February 25, 2020

California Office of the Attorney General
ATTN: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

Submitted via privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Proposed Modified Regulations

The Interactive Advertising Bureau ("IAB") provides these comments on the proposed modified regulations issued by the California Attorney General ("AG") on February 10, 2020 to implement the California Consumer Privacy Act ("CCPA").

Founded in 1996 and headquartered in New York City, the IAB (www.iab.com) represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, our members account for 86 percent of online advertising in the United States. In California, we contribute $168 billion to the state gross domestic product and support over 478,000 full-time jobs in the state.[1] Working with our member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. The organization is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of our public policy office, the IAB advocates for our members and promotes the value of the interactive advertising industry to policymakers and legislators across the country.

IAB broadly supports the CCPA's purpose and intent to enhance consumer privacy by providing transparency and choice about the use of personal information. And we appreciate the AG's consideration of our comments to the AG from December 6, 2019. However, certain provisions of the modified rules continue to stray from or contradict the text of the CCPA itself. Other provisions, as drafted, may ultimately reduce consumer choice and undermine privacy, rather than advancing it. IAB urges the AG to consider consumers' support for the ad-driven Internet model and asks the AG to update the modified rules so they empower consumers by giving them increased choices and control over online data. IAB provides the following comments below, addressing specific provisions of the modified rules that should be updated or clarified to further consumer choice and privacy and enable compliance with the law.

I. Update the Guidance Regarding the Definition of "Personal Information" to Encourage Privacy by Design

[1] John Deighton, *The Economic Value of the Advertising-Supported Internet Ecosystem* (2017), available at https://www.iab.com/insights/economic-value-advertising-supported-internet-ecosystem/.

The modified regulations state as an example that "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."[2] Businesses that maintain pseudonymous information such as an IP address are often structured to separate that non-identified information from a consumer's identity. Furthermore, businesses often apply security measures, such as encryption, and administrative controls, such as contractual requirements, to further protect the consumer. The modified regulations do not clarify what would constitute the ability to "reasonably link" information with a particular consumer or household. They consequently emphasize an indeterminate and ambiguous standard in the definition of personal information without providing any clarity as to what it means. We encourage the AG to recognize privacy by design measures taken by businesses to separate identifiable data from non-identifiable data and clarify the draft rules by modifying section 999.302 as follows:

> *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."*

II. Clarify that Notice Obligations for Data Brokers Apply to Explicit Notice

The modified regulations state that "a business that does not collect information directly from consumers [that] is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, et seq…. does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out."[3]

However, the regulations do not specifically indicate whether or not this section also applies to the explicit notice requirements for onward sales of personal information about a consumer by a third party that appear in the text of the CCPA. The CCPA itself states that a third party may not "sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provide an opportunity to exercise the right to opt-out pursuant to Section 1798.120."[4] We ask the AG to clarify that a business has met its "explicit notice" and opt-out opportunity requirements under 1798.115(d) if it is registered as a data broker and includes in its registration submission a link to its online privacy policy with instructions on how a consumer can submit a request to opt-out. This clarification would help bring the CCPA's express provisions regarding explicit notice in line with the modified proposed rules' terms, thereby enhancing clarity and consistency within the CCPA's regulatory framework.

[2] Cal. Code Regs. tit. 11, § 999.302(a) (proposed Feb. 10, 2020).
[3] *Id*. at § 999.305(d).
[4] Cal. Civ. Code § 1798.115(d).

III. Ensure Requirements for an Opt-Out Button Align with CCPA Requirements

The CCPA requires businesses to "[p]rovide a clear and conspicuous link on the business's internet homepage, titled 'Do Not Sell 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 of the consumer's personal information."[5] The modified regulations state that "[w]hen the opt-out button is used, it shall appear to the left of the 'Do Not Sell My Personal Information' or 'Do Not Sell My Info' link as demonstrated below, and shall be approximately the same size as other buttons on the business's webpage."[6] This provision of the draft regulations is ambiguous and fails to capture the nuances of providing consumer choice across diverse contexts and applications. It refers to "the opt-out button" generally, and therefore it is unclear whether the regulation is specifying that businesses must place the button *next to* the "Do Not Sell My Personal Information" link on their webpage, or whether the regulation is only requiring a toggle button, and unclearly describing where the toggle button is required to be placed. It is also unclear whether the toggle button or the opt out link itself must "link to a webpage or online location containing the information specified in section 999.306(c)."

In order for this instruction from the AG to be consistent with the requirements of the CCPA, the AG should clearly state that when used, a toggle button is required to be placed next to the words "Do Not Sell My Personal Information" or "Do Not Sell My Info" on an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information." The regulations need to make clear that a toggle button is not required to be placed on a business's homepage next to the "Do Not Sell My Personal Information" link or in the business's privacy policy.

IV. Remove the Requirement to Provide an Estimate of the Value of Consumer Data and the Method of Calculating the Value of Consumer Data in a Notice of Financial Incentive

If a business offers a financial incentive or a price or service difference to a consumer in exchange for the retention or sale of personal information, the proposed regulations require the business to provide a notice to the consumer that includes: (1) a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and (2) a description of the method the business used to calculate the value of the consumer's data.[7] IAB respectfully asks the AG to remove the requirement to provide an estimate of the value of the consumer's data and the method of calculating such value, as these obligations are not contemplated by the CCPA itself, would be difficult if not impossible for a business to provide, and could potentially reveal confidential or proprietary information about the business's internal practices and economic assessments.

First and foremost, the requirement to provide an estimate of the value of the consumer's data and the method of calculating such data exceeds CCPA's statutory obligations. These provisions of the proposed regulations represent brand new business obligations that were not

[5] *Id*. at § 1798.135(a)(1).
[6] Cal. Code Regs. tit. 11, § 999.306(f)(2) (proposed Feb. 10, 2020).
[7] *Id*. at § 999.307(b)(5).

included in the text of the CCPA itself. Businesses have spent over a year preparing for the CCPA's effective date of January 1, 2020. Adding substantial and disruptive new requirements to the CCPA, such as these requirements related to financial incentives, mere months before the law will go into effect causes significant compliance complications and challenges for businesses of all sizes.

Second, it may be impossible for businesses to comply with the requirement to provide an estimate of the value of the consumer's data, because data lacks clear, objective value. Academics have come up with wildly different estimates for the value of data-enabled services,[8] and experts are likely to come up with differing values for these services in the future as well. The reason certain businesses can offer their services free of charge is because they derive revenue from selling advertisements. Businesses sell advertisers the opportunity to present their messages to users, and advertisers pay businesses based on objective metrics such as the number of people who see their ads or the number of people who click on their ads. As a result, any revenue linked to a particular advertising campaign is determined when the campaign is completed. The final figures, however, have little relation to any single consumer's data, and thus providing an estimation of the value of such data would be inaccurate and misleading to consumers.

Finally, the requirement to provide an estimate of the value of the consumer's data and the method for computing such value could expose confidential, proprietary business information or put a business's competitive position at risk.[9] The method by which a business values personal information associated with a consumer may constitute proprietary information about the business's commercial practices. Forcing businesses to reveal such confidential, secret information could harm businesses' ability to compete in the marketplace, as competitors and customers would become aware of the value a business has assigned to the data it maintains. Obligating businesses by law to reveal this information could harm the economy and healthy business competition by forcing companies to reveal confidential information.

For the foregoing reasons, IAB asks the AG to remove the proposed regulations' requirement that a business must, in a notice of financial incentive, provide an estimate of the value of the consumer's data and the method by which it calculated such value. This directive constitutes a requirement that goes far beyond the requirements of the CCPA itself.

V. Ensure Requirements for Requests to Know and Delete Align with the CCPA's Text, Consider Real-World Implications, and Empower Consumer Choice

Certain provisions in the proposed regulations set forth rules about consumer requests to know and requests to delete that do not align with the CCPA, and other portions of the proposed

[8] Asha Saxena, *What is Data Value and should it be Viewed as a Corporate Asset?* (2019), located at *https://www.dataversity.net/what-is-data-value-and-should-it-be-viewed-as-a-corporate-asset*.

[9] IAB also respectfully disagrees with the AG's assessment that providing consumers with these calculations will provide meaningful information about the costs and benefits of the financial incentive to the consumer specifically. *See* Office of the California Attorney General, *Initial Statement of Reasons for Proposed Adoption of California Consumer Privacy Act Regulations* at 12 (Oct. 2019) (hereinafter, "ISOR"), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccps-isor-appendices.pdf. The calculations described in the proposed regulations reflect the value proposition to the business, not to the consumer, as expressly indicated in Section 999.301(w).

regulations fail to consider significant real-world outcomes associated with their requirements. Finally, some of the provisions thwart consumers' ability to make choices and require businesses to take action on personal information in ways that may not be approved by the consumer. IAB requests that the AG update the proposed rules, as further described below, to conform them with the CCPA's text, better align them with practical realities, and empower consumers to make meaningful choices that businesses must respect.

a. Expressly acknowledge that a business may withhold specific pieces of personal information if divulging such information could lead to unreasonable security risks

The modified regulations remove language that states "[a] business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."[10] The modified regulations replace this language with language relating to when a business is not required to search for personal information when responding to requests to know.

In many instances, businesses may not be able to verify consumers to a degree of certainty necessary to disclose specific pieces of personal information. For example, a business may maintain data that would not, on its own, be associated with a named actual consumer. For example, a company may associate a random ID number with other non-identifying information about a consumer for internal use only. Because this information may not be tied to actual consumer names or identifying information, businesses holding such information may not be able to verify a consumer's request for specific pieces of personal information to a "reasonably high degree of certainty," as the consumer may not be able to provide "pieces of personal information" the business would need to verify the consumer's request.[11] However, in the absence of clear guidance, as provided in the previous draft regulation, that a business shall not provide consumers with specific pieces of information, a business may feel compelled to divulge the information it maintains due to a legal requirement. This result could put the consumer, the consumer's information, and/or the business at unreasonable risk, such as unauthorized access. Such a requirement would be contrary to the intent of CCPA and less privacy protective for consumers. IAB requests that the AG reinsert the provision that was deleted from section 999.313(c)(3) that enables a business to decline to provide specific pieces of information to a consumer if doing so would create a substantial, articulable, and unreasonable risk to the security of that personal information.

b. Provide needed improvements on the scope of the right to know considering the burden on businesses.

The modified regulations include new limitations on when a business is required to search for personal information in response to a request to know.[12] However, these limitations are too narrow to effectively protect consumers from the risks associated with identifying,

[10] Cal. Code Regs. tit. 11, § 999.313(c)(3) (proposed Feb. 10, 2020).
[11] Cal. Code Regs. tit. 11, § 999.325(c) (proposed Feb. 10, 2020).
[12] Cal. Code Regs. tit. 11, § 999.313(c)(3) (proposed Feb. 10, 2020).

compiling, and making available upon request detailed information. Furthermore, the modified regulations create significant costs for businesses.

Under the proposed regulations, a business would not be required to search for personal information that the business (1) does not maintain in a searchable or reasonably accessible format; (2) maintains solely for legal or compliance purposes; and (3) does not sell and does not use for any commercial purpose. In most instances, it is unlikely that personal information would meet these requirements. As a result, the proposed regulations provide for few practical limitations on access requests, and businesses could be required to associate information with an identifiable consumer than they would otherwise keep separate and secure. IAB suggests the AG revise the regulations to permit businesses not to provide personal information that meets any, rather than all, of the conditions in section 999.302(c)(3). In addition, IAB suggests an new limitation in section 999.302(c)(3) for personal information the business does not associate with an identifiable consumer in the ordinary course of business.

VI. The AG Should Modify Service Provider Requirements to Provide Greater Certainty and Align with Business Realities

The modified regulations exclude "cleaning or augmenting data acquired from another source" as a permissible internal use by a service provider.[13] The regulations do not define these new terms. To avoid unnecessary confusion, better align the text of the regulations with the legislative intent of the CCPA, and preserve service provider uses that have clear consumer privacy benefits, IAB asks that the AG remove "cleaning or augmenting data acquired from another source" from the modified regulations.

The ability of service providers to conduct ordinary business activities, such as updating data with a service provider's data, provides a variety of benefits to consumers. For example, cleaning or augmenting data could include activities that allow service providers to correct personal information and better ensure that it is accurate, which enhances consumer privacy. Without this ability, for example, service providers would not be able to accurately update consumers' postal addresses when they relocate. This could result in consumers receiving mail and other information, such as offers and notices, that are not relevant to or intended for them. Consequently, restricting service providers' ability to clean data could result in consumers receiving more information than they presently do. Service providers' ability to internally clean and augment personal information to improve services makes the overall market more efficient and provides a benefit to both consumers and businesses alike. Accordingly, this valuable and privacy enhancing activity should not be limited or restricted.

VII. The AG Should Remove the Obligation for Businesses to Comply with User-Enabled Privacy Controls, Such as Browser Settings

The proposed regulations state that "[i]f a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted… for that

[13] *Id*. at § 999.314(c)(3).

browser or device, or, if known, for the consumer."[14] This proposed regulation exceeds the CCPA's scope, imposing new substantive requirements on businesses that the legislature has previously considered and elected to not include.[15] We request that the AG remove this requirement, or alternatively, where a business offers a "Do Not Sell My Info" link as a means to opt out from sale, the business should not be required to treat the proposed user-enabled privacy controls as a verifiable opt-out request. Such an approach would be consistent with the approach taken by the legislature when it amended the California Online Privacy Protection Act.

Mandating that businesses treat browser-based signals as valid consumer opt-out requests removes the option for consumers to make their own choices regarding the selling of personal information directly with relevant businesses. Given the CCPA's broad definition of sale, which may cover a range of activities that the ordinary consumer would not regard as a "sale" of personal information, it is further questionable whether a global device setting accurately reflects this intent on the part of consumers. Such settings mean that consumers would be limited from allowing some businesses to sell data while prohibiting others from engaging in these uses. This result would remove meaningful consumer choice from the marketplace and reduce the options available to consumers to set personalized preferences for the use and transfer of data.

In addition, requiring businesses to honor user-enabled privacy controls could enable intermediaries to tamper with or block the individualized choices that consumers communicate directly to businesses. For example, intermediaries can interfere with businesses that use plugins, cookies, JavaScript, and other technologies to catalog and act on consumer preferences. Intermediaries such as browsers stand between consumers and businesses in the Internet ecosystem and provide no way for individual businesses to verify whether an expressed privacy control signal is truly a consumer-set preference. These parties are able to manipulate signals and alter settings in ways that may not reflect actual consumer preferences and could potentially stand in the way of a consumer's actual choice being expressed or communicated to a business. As such, concentrating power in the hands of these intermediaries could hinder consumers' from seeing their actual choices expressed in the marketplace, which could have a negative revenue impact on the publishers and services consumers rely on and trust.

The AG takes the position that in the absence of mandatory support for privacy controls, "businesses are likely to reject or ignore consumer tools."[16] While it is true that adoption of certain existing privacy controls has varied across publishers and platforms (*i.e.*, adoption of the Do-Not-Track standard), IAB urges the AG to recognize that the CCPA is without precedent and represents a fundamental shift in California privacy law. IAB expects to see market forces continue to drive strong demand for compliance solutions that can facilitate both consumer choice and business compliance. Throughout the online ecosystem, IAB also expects to see consumers take advantage of multiple compliance solutions, informed by privacy notices directing consumers on how to communicate their privacy choices. Mandating that businesses respect ill-defined global opt-out technologies could impede the development of various helpful tools and solutions for consumers to use to exercise choice in the marketplace, increasing the

[14] *Id*. at § 999.315(d).
[15] *See* AB 370 (Cal. 2013); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).
[16] *See* ISOR at 24.

likelihood of disharmonized and conflicting signals. This could create confusion and uncertainty for consumers and businesses alike.

For these reasons, and in light of significant issues around reliability and authenticity of browser-based signals as well as difficulties with clearly communicating which consumers are California residents, it would be premature to regulate in this area or mandate that every business comply with each and every type of user-enabled signal developed to facilitate CCPA compliance. We therefore respectfully ask the AG to remove the requirement to treat user-enabled privacy controls as valid requests to opt out of personal information sale and update the draft rules so that businesses may respect such user-enabled controls *or* offer consumers with another workable method to opt out of personal information sale, such as a "Do Not Sell My Personal Information" button.

VIII. Provide Additional Flexibility for the Two-Step Requirement for Opting In to the Sale of Personal Information

Per the proposed rules, if a consumer wishes to opt in to the sale of personal information after previously opting out of such sale, the consumer must undertake a two-step process to confirm their choice to opt in.[17] "Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in."[18] This two-step requirement creates unnecessary friction in the user experience and makes it more difficult for businesses to take action to effectuate a consumer's valid choice to opt in to personal information sale. Businesses should be able to accept a consumer's single communication of a desire to opt in to personal information sale as a legitimate consumer preference and should be able to act on that validly communicated consumer choice. IAB therefore requests that the AG reconsider this requirement to empower businesses to act on consumers' expressed choices to opt in to personal information sale after previously opting out.

IX. Clarify that Businesses Need Not Keep Records About Opt Out Requests Served on Other Businesses

The proposed regulations require all businesses to "maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months."[19] This requirement creates compliance challenges for businesses when it comes to retaining records about consumer opt-out requests depending on the actual entity that is effectuating the opt out. For example, in many situations in the online Internet ecosystem, first-party publisher businesses may not have any control over or the ability to know how a third-party business responds to a consumer's opt-out choice. IAB therefore asks the AG to clarify that businesses only must keep records about the opt out requests they receive directly from consumers and the actions the business itself took to respond to those requests. Businesses should not be required to maintain information about other businesses' responses to consumer opt out requests.

[17] Cal. Code Regs. tit. 11, § 999.316(a) (proposed Feb. 10, 2020).
[18] *Id.*
[19] *Id.* at § 999.317(b).

X. Affirm that Businesses Are Not Required to Identify Pseudonymized Information Stored in a Manner that is Non-Identifiable and Not Associated with an Actual Person

The proposed regulations state that "[w]henever feasible," a business must "match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service" in order to verify a consumer request.[20] This requirement threatens to destroy the longstanding privacy-protective business practice of keeping pseudonymized and non-identified personal information separate from personal information that could identify a consumer. In addition, this requirement may contravene a provision in the proposed regulations stating that "[i]f a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request," a concept that is also mirrored in the CCPA itself.[21] IAB therefore asks the AG to clarify that businesses are not required to identify pseudonymized information stored in a manner that is non-identifiable and not associated with a named actual person in order to effectuate CCPA requests.

Businesses that maintain non-identified data such as cookie or device IDs are usually structured to separate that non-identified information from a consumer's identity. This practice is privacy-protective for consumers, because it maintains a level of anonymity for the consumer within the business's database. Without an update to the proposed rules, businesses may feel compelled to collect information from consumers so that they can associate or combine non-identifiable personal information with identifiable personal information to meet the CCPA's verification requirements. IAB therefore respectfully asks the AG to clarify the proposed rules such that businesses do not need to identify non-identified information with a named actual person in order to facilitate CCPA requests. This clarification would benefit consumers by keeping non-identified data separate from other personal information that directly links it to an identified consumer.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the AG on developing final regulations to interpret the CCPA. If you have questions, please contact me at 202-800-0770.

Respectfully submitted,

Alex Propes
Vice President, Public Policy & International
Interactive Advertising Bureau

[20] *Id*. at § 999.323(b)(1).
[21] Cal. Civ. Code § 1798.145(k); Cal. Code Regs. tit. 11, § 999.323(f) (proposed Feb. 10, 2020).