December 6, 2019

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 Regulations

The Interactive Advertising Bureau ("IAB") provides these comments on the proposed regulations issued by the California Attorney General ("AG") on October 11, 2019 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.

The modern U.S. economy is dependent on data, and consumers derive substantial benefit from the data-driven economy. The free flow of data and information online benefits consumers by enabling access to innovative and informative content, as well as products and services. and by subsidizing the vast and varied offerings that are available to consumers through the Internet. Data-driven advertising plays a substantial role in this ecosystem by making it possible for businesses to provide low or no cost content and services to consumers through video, news, music, and much more. In fact, a recent study by Harvard Business School Professor John Deighton found that in 2016, the U.S. ad-supported Internet created 10.4 million jobs and the data-driven ad industry added 1.121 trillion to the U.S. economy, doubling its contribution over just four years and accounting for 6 percent of U.S. gross domestic product.[2] Other studies and surveys show that consumers are aware that online products and services are enabled by data collected about their interactions and behavior online, and they support that exchange of value. For instance, a Zogby survey commissioned by the Digital Advertising Alliance found that 85 percent of consumers surveyed stated they like the ad-supported Internet,

[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/.
[2] *Id.*

and 75 percent indicated that they would greatly decrease their engagement with the Internet if another model were to take its place.[3]

IAB broadly supports the CCPA's, and the proposed regulations', purpose and intent to enhance consumer privacy by providing transparency and choice about the use of personal information. However, certain provisions of the proposed rules 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. Finally, a few provisions set forth entirely new obligations for businesses that will be excessively burdensome to implement. IAB urges the AG to consider consumers' support for the ad-driven Internet model and asks the AG to update the proposed 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 proposed rules that should be updated or clarified to further consumer choice and privacy and enable business compliance with the law.

I. Allow Businesses the Flexibility to Provide Effective Notices At or Before the Point of Personal Information Collection

The proposed regulations provide information about how businesses must comply with the CCPA requirement to, "at or before the point of [personal information] collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."[4] As described in more detail below, IAB asks the AG to update the proposed regulations so they better align with the text of the CCPA and allow businesses flexibility in the mechanisms they may use to meet this requirement.

a. *Clarify that notices may be visible at the time personal information is collected*

The CCPA requires businesses that collect personal information to provide a notice at or before the point of collection of the categories of personal information the business collects and the purposes for which the categories are used.[5] The proposed regulations helpfully state that businesses that collect personal information from consumers online may give such a notice by providing a link to the section of the business's privacy policy that contains the required information.[6] However, the proposed regulations also state that the notice must "[b]e visible or accessible where consumers will see it *before any personal information is collected*."[7] This contradicts the CCPA, which clearly requires a notice *at or before* the point of personal information collection. We ask the AG to update this provision in the proposed regulations to reflect the statute.

In addition, the AG's draft rule does not align with common market practice online. A business typically begins collecting personal information when a consumer visits an online

[3] DAA, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.
[4] Cal. Civ. Code § 1798.100(b).
[5] *Id*.
[6] Cal. Code Regs. tit. 11, § 999.305(c) (proposed Oct. 11, 2019).
[7] *Id*. at § 999.305(a)(2)(e) (emphasis added).

website, service, or mobile application owned by the business. It is therefore difficult to imagine how a business could serve a notice to a consumer before the point of personal information collection. As such, we ask the AG to modify Section 999.305(a)(2)(e) of the draft regulations to clarify that notice at or before the point of collection must be visible *at the time of* or before any personal information is collected. This update would bring the proposed regulations into conformity with the CCPA's text and better reflect what is possible given the realities of the online data-driven ecosystem.

b. *Clarify that businesses may make new uses of collected personal information by providing notice of the new use to the consumer*

The CCPA states that a business may not "collect additional categories of personal information or use personal information collected for additional purposes [other than those identified in the notice at collection] without providing the consumer with notice" of such new categories of personal information or additional purposes.[8] However, the proposed regulations state that "[i]f the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use *and obtain explicit consent* from the consumer to use it for this new purpose."[9] This "explicit consent" requirement in the proposed regulations does not align with the CCPA's text, which focuses exclusively on notice to the consumer and does not refer to explicit consent. This point is further supported by the CCPA's definition of one of the exceptions to the "sale" definition where a third party assumes control of a business and makes a material change to the privacy policy, noting a prominent notice requirement, but not mentioning a consent requirement.[10] We ask the AG remove the following language "*and obtain explicit consent* from the consumer to use it for this new purpose" as it exceeds the scope of the CCPA's statutory language.

The requirement to obtain "explicit consent" for a new use of personal information moves beyond the CCPA's text and imposes a substantial requirement on businesses that was not intended by the California legislature when it considered and passed the CCPA. Such a requirement also would lead to an inconsistency in the CCPA requirements on when new data use occurs by a business versus a third party that assumes control of a business. Furthermore, this provision of the proposed regulations is clearly outside of the scope of the CCPA, as the law itself only requires businesses to notify consumers of a new use of data and does not require "explicit consent." IAB therefore asks the AG to revise the proposed regulation in line with the CCPA's text and remove the proposed requirement that businesses need to obtain "explicit consent" for such new uses.

c. *Allow third parties to rely on attestations from data suppliers stating that consumers were given notice and choice consistent with the CCPA*

According to the proposed regulations, although a business that does not collect information directly from consumers does not need to provide a notice at collection, such a

[8] Cal. Civ. Code § 1798.100(b).
[9] Cal. Code Regs. tit. 11, § 999.305(a)(3) (proposed Oct. 11, 2019) (emphasis added).
[10] Cal. Civ. Code § 1798.140(t)(2)(D).

business must take certain specific actions before selling personal information.[11] Before selling personal information, a business that does not collect information directly from consumers must either: (1) contact the consumer to provide notice of sale and notice of the right to opt-out of sale, or (2) confirm that the source provided a notice at collection, obtain signed attestations describing how the source provided such a notice, obtain an example of the notice, retain the attestations and example notices for at least two years, and make them available to consumers upon request.[12] IAB asks the AG to amend the proposed regulations so that businesses may rely on signed attestations from their immediate data suppliers that the consumer was given notice of personal information sale and an opportunity to opt-out only, and need not obtain samples of the notices that were provided to consumers, retain them, or make them available to consumers upon request. IAB also asks the AG to confirm that the attestations companies receive, and the example notices they may be required to maintain do not need to be returned to consumers in response to CCPA access requests.

Allowing entities to obtain contractual representations from their immediate data suppliers that the consumer was notified of personal information sale and the right to opt-out of such sale provides the same consumer benefits as requiring businesses to maintain an example of the notice that was actually provided to the consumer. The requirement to retain examples of the notice provided to consumers and to make them available at a consumer's request is unmanageable for businesses, as they could have to maintain thousands if not millions of notices. For example, in the programmatic advertising context where billions of data exchanges occur on a second-by-second basis, businesses would have no reasonable way to pass model notices to entities in the ecosystem that receive data. In addition, this provision could be interpreted to require businesses to pass example notices down the chain from the original source of data to other businesses who may receive personal information, which is an unrealistic and potentially impossible burden for businesses to meet. Consumers receive little if any additional benefits from the example notice requirement, as consumers receive the same level of transparency and choice through requiring businesses to obtain attestations that consumers were given such notices. Moreover, requiring businesses to obtain examples of the consumer notices that were provided and retain this information for two years would require companies to amend agreements that have recently been amended under prior interpretations of the CCPA.

In addition, IAB urges the AG to update the proposed rules so that businesses are not obligated to return the sample notices they may be required to maintain or the attestations they receive from data sources to consumers in response to access requests. The California legislature determined that businesses are not required to disclose particular data sources to consumers in response to access requests by expressly stating that the access right requires the disclosure of categories of sources of personal information and not the particular data sources themselves. In addition, a requirement to return attestations and sample notices to consumers in response to an access request runs the risk of exposing confidential or proprietary business terms to the public. Moreover, in a practical sense, it is unworkable for businesses to have to link individual data points to consumers and contractual terms.

[11] Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).
[12] *Id.*

IAB asks the AG to clarify that businesses may rely on signed attestations from their immediate data suppliers that the consumer was given notice of the personal information sale and an opportunity to opt-out. IAB also asks the AG to clarify that a business is not required to produce the attestations it receives from data sources or sample notices it may be required to maintain to a consumer in response to an access request.

To provide clarity on additional business cases, we would also ask that the AG clarify that a third party, without knowledge of presentation of an opt-out, may present the opt-out opportunity to the consumer, so long as the consumer has adequate notice of the third party's collection of the data at the time of collection. In this way, a third party may provide the opt-out service to its customers' consumers who are in the position of direct collection.

II. 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.[13] 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 is extralegal. These provisions of the proposed regulations represent brand new business obligations that were not 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, less than three 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,[14] and experts are likely to come up with differing values for these services in the future as well.

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

[13] *Id*. at § 999.307(b)(5).
[14] 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*.

or put a business's competitive position at risk.[15] Despite the challenges of estimating the value of the consumer's data, the method by which a business values personal information associated with a consumer in order to comply with their obligations under the proposed rule 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. Furthermore, the requirement could be impossible for businesses to effectuate and would risk distorting business competition.

III. 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 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. *Consistent with the text of the CCPA, enable businesses that have direct consumer relationships and operate exclusively online to provide an email address only for consumers to submit CCPA requests to know*

The CCPA, as recently amended by California AB 1564,[16] states that "[a] business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115."[17] However, the proposed regulations state that "[a] business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's

[15] 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* Initial Statement of Reasons at 12. The calculations described in the proposed regulation reflect the value proposition to the business, not to the consumer.
[16] AB 1564 (Cal. 2019).
[17] Cal. Civ. Code §§ 1798.105(a), (c).

website or mobile application."[18] The CCPA and proposed regulations are therefore directly at odds, as the CCPA requires businesses with direct consumer relationships that operate exclusively online to provide an email address only for consumers to submit requests to know, while the proposed regulations require a toll-free number and an interactive webform for businesses to receive such requests. IAB asks the AG to conform the proposed regulations to the text of the CCPA and clarify that businesses who maintain direct relationships with consumers and operate exclusively online must provide only an email address or webform for receiving consumer requests to know.

b. *Extend the time period within which businesses must confirm receipt of a request to know or delete and provide information about how the business will process the request*

The proposed regulations state that "upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 days and provide information about how the business will process the request."[19] This requirement is impractical for businesses, as it provides insufficient time for a business to decide how it will process a request. Ten days does not allow enough time for a business to fully vet a request, verify the identity of the requestor, ascertain whether it must avail itself of a permitted exception to fulfilling the request, or take any other due diligence steps necessary to be able to provide an accurate description of how it will process the request to the consumer. IAB therefore asks the AG to extend the time period within which businesses must confirm receipt of a request to know or a request to delete and provide information about how it will process a request. IAB suggests the AG extend the period to thirty days, which is a time period within which businesses must comply with consumer requests under other privacy regimes, such as the General Data Protection Regulation.

Furthermore, we ask that a business's request for information to verify a consumer's identity before effectuating a consumer request tolls or pauses the 45-day window within which the business must respond to the request. Consumer verification is necessary for businesses to accurately effectuate consumers' CCPA rights. Robust and accurate verification is in the interest of consumers, because without it, businesses run the risk of erasing or returning data that does not pertain to the requesting consumer.

c. *Confirm that businesses need not delete personal information if maintaining it is necessary to provide expected subscription messages*

The CCPA requires businesses to delete "any personal information about the consumer which the business has collected from the consumer" upon receipt of a verifiable consumer request.[20] The law exempts businesses from the need to delete personal information if maintaining it is necessary for the business to "provide a good or service… reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract with the consumer,"[21] but it does not explain what conduct can

[18] Cal. Code Regs. tit. 11, § 999.312(a) (proposed Oct. 11, 2019).
[19] *Id*. at § 999.313(a).
[20] Cal. Civ. Code §§ 1798.105(a), (c).
[21] *Id*. at § 1798.105(d)(1).

be considered "reasonably anticipated" within an "ongoing business relationship" with a consumer. IAB asks the AG to clarify this CCPA exception to the deletion right so that businesses may continue to provide expected subscription messages to consumers that are reasonably anticipated within the context of the business's ongoing relationship with a consumer.

We urge the AG to clarify what is "reasonably anticipated within the context of a business's ongoing business relationship with the consumer." Such a regulation should explicitly confirm that expected subscription messages are reasonably anticipated within an ongoing business relationship with a consumer that maintains a subscription with the company following a deletion request. If a consumer maintains a subscription with a company after requesting that the company delete the consumer's personal information, it is reasonable for the company to assume the consumer did not mean to cancel his or her subscription. As such, the AG should clarify that requests to delete personal information do not require businesses to delete information they would need to provide consumers with messages they expect to receive during the course of a subscription arrangement with a business. Such a rule would advance consumer privacy by reducing uncertainty around the kinds of data businesses must delete in response to a verifiable request. It would also provide further clarity for businesses with respect to their obligations under federal privacy laws on direct marketing.

d. *Remove the requirement to treat deletion requests as requests to opt-out of the sale of personal information if a requestor's identity cannot be verified*

Per the proposed regulations, if a business cannot verify the identity of a requestor who has submitted a request to delete, the business may deny the request to delete.[22] The business must then "inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale."[23] This requirement essentially forces businesses to act in ways that may not align with consumer choices or preferences. A consumer request to delete personal information does not mean that the consumer would agree to the business transforming that request into a request to opt-out of the sale of personal information. Furthermore, the requirement to transform unverifiable requests to delete into requests to opt-out of personal information sale ignores the fact that if a business cannot verify a consumer request, it may not be able to associate the requestor with any personal information to opt-out from sale. As such, IAB asks the AG to reconsider the requirement to act on unverifiable requests to delete as if they are requests to opt-out of personal information sale, as this mandate does not honor consumer preferences or acknowledge practical realities associated with unverifiable consumer requests.

The AG's proposed rule requiring businesses to pass opt-outs to third parties to whom they have sold personal information in the past 90 days would mean that unverified deletion requests that are converted into opt-out requests could have extremely broad and far-reaching implications for consumers. This result may not align with a consumer's expectation when submitting a request to delete. While a request to delete has effects for the business that receives the request, a request to opt-out has effects for third parties and the consumer, as third parties who receive consumer data may be providing consumers with products and services. If, as suggested in the Initial Statement of Reasons, the AG's goal is to "at least [prevent] the further

[22] Cal. Code Regs. tit. 11, § 999.313(d)(1) (proposed Oct. 11, 2019).
[23] *Id.*

proliferation of the consumer's personal information in the marketplace," this can be solved through directing the consumer to opt-out of the sale of their personal information in correspondence with the consumer.[24] Otherwise, transforming consumer requests to delete into requests to opt-out if a request cannot be verified runs the risk of thwarting consumer choice and forcing businesses to act in ways that do not align with a consumer's wishes.

In addition, if a business cannot verify a consumer request to delete, the business may not be able to associate that consumer with any personal information it maintains in order to facilitate an opt-out. If a business cannot verify a consumer, it cannot ascertain that the consumer making the request is a consumer about whom it maintains personal information in its systems. As such, the lack of verification presents a challenge for businesses in their efforts to effectuate both consumer requests to delete *and* requests to opt-out, as businesses must achieve a certain level of consumer verification for both requests to ensure they are acting on the correct consumer's data in their systems. As a result, the proposed regulations' requirement that businesses transform unverifiable consumer requests to delete into requests to opt-out of personal information sale does not take into account that the lack of verification could thwart the business's ability to opt the consumer out from personal information sale just as it thwarts the business's ability to delete consumer personal information.

Because the requirement to turn unverifiable requests to delete into requests to opt-out of personal information sale could contradict consumer preferences, and because businesses will have the same difficulties effectuating unverified requests to opt-out as they will unverified requests to delete, IAB asks the AG to reconsider the provision that requires businesses to transform unverified requests to delete into requests to opt-out. Removing this requirement from the proposed regulations will ensure that consumer choices are not hindered by businesses taking unilateral actions to transform their requests.

e. *Retain the deletion exception for archival and backup systems and the ability for businesses to present consumers with granular deletion choices*

The proposed regulations helpfully clarify that a business can comply with a consumer's request to delete by "erasing the personal information on its systems *with the exception of archived or back-up systems*."[25] IAB appreciates the AG's recognition of the challenges associated with fulfilling consumer requests as they relate to data in archival and backup systems. As IAB highlighted in its pre-rulemaking comments to the AG in March, if consumer requests can reach data held on backup or archival systems, the costs associated with these requests would be excessive. In addition, if deletion requests were required to reach such systems, businesses' ability to rebound from data failures and comply with legal obligations would be severely limited.

However, the proposed regulations state that a business "may delay compliance with [a] consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used." While IAB supports the AG's consideration of the challenges associated with data deletion in certain storage scenarios, we

[24] *See* Initial Statement of Reasons at 20.
[25] *Id*. at § 999.313(d)(3).

recommend that archived and backup systems be fully exempted from consumer deletion requests by removing the proposed obligations that apply when archived and backup systems are next accessed or used.[26]

In addition, the proposed regulations note that "[i]n responding to a request to delete, a business may present the consumer with the choice to delete select portions of the personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices."[27] IAB supports this provision, as it gives consumers the ability to delete granular pieces of personal information and does not force them to make all-or-nothing choices when it comes to personal information deletion. IAB recommends retaining this option when the AG finalizes its rules implementing the CCPA.

f. Clarify that a business may provide only the data "as of" the date of the request instead of "as of" the date of the disclosure

Businesses with large amounts of data to query to fulfill the consumer's data request cannot practically query their data and render it in real time. If the data is gathered that is on hand on the date the consumer makes the request and any new data would be similar, the consumer has received the transparency contemplated by the law. The AG should permit this to allow different types of businesses the ability to comply with the law.

IV. Update the Service Provider Limitations to Conform with Permissible Business Purposes Enumerated in the CCPA

The proposed regulations state that "[a] service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity."[28] This language is qualified by two exceptions: "A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity."[29] Taken together, these provisions could be read to prohibit service providers from using data for the full range of internal operations purposes for which they are permitted to use it under the CCPA. As such, IAB requests that the AG revise these proposed rules to reflect that using personal information received from a person or entity a service provider services for the purpose of providing services to another person or entity is a permissible "business purpose" under the CCPA. This change could be accomplished by adding an additional exception for a service provider "to perform services that fulfill a business purpose, so long as such use is for the benefit of the business, is described in the written contract between the business and service provider, and is consistent with the CCPA."

The draft regulations limit service providers' permissible uses of data in ways that contradict the statutory definitions of "service provider" and "business purpose." The text of the CCPA explicitly permits disclosures to "service providers" for a list of enumerated "business

[26] Cal. Code Regs. tit. 11, § 999.313(d)(3) (proposed Oct. 11, 2019).
[27] *Id*. at § 999.313(d)(7).
[28] *Id*. at § 999.314(c).
[29] *Id*.

purposes" under the statute.[30] The statute then defines "business purpose" to include *both* a business's *or a service provider's* operational purposes or other notified purposes.[31] As such, so long as a permissible service provider "business purpose" is authorized as part of the contracted-for "services" provided to the business, the CCPA permits a service provider to use the personal information it receives for such a business purpose.

Because a service provider's business purposes may include using personal information for the benefit of one business in a way that may also benefit other businesses, the CCPA is best interpreted to permit a service provider to use personal information it receives to provide services to all of its business partners, as long as such use is for the benefit of the business that provides the information to the service provider, is performed for a valid business purpose, and is otherwise consistent with the CCPA. However, the proposed regulations depart from the CCPA text, as they seem to prohibit service providers from using personal information they receive from one entity to provide services to another entity, even if such use stands to benefit the business that provided the personal information to the service provider for a business purpose.

Moreover, the draft regulations improperly read out of the statute that the definition of "business purpose" includes the use of personal information for the "service provider's operational purposes or other notified purposes."[32] The activities included in the list of business purposes (*i.e.*, performing services on behalf of the business or service provider, including providing advertising or marketing services, providing analytic services, or providing similar services) require the combination and use of personal information received from and for the benefit of multiple businesses. Focusing solely on the business purposes of the business renders the CCPA's text meaningless, and potentially invalidates several activities included in the definition of permissible business purposes under the law. As such, IAB asks the AG to clarify that a service provider may use personal information if the usage is within the scope of a "business purpose" as authorized as part of the contracted-for "services" provided to the business, or necessary for the service provider's own operational purposes and is otherwise consistent with the requirements of the CCPA.

Importantly, if the AG were to maintain the proposed restrictions on service providers, the AG has not conducted an adequate standardized regulatory impact analysis ("SRIA").[33] The SRIA submitted with the draft regulations is entirely silent on the likely detrimental impact of restricting service providers from performing services for a business purpose.[34] As a result, the SRIA fails to consider possible "elimination of existing businesses within the state" or "competitive … disadvantages for businesses currently doing business within the state," falling far short of the mandatory analysis required by the California Administrative Procedure Act.[35]

---

[30] Cal. Civ. Code §§ 1798.140(d), (v).
[31] *Id*. at § 1798.140(d).
[32] *Id*.
[33] *See* Cal. Gov. Code § 11346.3(c).
[34] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations (Aug. 2019), at 17 (hereinafter "SRIA") (concluding with regard to the draft regulations pertaining to service providers, "all other economic impacts associated with language in Article 3 are assumed to be attributable to the CCPA and are therefore included in the regulatory baseline.").
[35] Cal. Gov. Code § 11346.3(c)(1)(B), (C).

V. The AG Should Confirm That Section 999.314(c) Does Not Limit Businesses from Collectively Engaging Service Providers to Conduct Necessary Operational Activities Pursuant to "Business Purposes"

Additionally, upon IAB's review of Section 999.314(c), we do not see that it applies to or otherwise conflicts with the ability of multiple "businesses" that have collectively engaged service providers through the same contract or otherwise to conduct certain operational activities pursuant to "business purposes" that involve the combination of personal information. In such circumstances, Section 999.314(c) does not apply because these activities fulfill the "commercial purposes" of the contracting businesses, rather than serve the "commercial purposes" of the service providers. While we see no conflict with the existing language in such circumstance, IAB respectfully requests that the following clarifying language be added to Section 999.314(c):

> ***Notwithstanding the above restrictions, service providers that are engaged jointly or collectively on behalf of two or more businesses to fulfill necessary business purposes can combine, use, and share personal information as long as such activities are consistent with the commercial purposes of the businesses rather than the commercial purposes of the service providers.***

This clarification is consistent with the express language of the CCPA permitting service providers to use personal information for operational and permitted business purposes,[36] and supports the CCPA's privacy objectives to restrict a service provider from using personal information for its own "commercial purposes."[37] The clarification also satisfies the underlying goal stated in the Initial Statement of Reasons to prevent advancing the "commercial interest" of the service provider, rather than fulfilling the contracted "business purpose."[38]

The impetus for this clarification is the prevalence of joint engagements, operations or co-venture business models that hire service providers to support their joint activities. For example, companies may offer co-branded services wherein two companies provide a single offering to consumers. Similarly, businesses may enter into a joint agreement to provide a consistent user experience across digital platforms, devices, or internet domains. In these examples, the businesses require the ability to contract with a common set of service providers that, on behalf of the businesses, use personal information to support the businesses' operations (*i.e.*, the businesses' commercial purposes for providing the services).

For these reasons and to avoid any confusion or unnecessary disruption of multiple industries that rely on service providers to work jointly to assist a business, IAB urges the AG to clarify that Section 999.314(c) does not prohibit businesses from collectively engaging service providers to perform operations necessary for the businesses' commercial purposes, such as in joint or co-venture arrangements.

---

[36] Cal. Civ. Code §§ 1798.140(d), (v).
[37] *See* Cal. Civ. Code § 1798.140(v).
[38] Initial Statement of Reasons at 22.

VI. Consumer Opt-Outs Should Empower Consumers

IAB recommends that the AG make changes to the draft regulations' provisions related to opt-out requests so that they conform with the CCPA's text, as requirements that are not supported by the law's text do not further the California legislature's intent in enacting the CCPA.

a. *Requiring businesses to honor browser plugins or settings goes beyond the scope of the CCPA and creates significant compliance challenges that could impede consumer choice*

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 browser or device, or, if known, for the consumer."[39] 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.[40] We request that the AG remove this requirement, or alternatively, where a business offers a "Do Not Sell My Info" link and a means to opt-out from sale, the business is not required to treat the proposed controls as an opt-out. Such an approach would be consistent with the approach taken by the legislature when it amended the California Online Privacy Protection Act.

At this juncture, it would be premature to regulate in this area or mandate that every business comply with each type of signal developed to facilitate CCPA compliance. Given that no standard technology currently exists for such browser plugins or privacy settings, it is not clear what browser plugins or privacy signals should be honored or how they should be honored. Absent standard technical and policy protocols around how to honor such signals, the proposed regulations would give rise to different signals and interpretations and result in confusion among businesses and consumers alike.

The AG takes the position that in the absence of mandatory support for privacy controls, "businesses are likely to reject or ignore consumer tools."[41] As the CCPA comes into effect in 2020, IAB expects to see market forces leading to 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.

If the AG chooses to maintain this requirement, we suggest that the AG alter it so that a business engaged in the sale of personal information must *either* abide by browser plugins or privacy settings or mechanisms, or may not honor such settings if the business includes a "Do Not Sell My Personal Information" link and offers another method for consumers to opt-out of personal information sale by the business. This approach affords consumers with robust choice and control over the sale of personal information. Browser-based signals or plugins would

---

[40] *See* [CalOPPA & September 2018, 2019 amendments to CCPA]
[41] *See* Initial Statement of Reasons at 24.

broadcast a single signal to all businesses opting-out a consumer from the entire data marketplace. It is not possible through these settings for a consumer to make discrete choices among businesses allowing the consumer to restrict certain businesses while permitting other businesses to transfer data to benefit the consumer. In addition, it is not possible for a business to verify if a consumer set the browser setting or some intermediary did so without the authorization of the consumer.

b. *Remove the requirement to communicate opt-out requests to third parties that received the consumer's personal information within the prior ninety days*

As noted above in Section III(d), the proposed regulations require a business that receives an opt-out request to notify all third parties to whom it has sold personal information about the consumer making the opt-out in the past 90 days prior to the request that the consumer has opted out and instruct those third parties not to further sell the information.[42] IAB asks the AG to withdraw this proposal because it has no basis in the CCPA's statutory text and would result in negative consequences for consumers by amplifying, without a reasonable basis, the consumer's opt-out request aimed at just one business.

The proposed rule is not supported by the CCPA's text and goes beyond the proper scope of the AG's rulemaking authority. The CCPA states that a consumer has "the right, at any time, to direct *a business* that sells personal information about the consumer to third parties not to sell the consumer's personal information."[43] The plain language of the statute makes clear that the legislature intended the opt-out to apply to businesses only and did not grant consumers an opt-out right vis-a-vis third parties to whom personal information was already sold. Had the legislature intended the opt-out to have retroactive application to already sold personal information, it would have done so in the statute.[44]

The proposed rule also fundamentally changes the careful balancing of privacy rights with burdens on businesses, which the legislature decided upon with the CCPA. Indeed, the definition of a "sale" indicates the sale takes place for "monetary or other valuable consideration." Obligating a business to later restrict a recipient from further selling personal information is a material retroactive change to the basis of the bargain upon which the personal information was "sold" for consideration. If the draft regulations impose obligations on the seller and buyer after the sale, the seller and buyer will essentially be required to agree to a contingent transfer subject to the receipt of do not sell requests. This contingency will impact the value of the personal information sold and the underlying consideration of the transaction. The legislature did not contemplate such an outcome.

Additionally, the CCPA is structured in a manner that makes clear the legislature's intent that the opt-out applies to businesses and not to third parties. The CCPA only once refers to

---

[42] Cal. Code Regs. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).
[43] Cal. Civ. Code § 1798.120(a).
[44] *See W. Sec Bank v. Super. Ct.*, 933 P.2d 507, 513 (Cal. 1997) (statutes will not "operate retrospectively unless the Legislature plainly intended them to do so."); *see also Myers v. Philip Morris Cos., Inc.*, 50 P.3d 751, 759 (2002) ("unless there is an express retroactivity provision, a statute will *not* be applied retroactively unless it is *very clear* from extrinsic sources that the Legislature . . . must have intended a retroactive application" (citations and quotation marks omitted; emphases in original)).

third party obligations regarding the handling of personal information that has been sold to the third party.[45] Otherwise, the CCPA focuses entirely on the obligations of businesses to provide the right to opt-out.[46] Through this emphasis on the obligations of businesses, the CCPA favors letting consumers make an opt-out choice up front before the personal information flows to third parties.[47]

The draft regulations are invalid to the extent that they exceed the scope of the AG's statutory authority[48] or read into the statute additional requirements that go beyond the statutory scheme of the CCPA.[49] It is true that the CCPA provides the AG with the ability to establish rules and procedures "to govern business compliance with a consumer's opt-out request."[50] However, that provision does not vest the AG with the authority to write rules that extend the scope of the opt-out beyond the plain language and clear intent of the statute such that the opt-out retroactively applies to third parties.[51]

In addition, the draft regulation will likely lead to consumer confusion around the meaning of the opt-out of sale request, with damaging economic effects. The proposal assumes that a consumer's desire to opt-out of one business's sale of personal information represents a request that the consumer would like to have this request applied retroactively to third parties to whom their personal information was already sold. It is not clear that a consumer would expect an opt-out of sale button to operate in this manner, and indeed, the consumer's actual intentions may be frustrated if the AG were to draw such an unfounded conclusion. Furthermore, obligating businesses to pass opt-out requests on to third parties and to instruct those third parties not to further sell information could have damaging effects on the Internet economy, as the free flow of data that powers the Internet will be stifled by a consumer expressing an opt-out choice aimed at one business only.[52] Consumers will receive fewer digital offerings and decreased access to products and services that interest them if this requirement becomes effective.

---

[45] *See* Cal. Civ. Code § 1798.115(d).
[46] *See* Cal. Civ. Code § 1798.120.
[47] *See* Cal. Civ. Code § 1798.120(b).
[48] *See In re J.G.*, 159 Cal. App. 4th 1056, 1066 (2008) (invalidating correction department regulation which exceeded statutory authority).
[49] *See Slocum v. State Bd. of Equalization*, 134 Cal. App. 4th 969, 981 (2005) (invalidating State Board of Equalization interpretative regulation because it acted to provide more relief than statutorily authorized); *see also Sabatasso v. Superior Court*, 167 Cal. App. 4th 791, 797 (2008) (invalidating penal regulation which went beyond scope of delineated statutory authority).
[50] Cal. Civ. Code § 1798.185(a)(4)(B).
[51] *See Home Depot, U.S.A., Inc. v. Contractors' State License Bd.*, 41 Cal. App. 4th 1592, 1600, 49 Cal. Rptr. 2d 302, 306 (1996) ("A regulation cannot restrict or enlarge the scope of a statute" (*citing* Cal. Gov. Code §§ 11342.1, 11342.2).); *Ontario Cmty. Foundations, Inc. v. State Bd. of Equalization*, 35 Cal. 3d 811, 816, 678 P.2d 378, 381 (1984) ("[T]here is no agency discretion to promulgate a regulation which is inconsistent with the governing statute.").
[52] The SRIA is also deficient on this point. *See* SRIA at 25-26. The SRIA indicates "[t]he incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible." *Id.* at 25. This comment overlooks the ripple effect as the opt-out of sale request will restrict uses of personal information including those generally occurring subsequent to the sale transaction. The SRIA should consider how restricting the sale of personal information by third parties in this way can "increase or decrease … investment in the state." Cal. Gov. Code § 11346.3(c)(1)(D).

Because the requirement to pass opt-out requests along to third parties is outside the scope of the CCPA and because of the negative effects such a requirement will have on consumers and the Internet economy alike, IAB asks the AG to remove this requirement from the proposed regulations. Doing so will help the CCPA better align with legislative intent and will stop the law from harming consumers by decreasing their ability to benefit from increased access to online products and services.

VII. 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.[53] "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."[54] 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 and provide additional flexibility for businesses and consumers for requests to opt-in to personal information sale after previously opting-out.

VIII. 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."[55] 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 and need not maintain information about other businesses' responses to consumer opt-out requests.

IX. Clarify the Household Concept

The CCPA gives consumers the right to access personal information, and the law's definition of personal information includes "household" data.[56] The proposed regulations define "household" to mean "a person or group of people occupying a single dwelling."[57] Moreover,

[53] Cal. Code Regs. tit. 11, § 999.316(a) (proposed Oct. 11, 2019).
[54] *Id*.
[55] *Id*. at § 999.317(b).
[56] Cal Civ. Code § 1798.140(o)(1).
[57] Cal. Code Regs. tit. 11, § 999.301(h).

per the proposed rules, if a consumer does not maintain a password protected account with a business, the business may respond to that consumer's request to know "household personal information" by providing "aggregate household information" so long as the requestor has been verified in accordance with the proposed regulations.[58] And if all consumers in a household jointly request to know "specific pieces of personal information for the household" or delete household personal information, the business must comply with the request if all the household members have been verified.[59] IAB asks the AG to clarify the household concept and provide instructions on how businesses can reasonably comply with the requirement to return household data in response to a consumer access request.

Returning household data to a requesting consumer or consumers creates privacy concerns, because a business might provide a consumer's personal information to a household member who should not have access to such data, creating the potential for a data leakage facilitated by a legal obligation. In addition, returning "aggregate" data to a single consumer requesting information about a household could still reveal private information about another member of the household. For example, if a business maintains information in the aggregate about a household income, returning that information in response to a single consumer's request could present income information about other members of the household to the requesting consumer. IAB therefore asks the AG to clarify how businesses can comply with the requirement to return household data, especially when doing so could reveal private or sensitive information about other members of the household.

* * *

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 us.

Respectfully submitted,

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

Michael Hahn
Senior Vice President & General Counsel
Interactive Advertising Bureau
212-380-4721

[58] *Id*. at § 999.318(a).
[59] *Id*. at § 999.318(b).