March 27, 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: Second Set of Modifications to California Consumer Privacy Act Proposed Regulations

The Interactive Advertising Bureau ("IAB") provides these comments on the second set of modifications to the proposed regulations issued by the California Attorney General ("AG") on March 11, 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 dated December 6, 2019 and February 25, 2020.[2] 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 advance it. IAB urges the AG to consider consumers' support for the ad-driven Internet model and asks the AG to update the modified rules in line with the suggestions in these comments so the regulations empower consumers by giving them increased choices and control over online data.

---

[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] *See* IAB, *California Consumer Privacy Act Proposed Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day-pt6.pdf at CCPA_45DAY_01296 - 01312; IAB, *California Consumer Privacy Act Proposed Modified Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf at CCPA_15DAY_000179 – 000187.

IAB also asks the AG to consider postponing enforcement of the CCPA until January 2021. The draft regulations implementing the CCPA are still not final, leaving little to no time for businesses to implement the ultimate requirements before the CA AG may begin enforcing the law. In addition, the unique and extraordinary state of affairs brought on by the COVID-19 crisis has forced businesses to quickly adjust their priorities in order to appropriately address the needs of their employees and the world in this difficult time. Beginning to enforce the CCPA when the economic and public health situation is so dire and uncertain would harm rather than help consumers and the economy-at-large, and the AG should consider these unprecedented circumstances in developing its enforcement approach.

In the spirit of improving the CCPA's regulatory regime and providing privacy protections that benefit all Californians while enabling the business community to continue to support California's economy, IAB submits these comments. IAB below addresses specific provisions of the modified rules that should be updated or clarified to further consumer choice and privacy and enable business compliance with the law.

I. Commence Enforcement in January 2021 Instead of July 2020

The unfinalized nature of the draft regulations implementing the CCPA leaves minimal time for businesses to implement the rules' ultimate requirements prior to July 1, 2020, the date the AG may begin enforcing the law.[3] Making matters even more challenging, the COVID-19 health crisis has significantly changed everyday life as well as standard business operations. Resources businesses had been dedicating to CCPA compliance efforts have been diverted to assist workforces and ramp up remote work capabilities. Californians and others in myriad states are under mandatory "shelter in place" or "stay at home" orders, which have disrupted the economy as well as entities' ability to build brand-new processes and compliance systems in advance of the CCPA's enforcement date.[4] The World Health Organization has deemed the coronavirus to be a global pandemic, and President Trump has declared California to be a "major disaster" zone as one of the primary epicenters of the virus outbreak.[5]

During the present health emergency, businesses should remain vigilant and focused on doing everything they can to assist the fight against the coronavirus and maintain viability so they can continue to employ individuals and support the economy. Entities all over the country are doing their part to put workers, consumers, and the world-at-large at the forefront of their considerations as they navigate new requests from government entities to reoutfit operations and

---

[3] Cal. Civ. Code § 1798.185(c).
[4] Alicia Lee, *These states have implemented stay-at-home orders. Here's what that means for you,* CNN (Mar. 24, 2020), located at https://www.cnn.com/2020/03/23/us/coronavirus-which-states-stay-at-home-order-trnd/index.html.
[5] White House, *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak* (Mar. 13, 2020) located at https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/; Office of Governor Gavin Newsom, *California Secures Presidential Major Disaster Declaration to Support State's COVID-19 Emergency Response* (Mar. 22, 2020), located at https://www.gov.ca.gov/2020/03/22/california-secures-presidential-major-disaster-declaration-to-support-states-covid-19-emergency-response/.

produce supplies to support hospitals and healthcare workers.[6] IAB members are providing their communities with connectivity, content, news, and services for free or at a reduced cost and partnering with groups such as the World Health Organization to provide timely information to American citizens through digital advertising.[7] Businesses should not be preoccupied with potential enforcement actions for technical violations of an entirely new legal regime when the world is facing such critical circumstances.

In the face of immense challenges, the quickly approaching enforcement date of July 1, 2020 leaves businesses strapped to bring their procedures into compliance as they are attending to calamitous and pressing matters. The AG, like data protection authorities in other jurisdictions, should consider delaying or pausing enforcement until January 2021 so businesses are not distracted from the task of supporting the economy and fighting the coronavirus.[8] We therefore ask you to postpone enforcement of the CCPA until January 2021.

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

The March 11, 2020 version of modified regulations removed previously proposed language that stated "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."[9] The AG should re-insert this subsection as it provides beneficial guidance to companies. Furthermore, we would recommend modifying the language to better reflect privacy by design principles.

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 re-inserting 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*

---

[6] *See, e.g.,* Samantha Masunaga, *California companies jump in to supply ventilators needed in coronavirus fight,* LA TIMES (Mar. 23, 2020), located at https://www.latimes.com/business/story/2020-03-23/coronavirus-california-companies-medical-supplies.

[7] https://www.iab.com/blog/good-works/

[8] United Kingdom Information Commissioner's Office, *Data protection and coronavirus: what you need to know*, located at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/covid-19-general-data-protection-advice-for-data-controllers/.

[9] *Compare* Cal. Code Regs. tit. 11, § 999.302(a) (proposed Feb. 10, 2020) *with* Cal. Code Regs. tit. 11, § 999.302(a).

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."

III. Revise the Proposed "Responding to Requests to Know and Requests to Delete" Regulations to Remove Undue Burdens for Business and Expressly Acknowledge That a Business May Withhold Specific Pieces of PI if Divulging Such Information Could Lead to Unreasonable Security Risks or Contravene Other Competing Public Policy Considerations

Section 999.313(c)(3) is overly restrictive, creates undue burdens for business, and increases privacy and security concerns. The right to know requires a business to disclose to the consumer personal information the business has "collected about that consumer." The statute requires the AG to promulgate regulations for access requests that "tak[e] into account," *inter alia*, "security concerns, and the burden on the business." 1798.185(a)(7). Subdivision (c)(3) properly recognizes that not *all* personal information a business has collected about a consumer need be made available. We appreciate and agree with the recognition that an absolute access requirement is not desirable or consistent with privacy best practices.

Moreover, the proposed provision is too restrictive and does not sufficiently recognize privacy concerns or undue burdens. As currently drafted, (c)(3) contemplates a four-part test when, in practice, no information will meet all four prongs. For example, if a business maintains the personal information solely for legal or compliance purposes, then it necessarily has to maintain it in a searchable or reasonably accessible format. If it did not, it could not search or access the information for its legal or compliance obligations. Or, if a business maintains personal information "solely" for legal or compliance purposes, then it cannot sell the personal information because it maintains the information for discreet legal or compliance purposes. In these ways, (c)(3) does not meaningfully limit the scope of what must be provided in response to access requests. Each of the prongs, on their own, should provide a sufficient basis for not providing personal information covered by that prong.

The modified regulations also do not sufficiently address privacy and security concerns as they 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." 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.[10] However, if a business is forced to divulge such the information it maintains anyway due to a legal requirement, this obligation could put the consumer, the consumer's information, and/or the business at unreasonable risk, such as unauthorized access to personal information. Such a requirement would be contrary to the intent of CCPA and less privacy protective for consumers. IAB therefore 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. Additionally, the draft regulations should recognize other important qualifications for when a business should not have to provide consumers with specific pieces of information.

Finally, subsection (c)(3) creates undue burdens for businesses. Many businesses possess personal information that is not typically readily searchable (and able to be produced) on a user-level basis. For example, businesses may maintain property or sales records that contain personal information of prospective customers, sometimes in paper form. Retrieving personal information belonging to specific individuals in these records would be overly burdensome if the business lacks the technical ability to identify which records contain personal information from the user. Because that data is not readily searchable or in a reasonably accessible format, under that factor alone, businesses should not be required to search for personal information within that data. IAB suggests the following text for § 999.313(c)(3):

> *A business shall not provide a consumer with specific pieces of personal information if the disclosure would: (1) create a substantial, articulable, and unreasonable risk to the privacy or security of that personal information, the consumer's account with the business, or the security of the business's systems, networks, or consumers; (2) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (3) disclose the covered entity's trade secrets or proprietary information; (4) would require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (5) violate federal, state, or local laws, including rights and freedoms under the United States Constitution.*
>
> - *In responding to a request to know, a business is not required to provide personal information ~~if all~~ that meets any of the following conditions ~~are met~~, provided the business describes to the consumer the categories of information it collects:*
>
> *a. The business does not maintain the personal information in a searchable or reasonably accessible format;*
> *b. The business maintains the personal information solely for legal or compliance purposes; or*
> *c. The business does not sell the personal information and does not use it for any commercial purpose.*

[10] Cal. Code Regs. tit. 11, § 999.325(c) (proposed Mar. 11, 2020).

IV. Make Clear that Internally Generated Data and Inferences Are Not Responsive to CCPA Access Requests Because They Are Not "Collected"

The CCPA states that in response to a consumer request to access personal information, a business must disclose "[t]he specific pieces of personal information it has *collected* about the consumer."[11] The AG recently revised the text of the draft rules to mirror this statutory language by specifically stating that a "request to know" means a "request that a business disclose personal information that it has *collected,*" including "[s]pecific pieces of personal information that a business has *collected* about the consumer."[12] We ask the AG to clarify that the data a business generates or infers internally is not collected and therefore is not responsive to a consumer's request to access specific pieces of information. This interpretation is rational given the plain text of the CCPA and its implementing regulations. It would also protect businesses' intellectual property and trade secrets and enable them to provide understandable privacy disclosures to consumers. As such, it is appropriate for your office to update the draft rules to exempt internally-generated and inferred information from the scope of access requests under the CCPA.

Businesses internally generate inferences and derived data regularly, and many of these inferences constitute intellectual property or trade secrets that are subject to protections under various state and federal legal regimes. Businesses should not be forced to reveal their intellectual property or trade secrets due to an ambiguous requirement in state law. The CCPA itself acknowledges that certain information may need to be exempt from the law's bounds and instructs the AG to "[e]stablish any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…."[13] Despite the mandatory nature of this requirement, to date, the Attorney General has not issued any draft regulations related to trade secrets and intellectual property rights. We request that, to comply with its obligations under the CCPA, the AG issue a regulation establishing an exception to the requirements of the CCPA to protect against violations of intellectual property rights and the disclosure of trade secrets. In so doing, we believe the Attorney General should take into consideration the proprietary nature of certain data, particularly internally generated or derived data, and the impact that may have on a business. To this end, IAB suggests the following text for **§** 999.319 on Intellectual Property and Trade Secrets:

> *The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate the business's intellectual property rights or result in the disclosure of trade secrets.*

Internally generated inferences and inferred data are created by virtually every business in its normal course of operations, and much of this data is duplicative of other information maintained in enterprise systems. For example, connecting an individual's name with his or her email address involves an inference made by the business processing the data. If businesses are required to return each and every inference connected with a consumer in response to a consumer's request to access specific pieces of personal information, the consumer would be

[11] Cal. Civ. Code § 1798.110(a)(5) (emphasis added).
[12] Cal. Code Regs. tit. 11, § 999.301(q) (proposed Mar. 11, 2020) (emphasis added).
[13] Cal. Civ. Code § 1798.185(a)(3).

inundated with hundreds if not thousands of pages of data that could bury important disclosures like a needle in a haystack. Consumers would be fatigued by excessively voluminous notices that would impede their ability to access important information about businesses' privacy practices. This result would not further the CCPA's purpose of providing consumers with enhanced transparency. To this end, the Attorney General should specify that businesses need not provide substantially similar or duplicative information to consumers in response to their requests to know. The CCPA already permits a business to refuse to act on "manifestly unfounded or excessive requests," recognizing that there are limits to information that must be provided to consumers in response to requests to know. Similarly, there are other instances in which it would be useful to limit the information required to be provided to consumers. For example, providing consumers with substantially similar or duplicative data would be disproportionately burdensome on businesses and not useful for consumers. An illustrative example is useful here. A business might keep the following specific pieces of information about a consumer: (1) data indicating a consumer watched a video; (2) data indicating that a consumer watched at least 25% of a video; (3) data indicating that a consumer watched at least 75% of a video; and (4) data indicating that a consumer watched at least 90% of a video. In response to a consumer's request to know what personal information a business has collected about her, the business should need only to produce a single data point to provide a consumer with a meaningful understanding of the information it has collected. IAB suggestions the following text for § 999.313(c)(12):

> *In responding to a verified request to know categories of personal information, a business shall not be required to produce substantially similar or duplicative specific pieces of personal information.*

Additionally, retrieving internally generated inferences from businesses' systems to return them to consumers is no small task; internally generated data is often housed in various disparate databases throughout an enterprise and is therefore excessively burdensome to amalgamate. Additionally, this information may be unstructured or not readable by the average consumer due to privacy-protective measures a business has taken to mask identifying information associated with the internal inference. Revealing such data would be meaningless to consumers and would provide them with no useful insights. The practical challenge of consolidating internal inferences coupled with the minimal privacy value it would offer to consumers if returned in an access disclosure warrants an interpretation from your office that such data is not responsive to consumer access requests for specific pieces of personal information.

The CCPA and its implementing regulations clearly require businesses to disclose inferences in responses to consumer requests for specific pieces of information if those inferences are actually collected or received by the business from another entity.[14] Additionally, if a business discloses or sells its internally generated inferences, the business must list the category of "inferences" in its response to a request to know pursuant to the requirement to provide the categories of personal information sold and disclosed.[15] However, internal inferences that are generated by a business and not received from another entity are not

[14] *Id*. at § 1798.110(a)(5); Cal. Code Regs. tit. 11, § 999.301(q) (proposed Mar. 11, 2020).
[15] Cal. Civ. Code §§ 1798.115(a)(2)-(3).

"collected", and therefore they should not be required to be returned in response to a consumer request to access personal information. We ask the AG to issue a regulation clarifying this interpretation, which would further legislative intent and better enable consumers to receive digestible and understandable privacy disclosures under the CCPA.

V. The CCPA regulations should allow service providers to process personal information for all business purposes permitted under the statute

In response to the initial draft CCPA regulations, several commenters raised concerns that the regulations' restrictions on service providers' use of personal information did not align with the text of the CCPA statute.[16] As many commenters recognized,[17] this creates regulatory uncertainty that frustrates businesses' ability to engage service providers to efficiently and effectively perform tasks critical to offering products and services to California consumers. We urge the Attorney General to further clarify (through the text of the regulations and the Final Statement of Reasons) that the regulations allow service providers to process personal information for any "business purpose," as that term is defined in the statute. Specifically, the regulations should make it clear that a service provider may use personal information for any "operational purposes" enumerated in Section 1798.140(d) of the statute permitted under the written agreement between the business and the service provider without introducing non-statutory restrictions on service providers.

The CCPA defines "service provider" as a for-profit entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose, pursuant to a written contract."[18] Accordingly, a service provider's rights to use personal information received from a business depends on what constitutes a "business purpose" under the statute.

The statute defines "business purpose" as "the use of personal information for the business's *or a service provider's operational purposes*, or *other notified purposes.*"[19] As multiple commenters have explained, this statutory text plainly affords service providers flexibility to process personal information not only for the *business's* purposes, but also for the *service provider's* own purposes so long as those purposes are necessary to perform the services specified in the contract.[20]

The statute provides several examples of permitted operational purposes, such as "[p]erforming services on behalf of the business or service provider, including . . . processing

---

[16] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of NAI at 24-25; Comments of California Cable and Telecommunications Association at 8-11; Comments of Consumer Data Industry Association at 13; Comments of CCIA at 7; Comments of CTIA at 14-16; Comments of Engine Advocacy at 5-6; Comments of California Chamber of Commerce at 11-12.

[17] See, e.g., Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of the Department of Justice at 5; Comments of the Entertainment Software Association at 4; Comments of the State Privacy and Security Coalition at 4; Comments of NAI at 14.

[18] Cal. Civ. Code § 1798.140(v).

[19] Id. at § 1798.140(d) (emphasis added).

[20] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of Entertainment Software Association at 4; Comments of Google at 1; Comments of TechNet at 12; Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of Entertainment Software Association at 4.

orders and transactions . . . providing advertising or marketing services . . . providing analytic services, or providing similar services on behalf of the business or service provider."[21] Operational purposes also include, for instance, "auditing related to a current interaction with a consumer, including but not limited to verifying the positioning and quality of advertising impressions,"[22] and "undertaking internal research for technological development and demonstration."[23]

The plain language of the "business purpose" definition sensibly limits uses of personal information to those which are "reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected."[24] The written agreement between the business and service provider, along with the privacy notices that consumers receive under the statute, specify the purposes for which personal information is collected and processed and also inform what uses are compatible with the context in which personal information is collected. Personal information disclosed to a service provider must be "pursuant to a written contract," which must prohibit the service provider from processing the information "for any purpose *other than for the specific purpose of performing the services specified in the contract* for the business . . . including retaining, using, or disclosing the personal information *for a commercial purpose other than providing the services specified in the contract with the business*."[25]

Permitting service providers to use personal information for their own operational purposes is not only required by a plain reading of the statutory text, but also is sound policy: in order to perform the contracted-for services on behalf of the business, service providers often *must* process personal information received from multiple businesses internally. For example, a business may hire a consulting service to help it determine the best location for its next retail store. To facilitate this analysis, the business likely will need to provide the service provider with personal information (such as names and transaction history) about its existing customers, consistent with its privacy policy. The service provider likely will need to combine this information internally with similar information it has collected from other customers to analyze where these existing customers, and other potential new customers with similar interests or preferences, might shop. Without disclosing any personal information received from other customers to the business, the service provider would use this combined data to inform the recommendations it provides to the business on where to build a new store. If the consultant is not permitted to combine personal information received from its different customers and use that information to perform its services consistent with its written agreements with those different businesses, the consultant's recommendations to the retail store would be based on incomplete and less relevant information that ultimately could produce a worse outcome for consumers.[26]

---

[21] Cal. Civ. Code § 1798.140(d)(5).
[22] *Id*. at § 1798.140(d)(1).
[23] *Id*. at § 1798.140(d)(6).
[24] *Id*. at § 1798.140(d).
[25] *Id*. at § 1798.140(v).
[26] Relatedly, the store might decide not to engage a service provider at all for these services if it meant having to treat the disclosure as a "sale" of data, which would require the store to expend significant resources to update its privacy notice, build and maintain an opt-out mechanism, and provide additional information when responding to consumers' "right to know" requests. This alternative is particularly problematic because reasonable consumers are

Importantly, this interpretation also ensures the privacy of consumers' personal information remains protected at all times for at least two reasons. First, consumers must have received notice that their personal information may be shared with the service provider for business purposes. Second, the CCPA requires that the written agreements between the service provider and its business customers prohibit the service provider "from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract," which safeguards the data from unauthorized processing and ensures that all uses are compatible with the context in which the personal information was collected.[27]

Moreover, this interpretation aligns the Attorney General's second modified draft regulations and the plain text of the enabling statute. The Attorney General cannot enact rules that are inconsistent with the statutory text, including by narrowing a statute.[28] And the California legislature also specified that the Attorney General's regulations must further the CCPA's purposes.[29] Accordingly, we ask that the Attorney General further clarify that the regulations allow service providers to process personal information received from a business for any "business purpose," as that term is defined in the statute. IAB proposes the following text for § 999.314(c):

- *The Attorney General should reinstate the deleted language in (c)(1) to clearly permit a service provider to use personal information for any permitted business purpose pursuant to the written agreement between the business and the service provider.*[30]
- *To clarify that the Attorney General's regulations are meant to be consistent, and not in conflict, with the statute, we request that the Attorney General further modify the draft regulations by adding the underlined language to § 999.314(c):*
    - *A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except <u>to the extent permitted by the CCPA, including</u>: . . .*

unlikely to consider such disclosures, where the recipient of the data is providing services to the business and is subject to contractual restrictions on how the personal information is processed, to be a sale of personal information.

[27] *See* Cal. Civ. Code §1798.140(v) (requiring service providers to receive personal information "for a business purpose" and to process personal information for "the specific purpose of performing the services specified in the contract for the business").

[28] *In re Edwards*, 26 Cal. App. 5th 1181, 1189, 237 Cal. Rptr. 3d 673, 679 (Ct. App. 2018) (quoting Gov. Code, § 11342.2). Agencies do not have the discretion to promulgate regulations that are inconsistent with the relevant statute. *See Ontario Community Foundations, Inc. v. State Bd. of Equalization* (1984) 35 Cal.3d 811, 816–817, 201 Cal.Rptr. 165, 678 P.2d 378, ("[T]here is no agency discretion to promulgate a regulation which is inconsistent with the governing statute.") (Emphasis, citations and internal quotation marks deleted.)

[29] Cal. Civ. Code §§ 1798.185(a)(1); (b)(2).

[30] Section 999.314(c)(3) permits service providers to process personal information for internal purposes but includes the limitation "provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business." For the reasons discussed above, this example must be in alignment with the permissions service providers enjoy under the statute. Therefore, we understand the limitation to apply *only if* the written agreement between the business and the service provider does not permit the service provider to process personal information to build or modify profiles for other businesses.

VI. Remove the Obligation for Businesses to Comply with Global Privacy Controls, Such as Browser Settings

The modified regulations state that "[i]f a business collects personal information from consumers online, the business shall treat global privacy controls, such as a browser plugin or privacy setting, device 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."[31]

IAB asks that the AG remove the requirement to comply with browser and device-level privacy controls, as these obligations are not contemplated by the CCPA itself, impose new substantive requirements on businesses that the legislature has previously considered and elected to not include, and impede the development of new opt out tools. IAB believes this proposal is based on an inaccurate understanding of today's Internet ecosystem and existing browser controls, and the outcome of this proposal will have dramatic negative impacts on competition in the state of California.

a. The AG has instituted new substantive requirements on businesses that the legislature has previously considered and elected to not include.

The AG's mandate that businesses must treat browser settings and global privacy controls as valid requests to opt out of personal information sale is nowhere in the text of the CCPA itself. Despite the numerous amendments to the CCPA that were enacted in 2018 and 2019, none of those legislative vehicles included a requirement to honor browser settings or global privacy controls.[32] Additionally, the California legislature considered global privacy controls and browser setting mandates in the past and elected not to enact such legislation. As such, the AG's institution of a browser mandate in the draft regulations contravenes legislative intent and exceeds the scope of the CCPA.

In 2011, California Senator Alan Lowenthal introduced SB 761, instructing the AG to adopt regulations allowing consumers to opt out of online tracking. This bill failed to pass after careful consideration by the legislature. SB 761's failure to be enacted by the legislature demonstrates how technical tools that send a single signal to the entire Internet marketplace have been at legislators' disposal for years. Though legislators in California are well aware of these tools, they have specifically declined to make them the law of the land in the state. No new developments have arisen to prompt the AG to infer any intent on behalf of legislators to enact such tools now or support them. To the contrary, past experience in the state suggests that its representatives would not and do not approve of a wholesale browser signal or global privacy control requirement.

The legislature again considered a blanket Do Not Track ("DNT") requirement when it amended the California Online Privacy Protection Act in 2013.[33] However, that proposal made clear that it merely required the disclosure of whether a business honors such DNT signals and

[31] Cal. Code Regs. tit. 11, § 999.315(d) (proposed Mar. 11, 2020).
[32] *See* SB 1121 (2018); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).
[33] AB 370 (Cal. 2013).

did not include an express mandate to respect the signals themselves. The California legislature declined to impose a one-size-all technical-based solution to effectuating consumer opt outs to personal information transfers in 2011 as well as 2013. The AG should not usurp that careful calculation by instituting a brand new and unprecedented requirement in California to respect such signals under the CCPA.

b. The privacy controls mandate will have negative consequences for consumers by interfering with business relationships and consolidating market power.

Requiring businesses to honor global 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, or whether the user is a California resident. 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 would thwart the aim of the CCPA to give consumers' control over personal information as well as have a negative revenue impact on the publishers and services consumers rely on and trust.

Concerns about concentrating power in the hands of intermediaries and consolidation of market power are not unfounded. There are four browser manufacturers that control over 90 percent of the browser market in the United States and three device manufacturers that control nearly 80 percent of the mobile phone market.[34] Examples of browsers interfering with consumer privacy preferences to the advantage their own revenue models have already been revealed.[35] The proposed rules' mandate that businesses must respect global privacy controls and browser settings stands to entrench these already deeply ingrained market players, and it places control in their hands rather than in the hands of consumers, effectively making these few companies gatekeepers to the Internet economy.

Moreover, the requirement advantages certain entities in the ecosystem over others. The AG's draft regulations note that if a browser control or global privacy setting conflicts with a setting set directly with the business, the business can contact the consumer to find out which signal should be respected.[36] Third parties that do not have a direct way to communicate with consumers will be disadvantaged over first party publishers who can serve notices and choices directly to consumers. This term therefore stands to distort the marketplace by providing

---

[34] *See Browser Market Share Untied States of America*, STATCOUNTER GLOBALSTATS, *located at* https://gs.statcounter.com/browser-market-share/all/united-states-of-america; *US Smartphone Market Share: By Quarter*, COUNTERPOINT RESEARCH, located at https://www.counterpointresearch.com/us-market-smartphone-share/.

[35] *See* Kimber Streams, *Internet Explorer 10 first browser to have Do Not Track as default*, THE VERGE (June 1, 2012), located at https://www.theverge.com/2012/6/1/3057265/internet-explorer-10-windows-8-do-not-track-default

[36] Cal. Code Regs. tit.11, § 999.315(d)(2) (proposed Mar. 11, 2020).

avenues for relief for certain entities at the expense of others, which likely would reduce revenue for independent publishers and online journalism.

The opportunity for intermediaries to interfere with consumer choices is magnified by the modified regulations' removal of the requirement that privacy controls shall not be designed with any pre-selected settings. The AG struck this provision from the draft rules, which stated: "[a]ny privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to the 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."[37] As a result, intermediaries have been given complete license to set default opt out signals that may not align with consumers' expressed choices and preference regarding sales of personal information.

The California Privacy Rights Act Ballot initiative recognizes the concern that businesses could leverage opt-out controls to gain unfair advantages over competitors, rather than to protect consumer privacy. As a result, the ballot initiative requires regulations for an opt-out preference signal that, among other things, ensures that platforms or browser device that sends the opt-out preference signal cannot unfairly disadvantage another business and must "clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent[.]"[38] Consequently, privacy initiatives on the horizon in California address the concern that intermediaries will set default signals without consulting consumers. The AG's draft rules should similarly address this issue. If the AG decides to include browser controls, IAB asks that the AG include previously proposed language that prevents interference with consumer choice signals and signals that may be set by intermediaries without first consulting the consumer.

c. Claims in favor of browser controls such as DNT ignore the many outstanding problems with such browser-level controls.

Those advocating for and referencing the World Wide Web Consortium's DNT proposal as an example of the benefits of global privacy settings have ignored the real-world implications of this standard and its well documented unintended consequences.

For one, some have argued that DNT improves consumer experience by reducing the number of privacy choices consumers must make to protect their privacy. There is no evidence to support this. 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, a universal opt-out will prevent consumers from receiving a wide variety of services they expect and would not consider to be a sale or harmful to their privacy. As a result, consumers will be inundated with whitelisting requests, further deteriorating the consumer experience without providing enhanced privacy.

Others have argued that the DNT standard accommodates granular controls. These arguments ignore the reality of how browser makers have implemented the DNT mechanism in their software. Today, browsers only offer a binary choice to consumers in their privacy settings

[37] *Compare* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Feb. 10, 2020) *with* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Mar. 11, 2020).
[38] Ballot Initiative 19-0021 (Nov. 4, 2019), California Privacy Rights Act of 2020, § 1798.185(19)(A).

pages. This blunt instrument fails to provide the flexibility and granular privacy preferences that consumers need and expect, and that is required by other laws, such as the GDPR.

An additional concern with browser-level toggles is that they assume the consumer understands the browser's relationship with other applications and services on their devices. Consumer expectations around what a browser-level DNT toggle would do vary widely, which leads to confusion about what selling activities are impacted. This increases consumer confusion and can lead to a false sense of security.

The unintended consequences of requiring browser signals have been documented at length in Europe with respect to the proposed ePrivacy Regulation. Due to the significant concerns with mandating such a system, subsequent drafts of the ePrivacy Regulation have removed browser and device level privacy settings.[39] Even lead developers of the DNT mechanism have acknowledged the risks and unintended consequences of requiring by force of law the use of such global privacy signals, and have recommended not including this requirement in the regulations until after further deliberation.[40]

d. The AG should provide businesses more flexibility and encourage innovative approaches to providing privacy preferences in line with consumer expectations.

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] While it is true that adoption of certain existing privacy controls has varied across publishers and platforms (*i.e.*, adoption of the DNT standard), IAB urges the AG to recognize that the CCPA is without precedent and represents a fundamental shift in California privacy law. 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. Mandating that businesses respect global privacy controls could impede the development of various helpful tools and solutions for consumers to use to exercise choice in the marketplace.

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 global signal developed to facilitate CCPA compliance. We therefore respectfully ask the AG to remove the requirement to treat global privacy controls as valid requests to opt out of personal information sale and update the draft rules so that businesses

---

[39] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications* (Feb. 20, 2020), located at https://data.consilium.europa.eu/doc/document/ST-5979-2020-INIT/en/pdf.

[40] See, e.g., Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of Aleecia M. McDonald at 14-15.

may respect such global 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.

* * *

We appreciate the opportunity to submit these comments. If you have questions, please contact me at 202-579-3243.

Respectfully submitted,

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