal standards.[19] Such a centralized repository of approved signals would benefit consumers and businesses alike. Consumers would be able to understand which opt-out preference signals are approved by the Agency and thus represent a control mechanism that must be given effect by businesses. In turn, businesses would gain clarity regarding which opt-out preference signals they must honor instead of having to constantly monitor the Internet for any in-market mechanism and independently validate or check its legality. Such a list would reduce the need for businesses to guess which signals are true expressions of consumer choice.

Regulations furthering the CPRA's opt-out preference signal safeguards are necessary to ensure businesses can verify that the signal, or the "mechanism" or "tool" that provides the signal, has complied with various requirements under the CPRA, including those related to presentation of choices, default settings, disadvantages to businesses, and reflection of consumer intent. Similarly, technical specifications would help developers understand their design obligations with respect to opt-out preference signal tools. The Agency must first address these statutory requirements concerning mechanisms that set opt-out preference signals before adopting regulations related to honoring such

[17] *Id.* at § 1798.185(a)(19)(A).
[18] Cal. Code Regs. tit. 11, §§ 7025(c)(1), (2) (proposed).
[19] *See* Colo. Regs. 5.07, located here (proposed).

signals. Guidance from the Agency to govern the mechanisms used to set signals is necessary to ensure such tools are offered in compliance with law and so businesses receiving such signals can be assured that the signals are legally set consumer preferences.

## III. Businesses Should Be Required to Conduct Due Diligence of Service Providers and Contractors Only If They Reasonably Believe Such Entities Are Misusing Personal Information.

The modified proposed regulations in Section 7051(c) states that a business "might" not be permitted to rely on a defense that it did not have reason to believe a service provider or contractor intends to use personal information in violation of the CCPA if the business does not enforce the terms of its contracts or exercise rights to audit or test service providers' and contractors' systems.[20] This provision would create significant costs for businesses without providing any real benefit to consumers. If left unchanged, the provision could effectively force businesses to audit and test every one of their partners' systems, thereby creating immense costs and the anticompetitive result of businesses limiting the number of service providers or contractors with which they do business. A better approach would be to rewrite the draft regulation to make clear that a business may not be permitted to avail itself of the defense if it *has reason to believe* a service provider or contractor is using personal information in violation of the CCPA and the business does not take steps to investigate that belief. The proposed rules should be updated to encourage businesses to take steps to exercise diligence when they have reason to believe a partner is using personal information in violation of the CCPA or the applicable contract.

## IV. Sufficient Consideration Should Be Given to the Data-Driven and Ad-Supported Online Ecosystem That Benefits California Residents and Fuels Economic Growth.

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A recent study found that the Internet economy's contribution to the United States' GDP grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.[21] In 2020 alone, it contributed $2.45 trillion to the U.S.'s $21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of $300 billion.[22] Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.[23] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.[24] The same study found that the ad-supported Internet supported 1,096,407 full-time jobs across California, more than double the number of Internet-driven jobs from 2016.[25]

### A. Advertising Fuels Economic Growth.

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulations that significantly hinder certain

[20] Cal. Code Regs. tit. 11, § 7051(c) (proposed).
[21] Deighton & Kornfeld 2021 at 5.
[22] *Id*.
[23] *Id*.
[24] *Id*. at 6. *See also* Digital Adverising Alliance, *Summit Snapshot: Data Drives Small-and Mid-sized Business Online, It's Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located here.
[25] *Compare* Deighton & Kornfeld 2021. at 121-123 (Oct. 18, 2021), located here *with* John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem,* INTERACTIVE ADVERTISING BUREAU, 106 (2017), located here (finding that Internet employment contributed 478,157 full-time jobs to the California workforce in 2016 and 1,096,407 jobs in 2020).

advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.[26] One recent study found that "[t]he U.S. open web's independent publishers and companies reliant on open web tech would lose between $32 and $39 billion in annual revenue by 2025" if third-party tracking were to end "without mitigation."[27] That same study found that the lost revenue would become absorbed by "walled gardens" or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.[28] Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated $15.5 billion in revenue.[29] Data-driven advertising has thus helped to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

### B. Advertising Supports Californians' Access to Online Services and Content.

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content that publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information. Advertising revenue is an important source of funds for digital publishers,[30] and decreased digital advertising budgets directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[31] In fact, consumers valued the benefit they receive from digital advertising-subsidized online content at $1,404 per year in 2020—a 17% increase from 2016.[32] Regulatory frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such regulatory frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

### C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media.

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desires relevant ads, and a significant majority (86 percent) desires tailored discounts for online products and services.[33] Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers

---

[26] *See* John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located here (hereinafter, "Deighton 2020")
[27] *Id.* at 34.
[28] *Id.* at 15-16. *See also* Damien Geradin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech*, EUROPEAN COMPETITION JOURNAL (Dec, 18, 2020), located here.
[29] Deighton 2020 at 28.
[30] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located here.
[31] *See* John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located here.
[32] Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at $1,400/Year; Annual Value Jumps More Than $200 Since 2016* (Sept. 28, 2020), located here.
[33] Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located here.

must pay for most content.[34] Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[35]

## V. Conclusion

During challenging societal and economic times such as those we are experiencing, laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the free and low-cost content we consume over the Internet is powered by open flows of information supported by advertising. We therefore respectfully urge you to carefully consider the proposed regulations' potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy as you continue to refine the draft rules.

* * *

Thank you in advance for your consideration of this letter.

Sincerely,


Christopher Oswald
EVP, Government Relations
Association of National Advertisers
202-296-1883

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322


CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

[34] Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located here.
[35] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located here.

## APPENDIX A

### Additional Concerns Regarding the Modified Proposed Regulations to Implement the CPRA

### I. The CPPA Should Delay Enforcement for One Year Following Finalization of Regulations.

As noted in our prior filings, the CPRA requires the Agency to finalize regulations implementing the law by July 1, 2022, providing businesses a full calendar year to ensure compliance before enforcement would begin on July 1, 2023.[36] Unfortunately, the statutorily-required date for finalized rules has long passed; regulations are still being developed nearly six months after the July 1, 2022 deadline. In addition, even once the Agency completes its rulemaking process, finalization of regulations is contingent on satisfactory review by the California Office of Administrative Law ("OAL").[37] Given the California Administration Procedure Act's ("CA APA") rolling effective dates for regulations, OAL-approved regulations may not be finalized until 2023.[38] Thus, business stakeholders not only remain uncertain about what measures may be needed to comply with forthcoming final regulations, but also may face an impossibly tight compliance deadline before the Agency begins enforcement. The potentially very late publication of the final rules may also confuse consumers who will be given a much shorter ramp up time to learn about how take advantage of their rights in line with the new rules' procedures. The companies we represent are eager to ensure compliance with forthcoming final regulations, but as the CPRA's statutory timeline acknowledged, will need sufficient time to do so.

Given the ongoing rulemaking process and the additional requirements of the CA APA, the Agency should wholly align with the CPRA by stating expressly in final regulations that it will not pursue enforcement until one year after regulations are finalized. We appreciate the Agency's acknowledgement that it will consider the "amount of time" between statutory and regulatory effective dates and the dates of alleged violations in determining whether to pursue investigatory actions.[39] An additional definitive statement in the regulations explicitly committing the Agency to delay enforcement for one year would not only align with the CPRA, but also would provide needed clarity for business and consumer stakeholders.

### II. Section 7050(b) is Duplicative of the CPRA and Should Be Removed From the Modified Proposed Regulations.

Because Section 7050(b) of the modified proposed regulations merely restates the CPRA and provides no additional clarity, the section should be removed. Section 7050(b) of the modified proposed regulations reaffirms the CPRA's text, which prohibits companies from offering cross-context behavioral advertising services to businesses while occupying the "service provider" role.[40] Section 7050(b) of the modified proposed regulations simply reiterates the law, which plainly permits entities to provide advertising and marketing services to businesses as "service providers," and even permits them to combine personal information for advertising and marketing purposes in some circumstances so long as they do not "combine the personal information of opted-out consumers that the service provider… receives from, or on behalf of, the business with personal information that the service provider receives from, or on behalf of, another person or persons or collects from its own

[36] CPRA, Cal. Civ. Code § 1798.185(d) (effective Jan. 1, 2023).
[37] Cal. Gov't. Code §§ 11349.1, 11349.3.
[38] *Id.* at § 11343.4.
[39] Cal. Code Regs. tit. 11, § 7301(b) (proposed).
[40] CPRA, Cal. Civ. Code § 1798.140(e)(6) (effective Jan. 1, 2023).

interactions with consumers."[41] The text used in Section 7050(b) of the modified proposed regulations is virtually identical to the text of the CPRA on this point. Because the modified proposed regulation restates the CPRA provision explaining that an entity may provide advertising and marketing services as a service provider, but may not engage in cross-context behavioral advertising (the targeting of advertisements to consumers based on personal information combined from multiple businesses),[42] Section 7050(b) adds no additional clarity to the CPRA and should thus be removed from the modified proposed regulations.

## III. The Modified Proposed Regulations Should Permit Businesses to Leverage Existing In-Market Icons and Choice Mechanisms.

Under the CPRA, businesses are permitted to offer a "single, clearly-labeled link" to enable consumers to easily opt out of the sale or sharing of personal information and limit the use or disclosure of sensitive personal information instead of posting separate 'Do Not Sell or Share My Personal Information' and 'Limit the Use of My Sensitive Personal Information' links."[43] The proposed rules would require the title for that "Alternative Opt-out Link" to be "Your Privacy Choices" or "Your California Privacy Choices," and would require it to direct a consumer to a webpage that enables them to make choices to opt out of sales, opt out of sharing, and limit the use and disclosure of sensitive personal information.[44] For entities that use such an Alternative Opt-out Link," the proposed regulations would require them also to include the following graphic adjacent to the link:

The proposed graphic icon is confusing. Its inclusion of just one check mark and one "x" suggests just *one choice* will be made via the alternative opt-out link, when in reality the link would provide consumers the ability to make three choices: (1) the choice to opt out of personal information sales; (2) the choice to opt out of personal information sharing; and (3) the choice to limit the use and disclosure of sensitive personal information. The study used to support the use of the Agency's chosen icon found that several different icons (including the DAA Privacy Rights Icon) performed roughly the same when paired with a text link.[45] The market should be permitted to determine icons that work best to facilitate awareness and effectuation of rights for consumers. The CPPA should remove the prescriptive opt-out icon requirement and instead allow the marketplace to continue to leverage new and existing, widely deployed iconography provided the mandatory language for the link—"Your Privacy Choices" or "Your California Privacy Choices"—is present.[46]

* * *

[41] *Id*.
[42] *Id*. at § 1798.140(k).
[43] CPRA, Cal. Civ. Code 1798.135(a)(3) (effective Jan. 1, 2023).
[44] Cal. Code Regs. tit. 11, §§ 7015(b) & (c) (proposed).
[45] Lorrie Faith Cranor, et. al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* at 27 (Feb. 4, 2020), located here.
[46] *See, e.g.,* Digital Advertising Alliance, *YourAdChoices*, located here.

**APPENDIX B**

October 19, 2022

Chairperson Jennifer M. Urban
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Chris Thompson
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Lydia de la Torre
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Vinhcent Le
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Alastair Mactaggart
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Executive Director Ashkan Soltani
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

**RE: Joint Ad Trade Comments on the CPPA's Proposed Consent Agenda to Resolve "Non-Controversial" Issues in the CPRA Rulemaking Process**

Dear California Privacy Protection Agency Board Members and Executive Director Ashkan Soltani:

On behalf of the advertising industry, we respectfully urge the California Privacy Protection Agency ("CPPA" or "Agency") to decline to consider or approve certain controversial regulatory provisions through a "consent agenda" process to expedite the proposed regulations implementing the California Privacy Rights Act of 2020 ("CPRA"). During the CPPA's September 23 meeting, the Agency expressed interest in placing certain regulatory provisions on a consent agenda for "non-controversial" issues. Shortly thereafter, the Agency published modified proposed regulations to implement the CPRA.[1] There are several issues in the modified proposed regulations that are controversial and unsettled, and therefore should not qualify for any potential consent agenda. Specifically, the following two areas are particularly in need of further discussion and consideration, as they were not addressed by the modifications to the proposed regulations and remain controversial:

I. Proposed regulations related to opt-out preference signals are missing statutorily mandated safeguards; and

II. Consumer notice should fulfill the CPRA's "necessary and proportionate" requirements rather than tying "necessary and proportionate" processing requirements to "average " or "reasonable" consumer expectations.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country and in California. These companies range

[1] CPPA, *Modified Text of Proposed Regulations*, located here.

from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.[2] Our group has more than a decade's worth of hands-on experience relating to matters involving consumer privacy and controls. We and the companies we represent, many of whom do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We have participated in every proceeding under this CPRA rulemaking, including filing comments in response to the initial draft of proposed regulations. We welcome the opportunity to continue to engage with you to develop regulations to implement the CPRA.

## I. The Issue of Opt-Out Preference Signals Is Unfit for a Potential Consent Agenda Given Outstanding and Unaddressed Statutorily Required Safeguards

As the current proposed regulations do not address important statutory safeguards for opt-out preference signals that the CPRA requires, the issue of opt-out preference signals remains controversial and should not be summarily settled via consent agenda consideration. Under the CPRA, the Agency *must* promulgate specific rules to define the scope and form of opt-out preference signals. Specifically, the regulations must "define the requirements and technical specifications for an opt-out preference signal . . . The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should" ensure the signal meets several safeguards: (1) avoids unfairly disadvantaging certain businesses or business models over others in the ecosystem, (2) is clearly described; (3) clearly represents a consumer's intent and does not employ defaults that presuppose such intent; (4) does not conflict with commonly-used privacy settings consumers may employ; (5) provides a mechanism for consumers to consent to sales or sharing without affecting their preferences with respect to other businesses; and (6) provides granular opt-out options for consumers.[3]

The statute requires CPRA implementing regulations to include such safeguards while "considering the legitimate operational interests of businesses."[4] However, such technical specifications and safeguards appear nowhere in the current proposed regulations.[5] If the Agency has not resolved where it stands on these statutorily mandated details or made them available for review by interested parties, the issue of opt-out preference signals cannot fairly be considered undisputed or proper for a consent agenda.

The lack of clarity about opt-out preference signals is further exacerbated by a possible truncated window between finalized CPRA implementing regulations and their enforcement date. The CPRA tasks the Agency with finalizing the regulations implementing the law by July 1, 2022, but unfortunately this deadline passed without the Agency issuing final regulations.[6] Yet,

---

[2] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located here (hereinafter, "Deighton & Kornfeld 2021").
[3] Cal. Civ. Code § 1798.185(a)(19)(A) (effective Jan. 1, 2023).
[4] *Id.* at § 1798.185(a)(19)(C).
[5] *See, e.g.,* Cal. Code Regs. tit. 11, § 7025 (proposed).
[6] Cal. Civ. Code § 1798.185(d) (effective Jan. 1, 2023).

enforcement of the CPRA regulations could begin on July 1, 2023.[7] Such an enforcement timeline would grant businesses less than the statutorily intended one-year period to bring themselves into compliance with new regulatory provisions, including provisions on the novel and technically complex subject of opt-out preference signals. The lingering ambiguity surrounding these signals, coupled with a potentially shortened enforcement window, highlights the importance of the statute's intent that the Agency first promulgate proposed regulations that address all statutorily required terms before mandating that businesses comply.

## II. The Proposed Regulations Overlook the CPRA's Recognition of Consumer Notice as a Valid Basis for Data Use, Presenting a Significant Dispute

The CPRA sets outs permissible business purposes for data use *and expressly* states personal information may be used for "other notified purposes."[8] Despite this statutory text, the proposed regulations introduce an "average" or "reasonable" consumer expectation standard that would make consumer notice obsolete under the statute.[9] The disharmony between the statutory text of the CPRA and well-established consumer privacy principles and what the proposed rules set forth underscores the importance of addressing this issue completely in regular order and not via a consent agenda. The issue deserves a thorough discussion of the benefits of permitting businesses' data use consistent with their notices to consumers, as well as an explanation of the Agency's perceived authority to contravene a standard stated clearly in the text of the CPRA itself.

## III. Conclusion

We and our members strongly support protecting consumer choice and privacy and preserving responsible data use by commercial businesses operating in California. Given the discussion during the Agency's September 23 meeting, we urge you to refrain from considering the matters we have mentioned above during any condensed consent agenda process. We will continue to raise these and other critical points in future comments to the CPPA so they may hopefully help to facilitate the CCPA's rulemaking proceedings. Again, we thank you for the opportunity to participate in the CPRA rulemaking process.

* * *

[7] *Id*.

[8] "A business's collection, use, retention, and sharing of a consumer's personal information shall 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." *Id.* at §§ 1798.100(c), 140(e).

[9] The proposed regulations would require "a business's collection, use, retention, and/or sharing" of personal information to be "reasonably necessary and proportionate to achieve… the purpose(s) for which the personal information was collected or processed… [or] another disclosed purpose that is compatible with the context in which the personal information was collected…." Cal. Code Regs. tit. 11, § 7002(a) (proposed). Both permitted uses of personal information require a consideration of average or "reasonable" consumer expectations. *Id*. at §§ 7002(b); (c)(1).

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
202-296-1883

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP