Network Advertising Initiative
409 7th Street NW, Suite 250
Washington, DC 20004

March 27, 2020

VIA ELECTRONIC MAIL: PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Second Set of Modifications to the Proposed Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

The Network Advertising Initiative ("NAI") is pleased to submit these comments regarding the second set of modifications to the regulations proposed for adoption[1] under the California Consumer Privacy Act of 2018 (the "CCPA").[2]

The NAI is looking forward to the conclusion of the rulemaking process and appreciates the continued efforts of the Office of the Attorney General ("OAG") to that end. The NAI has identified several issues in the second set of modifications to the proposed regulations (the "Regulations") that would benefit from further clarifications and changes before the Regulations are finalized, discussed below.

Overview of the NAI

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising in multiple media, including web, mobile, and TV.

[1] CAL. CODE REGS. tit. 11, §§ 999.300-341 (proposed March 11, 2020).
[2] CAL. CIV. CODE §§ 1798.100 *et seq.*

All NAI members are required to adhere to the NAI's FIPPs-based,[3] privacy-protective Code of Conduct (the "NAI Code"), which has undergone a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy.[4] Member compliance with the NAI Code is promoted by the NAI's strong accountability program, which includes a comprehensive annual review by the NAI staff of each member company's adherence to the NAI Code, and penalties for material violations, including potential referral to the Federal Trade Commission. These annual reviews cover member companies' business models, privacy policies and practices, and consumer-choice mechanisms.

Several key features of the NAI Code align closely with the underlying goals and principles of the CCPA and the Regulations. For example, the NAI Code requires member companies to provide consumers with an easy-to-use mechanism to opt out of different kinds of Tailored Advertising,[5] to disclose to consumers the kinds of information they collect for Tailored Advertising, and to explain how such information is used.[6] The NAI Code's privacy protections go further than the CCPA and the Regulations in some respects. For example, the NAI Code includes outright prohibitions against the secondary use of information collected for Tailored Advertising for certain eligibility purposes, such as credit or insurance eligibility, regardless of whether such information is ever sold, and even when a consumer has not opted out of Tailored Advertising.[7]

The NAI also educates consumers and empowers them to make meaningful choices about their experience with digital advertising through an easy-to-use, industry-wide opt-out mechanism.[8]

---

[3] *See, e.g.,* 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.

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

[5] *See, e.g., id.* § II.C.1.a. The NAI Code defines Tailored Advertising as "the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device. Tailored Advertising includes Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting. Tailored Advertising does not include Ad Delivery and Reporting, including frequency capping or sequencing of advertising creatives." *Id.* § I.Q. Capitalized terms used but not defined herein have the meanings assigned to them by the NAI Code. *See generally id.* § I.

[6] *See id.* § II.B.

[7] *See id.* § II.D.2.

[8] For more information on how to opt out of Tailored Advertising, please visit http://optout.networkadvertising.org.

Part I: Definitions

A. The Regulations should include guidance on the definition of personal information.

The first set of modifications to the Regulations added a new section titled "Guidance Regarding the Interpretation of CCPA Definitions," which consisted of guidance on the CCPA's definition of "personal information," as follows:[9]

> *Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."*

In the NAI's comments on the first set of modifications to the Regulations,[10] we requested further clarification from the OAG as to when IP addresses would not be considered personal information. However, the second set of modifications to the Regulations did not provide any further guidance, and instead deleted the above guidance.

Removing this guidance without explanation is likely to cause confusion among businesses as they struggle to understand the OAG's intent in proposing the guidance in the first place (which many businesses will presume remains the OAG's intent, notwithstanding the deletion of the language). Further, there likely still are circumstances wherein an IP address does not meet the statutory definition of personal information. For example, merely establishing a TCP/IP connection essential to all internet communications involves collecting the IP address of the device; however, many website operators (like bloggers or other small business website operators) that are technically "collecting" IP in this way do not, and could not reasonably, connect that information to a particular consumer or household. Unfortunately, with the deletion of the guidance, it is now very unclear whether the OAG's expectation is for those businesses to treat their unavoidable and purely technical collection of IP addresses as involving personal information.

Consistent with our previous comments, the NAI recommends restoring the guidance on the definition of "personal information," but further clarifying it by specifying that information such as an IP address is not personal information unless the business processing such information

[9] CAL. CODE REGS. tit. 11, § 999.302 (proposed Feb. 10, 2020).
[10] *See* Letter from Leigh Freund, President & CEO, Network Advert. Initiative, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice 3-4 (Feb. 25, 2020), https://www.networkadvertising.org/sites/default/files/nai_comment_letter_-_ccpa_modified_proposed_regulations_february_25_2020.pdf.

has linked it, or reasonably could link it, with additional pieces of information known by the business to identify a particular consumer or household, such as name and residential address.

Recommended Amendments to the Regulations:

Section 999.302(a)

Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, if a business collects the IP addresses of visitors to its website but does not link the IP addresses to any information known by the business to identify a particular consumer or household, such as a full name and residential address, and could not reasonably link the IP addresses with such information, the IP addresses would not be "personal information."

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. **The proposed regulations should clearly specify that businesses are not required to honor global privacy controls that do not represent an authentic consumer choice to opt out of sales.**

The second set of modifications to the Regulations include a change that could be interpreted as allowing software developers that will offer global privacy controls to offer those controls set "on" by default, despite the reality that the consumer using the control may never have interacted with those default settings, nor intended to opt out of a business's sale of personal information.[11]

However, in order for the Regulations to implement the letter and spirit of the CCPA, it is imperative that they clearly stipulate the need for consumers to affirmatively elect to opt out of sales of personal information. If software developers aren't clearly prohibited from setting global privacy controls to "on" by default, that would risk reversing the CCPA's intended opt-out framework and put the onus on consumers to take affirmative steps to turn off global privacy controls (*i.e.*, forcing them to opt in). This would muddle the clear intent of the CCPA (and the original draft regulatory language) to establish a framework where businesses are permitted to sell personal information, subject to a consumer's right to opt out of those sales.

For example, suppose that a web browser developer updates its web-browsing software to include a new "do not sell" signal. Under the second set of modifications to the Regulations,

[11] *See* CAL. CODE REGS. tit. 11, § 999.315(d)(1) (proposed March 11, 2020) (removing the language prohibiting privacy controls from using pre-selected settings).

that developer would not have as clear an indication that such a signal could not be turned on by default.[12] In that case, and even assuming that the browser adequately notified users about the "do not sell" mechanism and informed them that it is turned on by default, users of the browser would still be in the position of having to take affirmative action to turn off the opt-out signal. This would present substantial challenges for businesses trying to determine which opt-out signals represent true consumer requests to opt out of sales, and which are contentless default settings. If the final regulations take this approach, it will likely result in extensive confusion in the marketplace.

If the language clearly prohibiting default settings is not restored, it will also put NAI member companies in the difficult position of needing to comply with the unambiguous requirement in the Regulations to honor "user-enabled" privacy controls[13] without any equally clear indication in the Regulations that software developers may not send opt-out signals by default. As highlighted above, the possibility of default-on settings is not consistent with the statute, and will undermine the ability of NAI member companies to determine in which cases a global privacy control is truly user-enabled (not enabled by software developers). For example, if a web browser ships an update with a "do not sell" setting on by default, the Regulations do not appear to require businesses to honor that signal because it is not "user-enabled." However, if a user were to toggle the setting off for a time, and then toggle it back on at a later time, it arguably *would* be user-enabled. But businesses receiving the signal would have no way of differentiating which opt-out signals from that type of browser are user-enabled and which are not. As such, the best way to ensure that user-enabled global privacy settings are consistently honored is to clearly prohibit them from being set on by default. That way, businesses will know that whenever they encounter such signals, they were enabled by the user.

Finally, and not least of all, the proposed change places enormous discretion in the hands of large browser providers, who often are large businesses with significant data assets, and in some cases have their own advertising operations. Giving them the ability to control – virtually unilaterally, without consumer choice – the data rights of their (generally much smaller) competitors implements a business framework that is structurally anti-competitive. Even ascribing the best of intentions to those browser companies, by implementing a data rights structure that permits the largest of companies to control the data rights and data inventories of their competitors is a bad idea – at a minimum, it will deter competition and market entry. It is thus anti-competitive and ultimately will narrow choices for advertisers, publishers and consumers by significantly limiting competition (and presumably, driving up prices) in a US market that is vital to both advertisers (large and small), content publishers, and news organizations.

For those reasons, the NAI recommends that the Regulations be amended to restore the language prohibiting pre-selected opt-out settings:

---

[12] *See id.*
[13] *See id.*

Recommended Amendments to the Regulations:

Section 999.315(d)(1):

Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.

Part III: Service Providers

A. The proposed regulations should further clarify permissible internal uses of personal information by service providers obtained in the course of providing services.

The first set of modifications to the Regulations referred to a service providers' ability to "clean" or "augment" data acquired from another source.[14] The NAI advocated for removing reference to the terms "cleaning" and "augmenting" because they are not defined by the CCPA or the Regulations, and have no common meaning in the digital advertising industry.[15] Imposing requirements on service provider activity using terms without definitions or accepted meanings is likely to lead to inconsistent interpretations of those requirements. Nonetheless, the second set of modifications to the Regulations retained the basic structure of the requirement, but changed the word "cleaning" to "correcting."[16]

Even with this change, the Regulations are likely to cause confusion as to when service providers may engage in the simple and beneficial practice of improving the quality of data provided by one business with data already acquired from another business. The ability of service providers to improve the accuracy of data used by businesses they serve in this way does not present any appreciable risk to consumer privacy – but confusion about whether the Regulations permit it would lead to additional costs to businesses who may end up directing communications to consumers using, *e.g.*, an email or physical mailing address with a typo or other error. Costs for errors like that may run into the billions of dollars per year.[17] Those errors may also prevent consumers from receiving mis-directed communications.

To address the issues identified above, the NAI recommends further amending the Regulations as follows.

---

[14] CAL. CODE REGS. tit. 11, § 999.314(c)(3) (proposed Feb. 10, 2020).
[15] *See* Letter from Leigh Freund, President & CEO, Network Advert. Initiative, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice 14 (Feb. 25, 2020), https://www.networkadvertising.org/sites/default/files/nai_comment_letter_-_ccpa_modified_proposed_regulations_february_25_2020.pdf.
[16] CAL. CODE REGS. tit. 11, § 999.314(c)(3) (proposed March 11, 2020).
[17] *See* Letter from Kenneth M. Dreifach, Shareholder, ZwillGen, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice (Feb. 25, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf.

Recommended Amendments to the Regulations:

Section 314(c)(3):

A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except . . . [f]or internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business~~, or correcting or augmenting data acquired from another source~~.

Part IV: Enforcement

A. The OAG should delay enforcement of the Regulations until March 1, 2021

The NAI appreciates the fact that the OAG has engaged so thoroughly with the CCPA rulemaking process by carefully considering several rounds of written comments and making modifications to the Regulations where appropriate, including a number of material changes that affect compliance obligations for businesses. However, an inevitable consequence of that deliberative process is a rapidly diminishing timeline for businesses to understand and implement the final regulations.

There are a mere 66 working days until the July 1st enforcement date for the CCPA as of the writing of this letter.[18] However, businesses cannot reasonably plan compliance with the complex requirements of the Regulations before they are finalized. Further, businesses will likely have far fewer than 66 business days to prepare, as the OAG will need time to review this round of comments (even assuming there are no further material modifications), and the Office of Administrative Law may take up to 30 working days to approve the final regulations.[19]

Coming into material compliance with final regulations on such a short timeline would be extraordinarily difficult for businesses in ordinary times; however, the global COVID-19 pandemic has put unprecedented strain on the resources of NAI member companies and the entire global economy. The closing of physical workplaces has made collaboration difficult across and among product, legal and engineering teams, not to mention the human dimension of the pandemic. Concentrating resources into short-term compliance efforts would place further strain on businesses already struggling to maintain normal operations in the face of both office closures and increased childcare and education responsibilities of employees with children whose schools have closed.

Due to the already dwindling time until July 1st, and these uniquely difficult circumstances, the NAI respectfully requests a delay in the OAG's enforcement of the CCPA until March 1, 2021.

[18] *See* CAL. CIV. CODE 1798.185(c).
[19] https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-rulemaking-fact-sheet.pdf

Conclusion:

The NAI is grateful for the opportunity to comment on the Regulations. If we can provide any additional information, or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact Leigh Freund, President & CEO (leigh@networkadvertising.org) or David LeDuc, Vice President, Public Policy (david@networkadvertising.org).

******

Respectfully Submitted,

The Network Advertising Initiative

BY: Leigh Freund
President & CEO