NAI
PRIVACY, TRUST & ACCOUNTABILITY

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

February 19, 2025

Submitted via electronic mail to regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Legal Division - Regulations Public Comment
2101 Arena Boulevard
Sacramento, CA 95834

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

To the California Privacy Protection Agency:

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to comment on the proposed regulations regarding CCPA Updates, Insurance, Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology under the California Consumer Privacy Act (the "Proposed Regulations").[1] The NAI shares the concerns the California Privacy Protection Agency (the "Agency") has expressed regarding the proliferation of Automated Decisionmaking Technology ("ADMT") in the everyday lives of consumers and, as such, we support the Agency's efforts to introduce much-needed regulations to protect consumers and provide them with additional rights regarding businesses' use of ADMT. The NAI also applauds the ongoing commitment to public involvement and transparency the Agency is demonstrating through this important rulemaking process.

In addition to providing information about the NAI, we offer the following comments and recommendations related to the Proposed Regulations, which we hope will assist the Agency in meeting its objectives for the rulemaking while preserving a free, open, and secure internet for all California consumers:

- Remove Cross-Context Behavioral Advertising ("CCBA") from the definition of "Behavioral Advertising" to avoid presenting consumers with duplicative and potentially confusing choices.
- Consolidate the additional disclosures proposed for the ADMT Pre-Use Notice with the existing Notice at Collection requirements.
- Remove the proposed "remains deleted" language in section 7022 of the CCPA regulations to avoid inconsistencies with existing requirements to *permanently and completely* erase data.
- Clarify that, when conducting risk assessments, businesses must ensure that their use of ADMT does not *unlawfully* discriminate based upon protected classes.
- Clarify that the proposed right to access ADMT does not require a business to reveal any trade secrets when responding to a verifiable consumer access request.

[1] California Privacy Protection Agency Proposed Text, Cal. Code Regs. tit. 11 (proposed Nov. 22, 2024) (hereinafter "Proposed Regulations").

- Harmonize the attestation requirements for ADMT risk assessments with the grace period that relieves businesses from immediately conducting risk assessments of ADMT processing initiated prior to the effective date of the Proposed Regulations..

These comments are set forth in more detail below.

I. **About the NAI**

The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. The NAI has been a leader in this space since its inception in 2000,[2] promoting the highest voluntary industry standards for member companies, which range from small startups to some of the largest companies in digital advertising. NAI's members are providers of advertising technology solutions and include ad exchanges, demand and supply side platforms, and other companies that power the digital media industry by helping digital publishers generate essential ad revenue, helping advertisers reach audiences interested in their products and services, and helping to ensure consumers are provided with ads relevant to their interests.

The NAI was founded on a mission of responsible data collection and use for digital advertising to promote economic and societal benefits to consumers. In further accordance with this mission, the NAI recently brought together member companies and leading industry privacy experts to develop and launch our new NAI Accountability and Self-Regulatory Framework ("Framework").[3] The new Framework consists of five fundamental principles for privacy in digital advertising which our member companies must adhere to. The new Framework not only prepares NAI member companies for the ever-evolving legal and regulatory environment in which they are operating in, it reinforces the NAI as a leader in this new era of self-regulation and privacy. We offer the following detailed comments on the Proposed Regulations, which we are hopeful will assist the Agency in meeting its objectives for the rulemaking while preserving an open, global, and secure internet for all consumers.

II. **The Agency should remove "Cross-Context Behavioral Advertising" from the proposed definition of "Behavioral Advertising" to avoid confusing consumers without sacrificing privacy protections.**

Notice about and consumer control over certain uses of personal information are important and fundamental privacy protections. However, in order for those protections to be effective, they must be presented in simple, clear, and unambiguous terms. Otherwise, choices presented to consumers risk creating confusion about what choices are being offered and how they may be exercised – an issue the Agency has been appropriately attentive to through its focus on dark patterns.[4] However, by including CCBA – a term already clearly defined and regulated by the CCPA – within the umbrella term "behavioral advertising," the Agency risks creating unnecessary confusion among consumers seeking to exercise different opt-out rights without any corresponding privacy benefit. As explained in more detail below, we therefore recommend that the Agency remove CCBA from the definition of "behavioral advertising" in the Proposed Regulations.

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

[3] The NAI Self-Regulatory Framework, https://thenai.org/self-regulatory-framework/.

[4] *See* Enforcement Advisory No. 2024-02, *Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice*, https://cppa.ca.gov/pdf/enfadvisory202402.pdf.

A. Background on how the California Consumer Privacy Act of 2018 ("CCPA") regulates Cross-Context Behavioral Advertising ("CCBA").

The CCPA clearly defines CCBA and unequivocally requires businesses to provide transparency into how they conduct CCBA and to offer consumers methods to opt out of that activity.[5] However, the CCPA also distinguishes between CCBA – which inherently involves transfers of personal information such as "selling" or "sharing" personal information – from advertising that relies solely on personal information collected in a first-party context ("first-party advertising").[6]

The fact that CCBA is treated explicitly by the CCPA (and is distinguished from other types of advertising and marketing purposes like first-party advertising)[7] empowering the Agency to develop regulations and define requirements pertaining specifically to CCBA. Since its creation, the Agency has exercised this power by setting specific, detailed regulatory requirements for CCBA , including, amongst other things, that consumers be notified as to what personal information is sold or shared and to whom, and be enabled to opt out of the sale or sharing of their personal information.[8] Indeed, consumers have been given broad rights and, most importantly, the tools necessary to exercise those rights, with respect to CCBA.

While it may not meet the definition of CCBA, first-party advertising may still involve the collection of consumer personal information and its processing using ADMT to provide interest-based advertising to consumers. As neither the CCPA nor the Agency's regulations had previously defined *first-party* behavioral advertising, these advertising practices were not covered by the same notice and choice

[5] The CCPA defines CCBA as the "targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded internet websites, applications, or services, other than the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts." California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(k) (2018) (hereinafter "CCPA") (emphasis added). The CCPA requires businesses to provide consumers with prominent disclosures about their selling and/or sharing of personal information, including in the notice at collection. *See, e.g., id.* § 1798.100(a). It also grants consumers the direct right to opt out of sharing for CCBA, *see id.* § 1798.120, and requires businesses to provide a clear and conspicuous link enabling them to opt out of selling or sharing their personal information for CCBA, *see id.* § 1798.135(a)(1), (c)(2). *See also generally* Arsen Kourinian, *How Expansion of Privacy Laws, Adtech Standards Limits Third-Party Data Use for Retargeting*, IAPP (Apr. 27, 2021), https://iapp.org/news/a/how-the-expansion-of-data-privacy-laws-and-adtech-standards-limits-companies-ability-to-use-third-party-data-for-retargeting.

[6] The CCPA Regulations define "first party" as a consumer facing business with which the consumer intends and expects to interact. *See* Cal. Code Regs. tit. 11 § 7001(m). Conversely, the CCPA defines "sharing" as sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising. *See* CCPA at § 1798.140(ah)(1). As such, data collected by a social media platform from consumers browsing the platform for behavioral advertising would be considered first-party data under the CCPA. *See generally* Allison Schiff, *Here's How Facebook, Google and Amazon Are Tackling CCPA Compliance*, AdExchanger (Jul 9, 2020) ("Facebook isn't making major changes to its web and mobile-tracking services on the grounds that the way it collects and shares data through its tracking pixel doesn't constitute selling data.").

[7] *See* CCPA at § 1798.140(e)(6) (defininig"business purpose" to include "[p]roviding advertising and marketing services, *except for cross-context behavioral advertising*[.]" (emphasis added).

[8] *See, e.g.,* Cal. Code Regs. tit. 11 §§ 7013 & 7026.

requirements as CCBA. By defining "Behavioral Advertising"[9] in the Proposed Regulations, we believe the Agency's primary goals are to extend the rights consumers already possess relating to CCBA to first-party advertising, as well as other forms of ADMT that may not involve transfers of information like "selling" or "sharing." However, by proposing to include CCBA within the umbrella definition of "Behavioral Advertising," the Proposed Regulations introduce an unnecessarily confusing and duplicative set of requirements for CCBA *as a subset of behavioral advertising* when those same requirements already apply to CCBA directly through the CCPA and the existing regulations.

B. Including "Cross-Context Behavioral Advertising" in the definition of "Behavioral Advertising" is duplicative and potentially confusing for consumers and businesses.

Transparency and *choice* are most effective when business activities involving personal information processing are described clearly, simply, and unambiguously, and accompanied by simple, easy-to-use choice mechanisms. However, by including CCBA in the definition of "Behavioral Advertising," the Proposed Regulations would subject CCBA to a new set of notice and choice requirements that are entirely duplicative of those that already exist under the CCPA. As they are duplicative, the notice and opt-out rights associated with ADMT, as applied to CCBA, would present no benefit to consumers; but instead may cause confusion about the scope and meaning of an opt out when a consumer is presented with different options to opt out of "sales," "sharing," and "ADMT."

More specifically, and as discussed above,[10] the CCPA already grants consumers robust transparency and control into a business's processing of personal information for CCBA. However, if the Proposed Regulations also define CCBA as a form of behavioral advertising, it would also be subject to redundant notice and choice requirements.[11] This additional and duplicative information does not further inform consumers about how businesses process their personal information for CCBA beyond what is already required by the CCPA. Even worse, the additional information is likely to confuse or overwhelm consumers with redundant information about CCBA, running counter to the requirement that disclosures must be "easy to read and understandable[.]"[12]

In addition to duplicative transparency, the Proposed Regulations, as written, would also present consumers with duplicative and overlapping choices to opt out of CCBA. The CCPA already requires businesses to provide multiple methods for consumers to opt out of for CCBA,[13] including by honoring

[9] The Proposed Regulations define "Behavioral Advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity—both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services." Proposed Regulations at § 7001(g). As noted, this definition "includes cross-context behavioral advertising." *Id.* at § 7001(g)(1)

[10] *See supra* section II.A.

[11] *See, e.g.,* Proposed Regulations at § 7220 (requiring separate disclosures for ADMT).

[12] Cal. Code Regs. tit. 11 § 7003(a).

[13] A business conducting CCBA must (1) provide a clear and conspicuous link on the business' internet homepages, titled "Do Not Sell or Share My Personal Information," to an Internet web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale or sharing of the consumer's personal information; and (2) provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information. *See* CCPA at § 1798.135(a). The current regulations enshrine these statutory requirements in section 7013. *See* Cal. Code Regs. tit. 11 § 7003(a).

opt-out preference signals.[14] However, if the Proposed Regulations continue to include CCBA as a form of "Behavioral Advertising”, then businesses conducting CCBA would be subject to a separate and duplicative opt-out right.[15] This would risk confusing consumers about the meaning and scope of their opt-out rights while providing them no additional benefits, and would also run counter to the Agency’s existing requirements to provide information to consumers in a way that is straightforward, easy to read, and avoids technical and legal jargon.[16] By way of example, a consumer might interact with a business that provides opt-out mechanisms for sales, sharing for CCBA, and for certain forms of “profiling” as required by the Proposed Regulations. A consumer interacting with that business may wish to opt out of profiling by the business due to specific concerns about how the business might use a profile for employment purposes; but may also have made a conscious decision *not* to opt out of CCBA, given the separate choice mechanisms and the explanation given by the business of how advertising supports their operations . Under the proposed regulations, this consumer’s expectations would be frustrated because an opt-out of “profiling” would by definition also include an opt-out of CCBA, even though these are presented separately by the business in compliance with CCPA.

The Agency can prevent this potential for consumer confusion and upset expectations – without sacrificing any privacy benefits for consumers – simply by removing CCBA from the definition of behavioral advertising and allowing the existing provisions of the CCPA regarding CCBA to do their intended work directly.

C. Treatment of CCBA in other parts of the Proposed Regulations

The NAI recognizes that the Proposed Regulations create business obligations on their use of ADMT beyond consumer notice and choice (already discussed above). For example, the Proposed Regulations include a requirement for businesses to conduct a risk assessment for high-risk processing activities, including certain forms of ADMT.[17] Our recommendation to remove CCBA from the definition of behavioral advertising is not intended to excuse CCBA from risk assessments. Indeed, the Agency appears to have independently determined that selling and/or sharing personal information for CCBA is a high-risk processing activity in its own right.[18] Again, this is an example where removing CCBA from the definition of behavioral advertising will not prevent the Agency from meeting its goals for the treatment of CCBA.[19]

There may be other areas of the Proposed Regulations where similarly direct treatment for CCBA can meet the Agency’s goals without causing the confusion we anticipate if CCBA is left within the definition of behavioral advertising.

[14] *See* CCPA at § 1798.135(e).

[15] *See* Proposed Regulations at § 7221(c).

[16] *See* Cal. Code Regs. tit. 11 § 7003(a) (“Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.”); *See also* Enforcement Advisory No. 2024-02, *Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice*, https://cppa.ca.gov/pdf/enfadvisory202402.pdf.

[17] *See* Proposed Regulations at § 7150.

[18] *See id.* § 7150(b)(1).

[19] Other states have made similar determinations. For example, the Colorado Privacy Act requires businesses that are selling or sharing personal information for behavioral advertising to conduct *Data Protection Assessments* to ensure its processing does not present a heightened risk of harm to consumers. *See* Colo. Rev. Stat. § 6-1-1309(2)(b).

NAI Recommendation: For these reasons, we recommend modifying the definition of "Behavioral Advertising" to remove CCBA, as follows:

> (g) "Behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity~~— both across businesses, distinctly branded websites, applications, or services, and~~ within the business's own distinctly-branded websites, applications, or services.
>
> (1) Behavioral advertising does not include~~s~~ cross-context behavioral advertising, as defined by Civil Code section 1798.140, subdivision (k).
>
> (2) Behavioral advertising does not include nonpersonalized advertising, as defined by Civil Code section 1798.140, subdivision (t), provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party.

II. The Agency should consolidate the additional disclosures proposed for the Pre-Use Notice with the existing Notice at Collection requirements.

As noted above, the CCPA regulations require disclosures to consumers to be straightforward and avoid technical and legal jargon. Indeed, consumers must be provided language that is easy to understand when faced with privacy choices. To promote simplicity and ease of understanding, consumers interacting with a service that collects personal information and employees ADMT to process that information will be best served by a single, easy-to-read notice that explains the data processing taking place. For this reason, we recommend the Agency consolidate the additional disclosures proposed for the *Pre-Use Notice* with the existing disclosures required for the *Notice at Collection.*

The Proposed Regulations would require any business using ADMT to provide consumers with an *additional* pre-use notice informing consumers about the business's use of ADMT and the consumers' rights to opt-out of ADMT and to access ADMT. The Proposed Regulations would require the pre-use notice to include (1) an explanation of the specific purpose for using ADMT; (2) a description of the consumer's right to opt-out of ADMT; (3) a description of the consumer's right to access ADMT; (4) a statement that the business is prohibited from retaliating against consumers for exercising their CCPA rights; and (5) additional information about how ADMT works including the logic used in ADMT and the intended output of the ADMT.[20]

However, the CCPA and existing regulations already require a *Notice at Collection* for consumers, to ensure they have transparency into how a business may collect, use, and share their personal information at or before the point of collection. This notice must include (1) a list of categories of personal information about consumers; (2) the purpose of collecting and using the personal information; (3) whether personal information is sold or shared; (4) the length of time the business intends to retain the personal information; (5) a link to the right to opt-out of sale/sharing of data; and (6) a link to the business's privacy policy.[21]

[20] *See* Proposed Regulations at § 7220(c).

[21] *See* Cal. Code Regs. tit. 11 § 7012(e).

Because consumers are already entitled to clear, timely notice about how businesses will process their personal information, we recommend that the Agency consolidate the additional disclosures proposed for the ADMT pre-use notice with the existing notice at collection. This would continue to promote the Agency's objective of ensuring consumers are provided with meaningful information and an opportunity to exercise their rights regarding ADMT while avoiding unnecessarily complex and confusing disclosures for consumers.

NAI Recommendation: The Agency should consolidate the additional disclosures proposed in section 7220 with the existing *Notice at Collection* requirements in section 7012.

III. The Agency should remove the proposed "remains deleted" language in section 7022 to avoid inconsistencies with existing requirements to *permanently* and *completely* erase data.

The Proposed Regulations change how businesses comply with deletion requests by adding a requirement not only that the business delete the consumer's personal information consistent with the CCPA's requirements, but also "implement measures to ensure that the information remains deleted, deidentified, or aggregated" upon receiving a valid deletion request from a consumer.[22] While the NAI appreciates the Agency's efforts to ensure that valid deletion requests are fully effectuated by businesses, the practicalities of ensuring that a consumer's personal information "remain deleted" are inconsistent with other clear requirements in the CCPA and the existing implementing regulations.

Specifically, any measures that a business may implement to ensure that a consumer's personal information "remain deleted" would appear to require that the business actually retain personal information about the consumer — *i.e.*, for suppression purposes – instead of fully and completely deleting the consumer's personal information. However the CCPA and its existing regulations require that a business respond to a verifiable consumer request to delete by ***permanently and completely eras[ing] the consumer's personal information from their systems*** (emphasis added).[23] A business cannot, therefore, retain some of a consumer's personal information to ensure that other elements of it "remain deleted" without violating the requirement to "permanently and completely" delete the consumer's information.

Additionally, taking steps to ensure that a consumer's personal information remains deleted appears to change the plain meaning of a single request to delete into two distinct requests – one to delete personal information associated with the requestor, and a second one to stop collecting personal information about the requestor. In its *Initial Statement of Reasons*, the Agency explains that this language has been added to "ensure that a consumer's right to delete is meaningful" and that

[22] Proposed Regulations at § 7022(b)(1); *see also* § 7022(c)(1).

[23] *See* Cal. Code Regs. tit. 11 § 7022(b) ("A business shall comply with a consumer's request to delete their personal information by: (1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, or aggregating the consumer information; (2) Notifying the business's service providers or contractors of the need to delete from their records the consumer's personal information that they collected pursuant to their written contract with the business…; and (3) Notifying all third parties to whom the business has sold or shared the personal information of the need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort."); *id.* at § 7022(c) ("A service provider or contractor shall… cooperate with the business in responding to a request to delete by doing all of the following: (1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, aggregating the consumer information, or enabling the business to do so.").

consumers should not be required to "make repetitive requests to delete with the business, rendering the right to delete pointless."[24] However, the additional *remains deleted* language does not match the plain meaning of the word "delete" or the way it is treated under the CCPA and existing regulations . In some cases, it may also run afoul of consumer expectations. A consumer may wish to delete excessive or historical personal information a business has collected about them; but also wish to continue interacting with the business in a more limited or current manner. Requiring businesses to stop collecting information about the consumer in those circumstances is likely to be frustrating and confusing to consumers, as well as putting businesses at risk of violating the other dictates of the CCPA to completely delete the consumer's information instead of retaining some elements of personal information for suppression purposes.

Further, the California legislature has explicitly considered and provided a mechanism for an analog of the "remains deleted" requirement in the Delete Act. In effect, a consumer who in the future uses the Delete Request and Opt-Out Platform under development at CPPA to request deletion by registered data brokers will "remain deleted" by those brokers because data brokers must continue to delete all subsequently collected personal information of that consumer once every forty five days.[25] Data brokers are expected to achieve this result by integrating with a deletion mechanism maintained by the Agency at regular intervals.[26] This solution achieves the objective of ensuring a consumer's data *remains deleted* upon submitting a deletion request while avoiding the pitfall of a business needing to retain some personal information about the consumer – which is currently prohibited under the CCPA and its implementing regulations. The Proposed Regulations do not include – and the CCPA's drafters did not provide for – a comparable mechanism that would allow businesses to ensure a consumer remains deleted without violating the requirement to fully comply with a deletion request. For these reasons, we recommend removing the "remains deleted" language from the Proposed Regulations.

NAI Recommendation: The Agency should remove the proposed "remains deleted" language in section 7022 of the CCPA regulations to avoid inconsistencies with existing requirements to *permanently and completely* erase data.

IV. The Agency should clarify that businesses must evaluate whether their use of ADMT does not *unlawfully* discriminate based upon protected classes in § 7152(a)(6)(B)(i).[27]

Identifying and mitigating risks to consumers posed by discrimination based upon protected classes is an important objective of the Proposed Regulations, particularly where those classes of individuals have vulnerabilities or have been historically subject to harmful discrimination. However, because the Agency has not adequately defined or specified the type of discrimination it is seeking to address, the Proposed Regulations risk creating a prohibition on all distinctions made among consumers, even when those distinctions are otherwise lawful and beneficial to consumers.

[24] CALIFORNIA PRIVACY PROTECTION AGENCY – INITIAL STATEMENT OF REASONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) at 30, (Nov. 22, 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.

[25] *See* California Delete Act, Cal. Civ. Code § 1798.99.86(c) (2023) (hereinafter "Delete Act").

[26] *See id.* at § 1798.99.86(a).

[27] There are seven instances in the Proposed Regulations where "does not discriminate based upon protected classes" is mentioned. *See* Proposed Regulations at § 7152(a)(6)(B)(i); § 7152(a)(6)(B)(ii); § 7201(a)(1); § 7201(a)(2); § 7221(b)(3)(B).

For businesses using ADMT to conduct "extensive profiling," the Proposed Regulation require the business to evaluate whether the ADMT technology works as intended for the business's proposed use and "does not discriminate based upon protected classes[.]"[28] Protected classes are extensively defined in the State of California to include, amongst many other things, race, religion, gender, sexual orientation, medical condition, disability, and age if over forty years old.[29]

There are many scenarios where discriminating based on a protected class can cause consumer harm. For example, in its *Initial Statement of Reasons*, the Agency describes a scenario where ADMT is used to serve advertisements for high-paying job opportunities disproportionately to men. In this case, women may be deprived of the opportunity to learn about and apply for higher-paying jobs that they have historically been excluded from. In this scenario, the discrimination at issue would also be unlawful.[30] In a second example, the Agency describes a scenario where advertisers use social media to target housing advertisements based on protected classes, such as race, gender, and age.[31] In this scenario as well, the discrimination based on protected classes is unlawful.[32] As such, it appears that the type of discrimination based upon protected classes that the Agency is primarily concerned with is unlawful discrimination. The NAI therefore recommends that the Agency modify the sub-section to clarify that a business's evaluation must ensure the ADMT technology does not *unlawfully* discriminate based upon protected classes.

Further, In a recent Legal Advisory, the California Attorney General, Rob Bonta, provided specific guidance on the application of existing California laws to various uses of artificial intelligence (AI), which encompasses many of the same uses the Agency seeks to cover for ADMT in the Proposed Regulations. In his advisory, the Attorney General cited the Unruh Civil Rights Act, the California Fair Employment and Housing Act, and the California Consumer Credit Reporting Agencies Act as examples of laws that apply equally to AI systems as they do to systems without the involvement of any AI.[33]

[28] *Id.* at § 7152(a)(6)(B)(i).

[29] *See* Protected Classes in California, https://www.senate.ca.gov/protected-classes (last visited Feb. 1, 2025).

[30] For example, serving advertisements for high-paying job opportunities disproportionately to men is already unlawful under the California Fair Employment and Housing Act (FEHA). *See* Cal. Gov't Code § 12940(c); *e.g. Facebook EEOC Complaints*, ACLU (Sep. 25, 2019) https://www.aclu.org/cases/facebook-eeoc-complaints, (Facebook settles case where ACLU alleges Facebook delivered job ads selectively based on age and gender categories and agrees to require all advertisers to certify compliance with Facebook's policies prohibiting discrimination and with applicable federal, state, and local anti-discrimination laws).

[31] *See* CALIFORNIA PRIVACY PROTECTION AGENCY – INITIAL STATEMENT OF REASONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) at 62, (Nov. 22, 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.

[32] *E.g. Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising*, Department of Justice Office of Public Affairs (Jun. 21, 2022), https://www.justice.gov/archives/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known, (Facebook settles case where the Department of Justice alleges that Facebook's algorithms relied, in part, on consumer characteristics to serve housing ads in violation of the Fair Housing Act).

[33] *See* California Attorney General's Legal Advisory on the Application of Existing California Laws to Artificial Intelligence, https://oag.ca.gov/system/files/attachments/press-docs/Legal%20Advisory%20-%20Application%20of%20Existing%20CA%20Laws%20to%20Artificial%20Intelligence.pdf.

If the Agency does not specify that businesses must evaluate for *unlawful* discrimination, the current language would put legitimate, beneficial, and otherwise lawful distinctions between individuals in protected classes at risk. For example, and keeping to the advertising context, an advertiser may wish to reach an audience of individuals over 40 years old – a protected class under California law – to share information about financial products for retirement. Similarly, an advertiser may wish to reach a specifically male or female audience with advertising for men's or women's fashion; but doing so requires making a distinction based on gender, another protected class under California law. Failing to specify that the Agency intends to address *unlawful* discrimination is likely to cause confusion among advertisers seeking to reach relevant audiences without harmful or illegal discrimination and prevent consumers in protected classes – even simply based on age group or gender – from learning about products that are designed for them. Making this clarification would still require advertisers and the platforms they use to evaluate whether their methods for advertising for particular things – like housing, credit, or employment – could involve *unlawful* discrimination.

The NAI believes this recommendation is consistent with the agency's goals with the proposed requirement as well as consistent with the decades of carefully-crafted statutes and case law in the State of California that extensively define what unlawful discrimination is. This clarifying amendment would not only ensure the CCPA regulations are harmonized with other state laws[34] and regulations,[35] but it would also ensure that harmless uses of ADMT in advertising are not unnecessarily restricted by the Proposed Regulations. For these reasons, we recommend modifying the sub-section to clarify that a business's evaluation must ensure the ADMT technology does not "unlawfully discriminate" based upon protected classes.

NAI Recommendation: The Agency should clarify that businesses must evaluate whether their use of ADMT does not unlawfully discriminate based upon protected classes in § 7152(a)(6)(B)(i). For example:

> (A) For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3), the business must identify the following:
>
> (i) Whether it evaluated the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not unlawfully discriminate based upon protected classes ("evaluation of the automated decisionmaking technology");

[34] *See* Colo. Rev. Stat. § 6-1-1308(6) ("A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers."); Conn. Gen. Stat. Ann. § 42-520(a)(5) ("A controller shall… not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers[.]"); Md. Code Ann., Com. Law § 14-4607(A)(3) ("A controller may not… [p]rocess personal data in violation of State or federal laws that prohibit unlawful discrimination[.]") (going into effect on Oct. 1, 2025); N.H. Rev. Stat. Ann. § 507-H:6(e) ("A controller shall… [n]ot process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers[.]"); N.J. Stat. Ann. § 56:8-166.12(a)(5) ("A controller shall… not process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination against consumers[.]").

[35] Similar to what the Agency is proposing in this rulemaking concerning *Risk Assessments*, the Colorado Privacy Act Rules require businesses that are processing personal data for profiling to conduct a *Data Protection Assessment* to ensure its processing does not risk causing an *Unlawful Disparate Impact* on consumers. *See* Colorado Privacy Act Rules 4CCR 904-3, Rule 9.06(A). The Colorado Privacy Act Rules define *Unlawful Disparate Impact* as "conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers." *Id.* at Rule 9.06(D).

V. **The Agency should add language to section 7222 clarifying that nothing in the section may be construed to require a business to reveal any trade secrets when responding to a verifiable consumer access request.**

Providing consumers with the right to access information about an ADMT - be it the ADMT's purpose, data outputs, and how those outputs are then used with respect to the consumer - is an important objective of the Proposed Regulations.[36] However, the CCPA recognizes the importance of transparency to consumers with business interests in proprietary or trade secret information by requiring any adoption of regulations to include exceptions to ensure trade secrets are not disclosed in response to a verifiable consumer request.[37] As such, the NAI recommends adding language to section 7222 clarifying that nothing in the section may be construed to require a business to reveal any trade secrets when responding to a verifiable consumer access request.

NAI Recommendation: The Agency should add language to section 7222 clarifying that nothing in the section may be construed to require a business to reveal any trade secrets when responding to a verifiable consumer access request.

VI. **As businesses will have 24 months from the effective date to identify processing activities and conduct risk assessments, the Agency should add an exception to the attestation requirement.**

The Agency rightfully included a grace period for businesses to conduct risk assessments of ADMT processing initiated prior to the effective data of the Proposed Regulations. However, in doing so, the Agency inadvertently included language in the Proposed Regulations that risk requiring businesses to falsely attest that they abstained from their ADMT processing. As such, we recommend the Agency add an exception to the attestation requirement.

Under the Proposed Regulations, businesses will need to conduct risk assessments to determine whether the "risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing."[38] These assessments must be conducted and documented prior to initiating the use of ADMT, and be submitted to the Agency with an attestation stating "that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article."[39] However, in consideration of ADMT processing initiated prior to the effective date of the Proposed Regulations, the Agency gives businesses a 24 month grace period to "conduct and document a risk assessment in accordance with the requirements of this Article[.]"[40]

[36] *See* Proposed Regulations at § 7222.

[37] *See* CCPA at § 1798.185(a)(3) ("On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to… [e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.").

[38] Proposed Regulations at § 7152(a).

[39] *Id.* at § 7157(b)(1)(B)(iii).

[40] *Id.* at § 7155(c).

NAI Recommendation: Consistent with the grace period already included in the Proposed Regulations, the NAI recommends that the Agency clarify that it also applies to the attestation requirement. For example, section 7157(b)(1)(B)(iii) could be supplemented with the following redlined text:

> An attestation that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article unless the processing activity identified in section 7150, subsection (b), was initiated prior to the effective data of these regulations;

This recommendation will ensure businesses that currently use ADMT for processing will not be required to falsely attest that they abstained from ADMT processing.

VII. Conclusion

Thank you for your continued commitment to public involvement and transparency in this important rulemaking process concerning automated decisionmaking technology. 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@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)