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

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Dear Mr. Sabo,

On behalf of the Network Advertising Initiative (NAI), thank you for the opportunity to provide comments on the California Privacy Protection Agency ("CPPA" or "Agency") Preliminary Rulemaking Activities on cybersecurity audits, risk assessments, and automated decisionmaking.[1]

## I. Introduction

### A. Overview of the NAI

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising technology companies. 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 industry 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 enhancing consumer trust. As a non-profit organization, the NAI promotes the health of the digital media 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,[2] 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.[3] 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

[1] https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf

[2] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[3] *See* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter "NAI Code"], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

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.

## II. General Recommendations

The NAI supports the requirement for businesses that process personal information to conduct regular cybersecurity audits and data risk assessments. These risk assessments are also required by privacy laws in Virginia and Colorado—referred to as Data Protection Assessments ("DPAs")—and are essential for responsible data processing that minimizes risk posed by the collection and processing of personal information. As the NAI considers the needs of our member organizations, we have begun the process of aligning our requirements with those found in the California Privacy Rights Act ("CPRA") and in other state privacy laws. In response to the state requirements for risk assessments around various types of data and practices, the NAI has begun a process of mapping the requirements to digital advertising practices, with the goal to help companies tailor their own assessments building from core NAI compliance requirements as the foundation.

New state legal requirements for risk assessments can ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. However, a set of disparate requirements across multiple states threatens to create an environment where businesses are overwhelmed in their efforts to comply, with no discernable privacy benefit to consumers. The CPRA generally recognizes this by directing the Agency to cooperate with other states and countries "to ensure consistent application of privacy protections."

Therefore, the NAI urges the Agency to develop and implement regulations that seek to harmonize to the greatest extent possible with the other state laws. We also offer the following recommendations regarding data risk assessments and cybersecurity audits.

### *Data Risk Assessments*

First, in seeking to harmonize risk assessment requirements with other state laws, the Agency should identify a consistent set of criteria for assessments to provide for the performance of a single assessment by businesses. The Agency should maintain a clear emphasis on processing that presents a heightened risk of harm to consumers. The Colorado Privacy Act ("CPA"), Virginia Consumer Data Protection Act ("VCDPA"), and Connecticut Data Protection Act ("CTDPA") are largely consistent in their identification of activities requiring the performance of

a risk assessment, so aligning with these two laws would not only be a practical step, but also a relatively efficient process. Similarly, Europe's General Data Protection Regulation ("GDPR") requires the performance of data protection impact assessments ("DPIA") for data processing that "is likely to result in a high risk to the rights and freedoms of natural persons." The law sets out three categories in which DPIAs are always required: systematic and extensive profiling with significant effects, processing of sensitive data on a large scale, and systematic monitoring of public areas on a large scale.

Second, while the CPRA makes references to submission of risk assessments on a regular basis, the NAI recommends that the Agency clarify the requirement for performance of annual risk assessments, and allow the Agency to request risk assessments when they are relevant to an investigation or inquiry. This approach would conform with Virginia's privacy law, which provides for submission to the Attorney General upon request when there is an ongoing investigation of a business, and the assessment is relevant to that investigation. This is also consistent with the approach taken under the GDPR, where businesses are required to conduct data impact assessments and to make these records available to a European data protection authority in the event of an audit or investigation arising from the controller's use of the data. Importantly, it helps the Agency balance its resources more effectively by not creating an unnecessary overburden through an automatic production without cause.

Third, while the CPRA appropriately requires businesses to conduct risk assessments only after the law comes into effect on July 1, 2023, the Act does not explicitly clarify that data in a businesses' possession *prior* to the effective date would also not be subject to risk assessments moving forward. We therefore ask that the CPRA regulations clarify by adopting language consistent with Colorado law, which explicitly clarifies the application of the requirement to personal data that a business "acquired on or after" the CPA's effective date. This approach is clear and efficient, providing businesses the opportunity to establish forward-looking assessments and have greater confidence in their compliance efforts.

Finally, the assessments should be confidential, and the rules should recognize that privileged information or trade secrets will be redacted. This presents a practical approach to help companies maintain confidentiality of business practices.

***Cybersecurity Audits***

The CPRA implementing regulations should clarify that businesses are required to conduct cybersecurity audits on an annual basis, and they should establish clear requirements for retention of audit records. The requirement for cybersecurity audits should maintain a risk-based approach, where businesses can certify that they have implemented and adhere to policies and procedures designed to identify types of personal information and processing practices that present the greatest risk for the consumer's privacy or security. It should be a priority for the Agency to maintain consistency with existing security requirements and practices in California law, as well as those promoted by the FTC, and requirements recently enacted in other state privacy laws.

The NAI recommends that the regulations align with current California law, and other relevant laws, enabling business to utilize existing certifications, such as the ISO 27000 series certification and those that leverage the NIST Cybersecurity Framework. Companies should retain the ability to develop and conduct their own internal cybersecurity program and engage third-party auditors. The Agency can also look to the programs established in cases where audits are required pursuant to consent decrees established by the FTC. Finally, 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.

## III. NAI Responses to Questions for Public Comment

### A. Risk Assessments

The NAI supports the development of uniform, national standards for DPAs. As a self-regulatory body, we believe that standardized assessments are the best way to develop an understanding of emerging business practices, and they can serve as an important tool in compliance and regulation. The NAI's long-standing Code and compliance program is in essence a DPA program to identify and minimize risks surrounding the collection and use of consumer data for digital advertising purposes, predating the legal requirements established under the GDPR and newer U.S. state laws. The NAI's compliance team actively works with companies to assess practices, and as these practices evolve and new privacy risks are identified, we regularly update our Code and associated guidance documents, raising the bar to ensure that NAI members are upholding the highest standards among industry.[4]

The new state law requirements for DPAs can ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. Further, the ability of regulators to request access to the results of risk assessments in performing an audit provides enhanced transparency, provided that regulator audits provide essential protections of trade secrets and proprietary practices. Please see responses to some of the specific related questions below.

- **Q2:** ***What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?***

[4] *See* NETWORK ADVERTISING INITIATIVE, *Annual Report* (2021), http://thenai.org/wp-content/uploads/2022/08/2021NAIAnnualReport1.pdf.

Harms that can arise from processing data depend both on the nature of the personal information, and more importantly, on the use of this information. Therefore, harms from processing personal information arise not from ne processing sensitive data per se, but by how that data is processed and utilized. Indeed, some instances of processing sensitive data actually benefit the marginalized groups and broader society.

The CPRA's requirements emphasize the need to balance the benefits and risks. The CPPA's goal with respect to requiring and assessing DPAs should therefore be to discourage and protect against harmful practices and outcomes, while promoting beneficial uses of data not solely classifying and regulating sensitive versus non-sensitive data. Specifically, in crafting regulations, the CPPA could identify and categorize types of harm instead of data, to promote good uses of data, prevent entities from using privacy law as a pretext to attack competition, while at the same time allowing marginalized individuals to be presented with advertisements and other services relevant to their specific communities. In other words, a functionalist, outcome-based approach to enforcement better protects the civil liberties and rights of consumers while the current typological system abjectly fails to do so.

While the NAI's 2020 Code of Conduct definition of sensitive data largely aligns with the definition established by California and other state privacy laws, there are some categories of data where we diverge; notably, on requirements that consider information about a consumer's race or ethnicity to be sensitive. We recognize and agree that many consumers have increased sensitivity around these data types, and that they could present an increased likelihood of harm to consumers depending on certain processing activities, including disparate outcomes, particularly if processed for purposes such as eligibility determinations. For this reason, the NAI prohibits the use of any data collected for advertising and marketing to be used for eligibility determinations. This approach preserves the ability of companies to tailor advertising based on these categories, and it places restrictions on companies who the data is shared with, further mitigating the potential for harmful outcomes.

The Agency's consideration of privacy and harms in automated decisionmaking should therefore focus on how to identify and regulate the resulting impact from certain processing activities, instead of seeking to create limits on data collection and processing broadly, or based on an expansive set of "sensitive information." The NAI encourages the Agency to fully recognize the beneficial uses of data, including that which could be considered "sensitive," and to craft rules that do not unnecessarily limit the collection and use of data broadly, and to preserve opportunities to benefit protected classes and at-risk populations.

- **Q3:** ***To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):***
    - **Q3d:** ***What processing, if any, does not present significant risk to consumers' privacy or security? Why?***

As noted above, the NAI maintains a prohibition on the use of consumer data collected for advertising and marketing to be used for eligibility determinations. Using personal information to serve tailored advertising does not present a significant risk to consumers
Providing and serving advertisements related to an individual's interest in clothing or concerts for example,

In most instances, serving tailored ads for consumer goods and services does not present significant risk to consumers' privacy or security. Some harmful uses, like products and services involving eligibility determinations (such as for homes, jobs, or insurance) can be properly prevented with regulatory guardrails in place. For instance, as referenced above, NAI members are prohibited from using data collected for tailored advertising for these use cases.

### B. Automated Decisionmaking

The NAI appreciates the Agency's dedication to determining the appropriate scope of regulations around automated decisionmaking. Because the CPRA does not define automated decisionmaking, we believe it is important to properly scope the definition, to ensure that harmful uses the law aims to prevent are captured, while allowing for uses that do not create harms to consumers.

The GDPR and regulations in the European Union have attempted to define automated decisionmaking and pinpoint when these decisions produce legal effects and when they do not. For example, automated decisionmaking can be used to extend an interview to a job applicant, based on a computer's reading of the applicant's resume, and an algorithm's ability to rank that resume against other applicants. However, decisions like these can carry legal effects–the algorithm may, for example, be biased in favor of white applicants compared to Black applicants, or be biased in favor of men compared to women.

While the CPRA's definition of profiling necessarily incorporates what the CPRA considers to be cross-context behavioral advertising ("CCBA"), the legal effects of this type of decisionmaking are de minimis. The CCPA also provides for consumers to opt out of sales of their personal information, which includes CCBA, so there is not a need to incorporate consumer opt-out rights to tailored advertising within automated decisionmaking. One of the key distinctions worth noting is that automated decisionmaking is a common practice for performance of measurement and attribution in programmatic digital advertising, both tailored advertising and even contextual advertising. Such use cases do not pose significant risk to consumers and therefore should not fall within the definition of automated decisionmaking as it is intended to apply under the GDPR.

The NAI supports the Agency's aims of preventing harmful outcomes from automated decisionmaking, but urges the Agency to be cognizant of already-existing regulatory frameworks, and the different use cases for automated decisionmaking. Please see responses to some specific related questions below.

- **Q2:** ***What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?***

The NAI supports the CPRA's opt-out requirement associated with automated decision making activities, which includes profiling and tailored advertising. The NAI has long required members to provide consumers the ability to opt-out of tailored advertising. Processing that produces legal effects–*e.g.*, processing that affects an individual's rights, status, or rights under a contract –or similarly significantly affects a data subject is the kind of processing that should be considered the most sensitive, where an opt out would be most necessary.

Most tailored advertising and ad delivery and reporting does not produce legal effects. As discussed above, a legal effect is one where an automated decision affects an individual consumer's legal rights, such as the cancellation of a contract or granting or denial of a benefit guaranteed by law. Additionally, certain automated decisions could be covered by existing federal and state civil rights laws–such as a decision to extend a job interview to an applicant, where denial based on race would be in direct violation of the law. Comparatively, tailored advertising does not create a legal effect: an advertisement served on a website does not have an impact on an individual consumer's legal standing.

- **Q3:** ***With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:***

    - **Q3a:** ***How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?***

The CPRA does not fully define "automated decisionmaking." The text of the statute directs the Agency to include profiling in its regulations around automated decisionmaking. The CPRA defines profiling as "any form of automated processing of personal information… to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Other state privacy laws also reference automated processes in their definitions of profiling, including Colorado, Virginia, and Connecticut.

Outside the United States, the United Kingdom's Information Commissioner's Office ("ICO") defines automated decisionmaking as "the process of making decisions without any human

involvement."[5] While this definition is issued in guidance (and does not carry the force of law), it is informative for considering the scope of what automated decisionmaking technology should be. Further, the GDPR defines automated decisionmaking as "automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her," and defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse [*sic*] or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour [*sic*], location or movements."[6] The NAI believes that this definition is in line with the text of the CPRA.

- **Q8:** ***Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?***

As noted above, the CPRA already contains thoughtful, detailed requirements regarding CCBA, including requirements to comply with consumer opt-out rights, including honoring opt-out preference signals. Adding additional, differing requirements to the same activities, such as "profiling" through their inclusion as automated decisionmaking is likely to create confusion and extend this separate set of consumer rights more broadly than intended or desireable for policymakers and consumers.

Ultimately, a consumer's right to opt out of automated decisionmaking technology, including profiling, should vary depending on certain factors. While it is not practical to consider a comprehensive set of factors in regulations, the benefits of automated decisionmaking in

[5] Information Commissioner's Office, *What is automated individual decision-making and profiling?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/.

[6] General Data Protection Regulation (GDPR), Article 22, https://gdpr-info.eu/art-22-gdpr/. (Other policymakers agree with the definition of ADM being decisions based without any human involvement: EC Working Party: "Solely [ADM] is the ability to make decisions by technological means without human involvement," https://ec.europa.eu/newsroom/article29/items/612053; Irish DPC: "processing is 'automated' where it is carried out without human intervention . . . ," https://www.dataprotection.ie/en/individuals/know-your-rights/your-rights-relation-automated-decision-making-including-profiling; Australian Omudsman: ". . . .[AMA} make[s] decision without the direct involvement by a human being at the time of the decision," https://www.ombudsman.gov.au/__data/assets/pdf_file/0030/109596/OMB1188-Automated-Decision-Making-Report_Final-A1898885.pdf; Grindr: "process of making a decision by automated means without human involvement," https://blog.grindr.com/blog/automated-decision-making-and-grindr; Washington State SB 5116: "automated final decision system is 'an automated decision system that makes final decisions, judgements, or conclusions without human intervention,'" https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116.pdf?q=20230327135742.).

certain circumstances counsel against an overly broad right to opt out of all automated decisionmaking. Therefore, the regulations should encourage companies to adopt a risk-based approach that focuses on outcomes from automated decisionmaking that could have a harmful impact on consumers. When a consumer is served an advertisement based on an inferred interest in cross-country skiing, the harm to the consumer is small to nonexistent. Conversely, when a consumer is subjected to tailored advertising that pertains to eligibility determinations, there is a greater risk of harm or disparate impact. This is where there is an essential intersection with the requirement for companies to provide DPAs. During this process, companies should consider the role automated decisionmaking plays and the potential increased risk to consumers, ultimately determining where human oversight of an automated decision would be beneficial.

The NAI's self-regulatory approach has always tried to maintain a harms-first mentality. For example, in our Precise Location Information Solution Provider Voluntary Enhanced Standards ("Enhanced Standards"), we focus on the harms that come from processing and sharing personal information about certain sensitive Points of Interest, rather than an outright bar on the collection of all location information.[7] This allows for positive use cases–such as serving a consumer an advertisement for a local coffee shop when they search for "coffee shops near me"--while preventing negative, harmful outcomes, such as inferring a consumer is a part of the LGBT community based on a visit to a gay bar.

## IV. Conclusion

Again, the NAI appreciates the opportunity to submit comments to the Agency on this important topic. 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)

[7] NETWORK ADVERTISING INITIATIVE, *NAI Precise Location Information Solution Provider Voluntary Enhanced Standards* (June 22, 2022), https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/#:~:text=The%20Enhanced%20Standards%20create%20restrictions,LGBTQ%2B%20identity%2C%20and%20other%20places.