November 8, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

RE: Joint Ad Trade Comments in Response to the California Privacy Protection Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (PRO 01-21)

Dear California Privacy Protection Agency:

On behalf of the advertising industry, we provide the following initial, but not exhaustive, comments in response to the California Privacy Protection Agency ("Agency") invitation for preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020 ("CPRA").[1] We look forward to offering ongoing input to the Agency to help develop effective and workable regulations implementing the CPRA. We believe the implementing regulations can be drafted in a way that provides robust consumer protections while still allowing Californians to enjoy the full benefits of the data economy. Implementing rules, provided in a timely manner, are vital to ensuring consumers have access to the rights provided under the CPRA while also helping businesses operationalize the law's numerous new requirements.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses, to household brands, advertising agencies, and technology providers, including a significant number of California businesses. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Digital advertising contributes more than 1.1 million jobs to the California economy and approximately $2.4 trillion to the United States' gross domestic product ("GDP").[2] Our members engage in responsible data collection and use that benefits consumers and the economy, and we believe consumer privacy deserves meaningful and effective protections in the marketplace.

Our organizations responded to every request for comment from the California Attorney General ("OAG") to further its efforts to promulgate regulations under the California Consumer Privacy Act of 2018 ("CCPA"). For your reference, our comments in response to those requests are attached hereto as **Exhibit A**. We have consistently supported providing Californians with appropriate notice of businesses' data practices as well as the ability for those California consumers to exercise effective choices related to those practices. We ask the Agency to take our past

[1] *See* California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020*, located here (hereinafter, "RFC").
[2] *See* John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 5, 121-23 (Oct. 18, 2021), located here.

comments on the CCPA regulations into account as it begins the process of drafting regulations to implement the CPRA. We also ask the Agency to consider the following specific topics when issuing its initial draft regulations:

I. **The Agency Should Take a Leadership Role in Aligning State Privacy Laws.** The Agency is in a unique position to advance harmonization across differing state privacy laws, such as those in Virginia and Colorado. To the extent possible, we encourage the Agency to take steps to further uniformity across state privacy regimes.

II. **The Agency Should Ensure Opt-Out Preference Signals Are Truly User-Enabled and Are Not Set By Default.** The Agency should promulgate rules that reinforce the CPRA's requirement for opt-out preference signals to be affirmatively set by consumers. The Agency should prohibit intermediaries from setting such signals by default and should ensure that opt-out signals or other mechanisms do not inhibit businesses from communicating the consequences of opt out choices to consumers. We believe that this is in conformance with the California privacy laws.

III. **The Agency Should Appropriately Tailor Risk Assessment Requirements.** The Agency should require businesses to submit assessments only upon request in the context of a formal investigatory proceeding. The Agency should also make clear that turning assessments over to the Agency does not waive bedrock attorney-client privilege and work product protections.

IV. **The Agency Should Avoid Overly Prescriptive Rules Addressing Dark Patterns.** The Agency's dark patterns regulations should not overly constrain businesses' ability to engage with consumers. Such regulations should strike a balance of deterring deceptive and manipulative conduct while allowing for flexibility in the modes, methods, and content of business communications with consumers.

V. **The Agency Should Take Steps to Preserve the Benefits That Data-Driven Advertising Provides to Californians, to the Economy, and to All Consumers.** The Agency should recognize the benefits the data driven economy provides to consumers and should advance a regulatory approach that offers appropriate protections for Californians while still enabling them to benefit from the data economy.

We thank the Agency for the opportunity to provide comment on these topics, as discussed in more detail below, and we look forward to continuing to engage with the Agency as it promulgates draft regulations to implement the CPRA.

I. The Agency Should Take a Leadership Role in Aligning State Laws

In addition to California, Virginia and Colorado have recently enacted state privacy laws that are set to take effect in 2023.[3] To the extent possible, we encourage the Agency to use the

[3] Va. Code Ann. §§ 59.1-571 et seq.; Colo. Rev. Stat. §§ 6-1-1301 et seq.

regulatory process to work to harmonize the CPRA's requirements with privacy law requirements in other states. Although California was the first mover in the state privacy space and the Agency has been tasked with issuing regulations to address specific issue areas within the CPRA, the Agency should work to ensure its regulations' terminology and definitions align with other state laws to the extent practicable. Such alignment is in the best interest of consumers, the nation's policy on data privacy, and businesses alike. Because California is the first state to adopt broad data privacy regulations, the Agency has the unique opportunity to show leadership in this space by advancing harmonization of potentially conflicting state law standards.

Advancing uniformity across state privacy law requirements would not only create a more streamlined and less costly compliance environment for businesses with a national footprint,[4] but it would also minimize consumer confusion about potentially varying privacy rights and protections afforded in different states. In the absence of a national data privacy standard set by Congress, we ask the Agency to work intentionally to ensure its CPRA regulations are unified with, or at the very least do not conflict with, data privacy laws in other US jurisdictions.

II. Ensure Opt-Out Preference Signals Are Truly User-Enabled and Are Not Set By Default

In the Agency's invitation for preliminary comments, it requested comment on "[h]ow businesses should process consumer rights that are expressed through opt-out preference signals."[5] The CPRA appropriately sets a standard that enables businesses to elect whether to offer consumers the ability to opt out through a homepage link or through an opt out preference signal mechanism sent with the consumer's consent. We encourage the Agency to follow the explicit directives set forth in the CPRA by ensuring its rules surrounding opt-out preference signals further true consumer choice, allow businesses to communicate the consequences of opt out decisions to Californians, and do not allow opt-out preference signals to be set by intermediaries by default.

A. Legal Standard

The CPRA sets out a specific standard dictating when businesses must honor opt-out preference signals. According to the CPRA, businesses "**may elect**" to either "(a)… [p]rovide a clear and conspicuous link on the business's internet homepage(s) titled 'Do Not Sell or Share My Personal Information'" **or** (b) allow consumers to "opt-out of the sale or sharing of their personal information… through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]"[6] The CPRA makes this business choice explicitly clear by stating: "**A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or (b).**"[7] The CPRA therefore sets forth clear rules that specifically state businesses can elect whether or not to offer

[4] Estimated initial costs for CCPA compliance stand at a staggering $55 billion dollars, and estimated initial compliance costs for other state proposals, such as those in Florida, range from $6.2 billion to $21 billion. *See* California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019), located here; *see also* Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida* at 2 (Oct. 2021), located here.

[5] RFC at 5.

[6] CPRA, Cal. Civ. Code §§ 1798.135(a), (b) (emphasis added).

[7] *Id*. at § 1798.135(b)(3) (emphasis added).

consumers an opt-out preference signal option or an option to opt out via a clearly labeled homepage link.

B. Opt-Out Preference Signals Should Be User-Enabled

For businesses that elect to enable consumers to opt out of sales or sharing of personal information through opt-out preference signals or other such mechanisms, the CPRA directs the Agency to promulgate rules defining technical specifications for such controls. The CPRA places specific parameters around the Agency's promulgation of such rules. Namely, the opt-out signal or mechanism must "ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal **cannot unfairly disadvantage another business**."[8] According to the CPRA, the Agency must also ensure such opt-out preference signals or controls "clearly represent a consumer's intent and [are] **free of defaults constraining or presupposing such intent**."[9] The regulations should reflect these important elements of consumer choice that are set forth in the law. These parameters serve to help ensure consumer choices are genuine, and that opt-out preference signal regulations do not favor certain businesses over others, remove businesses' ability to communicate the consequences of opt out choices to consumers, or stand in the way of true and informed user choice.

Our past comments to the CCPA detail this issue in depth, as set forth in **Exhibit A**. In particular, beginning on page 2 of our March 27, 2020 comment to the OAG on the content of the CCPA regulations, we discussed ways that intermediary interference with consumers' use of global privacy controls could thwart the expression of true user choices. Finally, we addressed how the imposition of a global privacy control requirement should not turn the CCPA's and CPRA's explicit opt-out structure into an opt-in structure, thereby directly contravening the text of the law itself, which enables consumers to opt out of business sales of personal information, rather than have to turn off an automatic setting that assumes they want to opt out of sales across all businesses. We ask the Agency to review these comments for background and to ensure that regulations implementing the CPRA further informed consumer choice and the explicit opt out structure set forth in the law.

In addition, we provide in **Exhibit B** a consensus framework for evaluating whether opt-out preference signals or other mechanisms in the market are actually *user-enabled*. This consensus framework was developed by a broad group of stakeholders across the digital advertising industry. It requires an affirmative consumer choice to exercise the right to opt out and requires choice settings to be presented to consumers in ways that do not unfairly disadvantage certain businesses over others. The framework also requires a business to communicate the effect of the choice setting and the scope of the opt out to consumers. The framework also provides guidance regarding business transparency surrounding the choice signal and how consumers can opt in after previously having opted out of sales or sharing. We encourage the Agency to review the framework set forth in **Exhibit B** and to consider implementing it via regulation.

[8] *Id*. at § 1798.185(19)(A)(i) (emphasis added).
[9] *Id*. at § 1798.185(19)(A)(iii) (emphasis added).

C. Jurisdictional Signals

To ensure user choice is given the full force and effect under law, the Agency should permit a business to authenticate individuals submitting opt out requests as residents of California. Californians' rights to opt out of personal information sales and sharing may differ from the rights afforded to consumers in other states come 2023. For instance, in Virginia and Colorado, consumers will have the ability to opt out of "sales," "targeted advertising," and "profiling," as defined by those states' respective privacy laws. So that a business can determine the applicable state law and apply it accordingly, it is vital that requests indicate the relevant jurisdiction. The Agency should therefore take steps to clarify that opt-out preference signals must come with a jurisdictional tag so that businesses can afford the rights and privileges to consumers that align with their state of residence.

D. Default Settings

Californians should be permitted to exercise control over personal information associated with them, and that right should not be usurped by intermediary companies who stand between consumers and their access to the Internet. We ask the Agency to take steps to ensure that any technical standard or regulation promulgated surrounding opt-out preference signals or other global controls requires such mechanisms to be truly user-enabled and not set by default. Opt-out mechanisms should not permit such decisions to be set by intermediary companies or to be turned on by default. Ensuring that consumers – and not platforms, browsers, or other intermediaries – can make informed choices about personal information relating to them will help to ensure consumer preferences are carried out and consumer expectations are met.

We also encourage the Agency to issue regulations to make sure that opt out preference signals or other similar mechanisms are accompanied by effective notices that appropriately explain the effects and scope of choices that are available to consumers. Consumers should be given information about the consequences of their opt out choices so they can make informed privacy decisions. However, certain global privacy control implementations already in the marketplace are unconfigurable and set by default.[10] These default, unconfigurable controls inhibit consumers' ability to receive information about the implications of their privacy decisions. For example, the disclosures associated with the Brave browser's "Global Privacy Control" plugin provide no information on how the global control will impact the consumer, such as by increasing the likelihood the consumer will encounter paywalls or decreasing consumer's ability to receive ads that are personalized or relevant to them.[11] Global controls like this directly conflict with the requirements of CPRA, which require such controls to be free from defaults and "clearly described."[12] The Agency should take steps to ensure its regulations require opt out preference signals to be user-enabled and allow the effects of such signals to be appropriately explained to consumers.

---

[10] *See* Brave, *Global Privacy Control, a new Privacy Standard Proposal, now Available in Brave's Desktop and Android Testing Versions*, available at https://brave.com/web-standards-at-brave/4-global-privacy-control/ ("Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.")

[11] *Id*.

[12] CPRA, Cal. Civ. Code § 1798.185(19)(A)(iii).

III. Appropriately Tailor Risk Assessment Requirements

The Agency asked commenters to provide input on when processing should require a risk assessment under CPRA.[13] We encourage the Agency to: (1) require businesses to submit assessments to it only upon the Agency's request pursuant to a civil investigative demand or other formal investigatory process; (2) clarify that a single assessment conducted for purposes of compliance with other laws may satisfy CPRA assessment requirements; and (3) ensure that any requirements to turn over assessments to the Agency do not waive foundational attorney-client privilege or work product protections.

We ask the Agency to clarify that risk assessments must be provided to the Agency only upon request after it has served a civil investigative demand or similar formal inquiry on a business. Requiring risk assessments at any more regular cadence would create excessive compliance costs for businesses and would necessitate significant resources from the Agency to review assessments, thereby removing staff from devoting time to other areas of critical importance. In this area, the Agency can take steps to align the CPRA with other state privacy laws. For example, the Virginia Consumer Data Protection Act allows the Virginia Attorney General to request a company's data protection assessment pursuant to a civil investigative demand if such assessment is relevant to an ongoing investigation.[14] The Agency should adopt a similar approach to risk assessments under CPRA.

The Agency should also clarify that assessments conducted for purposes of compliance with other laws may satisfy CPRA requirements if the assessment conducted for compliance with another law addresses a comparable set of processing operations or includes similar activities. Laws that will go into effect imminently, such as the new privacy laws in Colorado and Virginia, require assessments for certain processing activities. Companies should not be required to perform separate assessments for each law if the processing activity that is the subject of the assessment is similar. The Agency should confirm that assessments conducted to comply with other privacy laws may satisfy CPRA requirements.

Finally, we encourage the Agency to clarify that a disclosure of a risk assessment to the Agency upon its request does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment. Attorney-client privilege and work product protections are crucial, long-standing principles that encourage open communications between businesses and their counsel. Declining to clarify that such protections extend to risk assessments would hinder businesses from being able to candidly work with their legal representatives to perform risk assessments to further compliance with data privacy laws. As a result, the Agency should clarify that its risk assessment regulations and any actions that would require a business to turn over risk assessments to the Agency do not waive critical attorney-client or work product protections.

---

[13] *See* RFC at 2.
[14] Va. Code. Ann § 59.1-576(c).

IV. Avoid Overly Prescriptive Rules Addressing Dark Patterns

In its request for comment, the Agency asked for input on "regulations, if any, that should be adopted to further define 'dark patterns.'"[15] The CPRA itself defines "dark pattern" to mean "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."[16] If the Agency takes steps to promulgate further regulations surrounding dark patterns, we ask it to avoid overly prescriptive mandates that do not enable flexibility for business communications with consumers.

While we agree the Agency should take steps to prevent unscrupulous actors from using deceptive and manipulative practices in the marketplace, we strongly believe overly prescriptive rules regulating the form and content of speech would not be in the best interests of California consumers or businesses. Notices and choice interfaces that are presented to consumers should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain elections. However, there should be flexibility for companies, channels, and platforms to present user information, choices, and notices to consumers in ways that make sense for the given company, channel, platform, and the consumer. For instance, a brick and mortar retailer may present notices and choices to consumers in a manner that is entirely different from a company that offers a smart speaker with no visible interface for written disclosures on the device. Regulations addressing dark patterns should not be so rigid that they limit businesses' ability to appropriately tailor and present disclosures and choices to their consumers, nor should they require businesses to present information in a way that lessens consumer engagement or hinders business innovation. We caution the Agency from overreaching in its rules on dark patterns, as overly prescriptive regulations could violate First Amendment protections for commercial speech as applied to the states through the due process clause of the Fourteenth Amendment.[17]

Responsible businesses do not endeavor to be deceptive or manipulative in their communications with consumers, because their relationships with customers are founded in consumer trust. Businesses are incentivized to maintain that relationship of trust with customers so consumers continue to come to them for products and services. We support regulations that would minimize deceptive and manipulative market practices when it comes to presenting consumer notices and choice interfaces, as we believe truthful, accessible, and clear notices and choice mechanisms benefit businesses and consumers alike. However, we ask the Agency to avoid issuing overly prescriptive rules that would too rigidly define how businesses must communicate with and present choices to consumers.

V. Data-Driven Advertising Provides Significant Benefits to Californians, to the Economy, and to All Consumers

Over the past twenty years, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A new study found that the Internet economy's contribution to the United States' GDP grew 22 percent per year since 2016 in a national economy that grows

[15] RFC at 6.
[16] CPRA, Cal. Civ. Code § 1798.140(l).
[17] *See* Exhibit A, December 27, 2020 Ad Trade Comments on Fourth Set of Proposed Modifications to Text of Proposed California Consumer Privacy Act Regulations at 3-6.

between two to three percent per year.[18] In 2020 alone, the Internet economy contributed $2.45 trillion to the U.S.'s $21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of $300 billion.[19] Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet, which amounts to 7 million more jobs than four years ago.[20] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.[21] The same study found that the ad-supported Internet contributed 1,111,460 full-time jobs across the state of California, well more than double the number of Internet-driven jobs from 2016.[22]

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulation that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy.[23] One recent study found that "if third-party tracking were to end "without mitigation" [t]he U.S. open web's independent publishers and companies, who are reliant on open web tech, would lose between $32 and $39 billion in annual revenue by 2025."[24] That same study found that the lost revenue would become absorbed by "walled gardens," entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.[25] Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated 15.5 billion in revenue.[26] Data-driven advertising has thus helped to democratize economic market power, ensuring that smaller online publishers can remain competitive with large corporations. A recent study showed that "long tail" publishers rely on third-party advertising technology, which accounts for approximately two-thirds of their advertising activity.[27]

B. Advertising Supports Californians' Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and life-saving information about COVID-19, in addition to other critical public health information related to missing children and catastrophic weather events such

---

[18] *See* John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 5 (Oct. 18, 2021), located here.
[19] *Id*.
[20] *Id*.
[21] *Id*. at 6.
[22] *Compare* John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 121-23 (Oct. 18, 2021), located here *with* John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem,* INTERACTIVE ADVERTISING BUREAU, 106 (2017), located here (finding that Internet employment contributed 478,157 full-time jobs to the California workforce in 2016 and 1,111,460 jobs in 2020).
[23] *See* John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located at https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf.
[24] *Id*. at 34.
[2525] *Id*. at 15-16.
[26] *Id*. at 28.
[27] Digital Advertising Alliance, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located at https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance.

as wildfires.[28] Advertising revenue is an important source of funds for digital publishers,[29] and decreased advertising spends directly translate into lost profits for those outlets. Since the coronavirus pandemic began, 62 percent of advertising sellers have seen advertising rates decline.[30] Publishers have been impacted 14 percent more by such reductions than others in the industry.[31] Revenues from online advertising support the cost of content that publishers provide and consumers value and expect. Regulations that inhibit or restrict preferred methods of digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, thereby compounding the detrimental impacts to the economy presented by COVID-19. The effects of such legislative models ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.[32] Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.[33] Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[34]

The ability of consumers to provide, and of companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We therefore respectfully ask you to carefully consider the potential impact of any

---

[28] Digital Advertising Alliance *Summit Snapshot: Data 4 Good – The Ad Council, Federation for Internet Alerts Deploy Data for Vital Public Safety Initiatives* (Sept. 2, 2021), located at https://digitaladvertisingalliance.org/blog/summit-snapshot-data-4-good-%E2%80%93-ad-council-federation-internet-alerts-deploy-data-vital-public.

[29] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[30] IAB, *Covid's Impact on Ad Pricing* (May 28, 2020), located at https://www.iab.com/wp-content/uploads/2020/05/IAB_Sell-Side_Ad_Revenue_2_CPMs_5.28.2020.pdf

[31] *Id*.

[32] Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

[33] Digital Advertising Alliance, *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.

[34] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

new regulations on data-driven advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing them through the rulemaking process.

* * *

In addition to the specific issues set forth above, we encourage the Agency to continue to engage with stakeholders who are impacted by the CPRA as it begins the process of drafting implementing regulations. Clear and consistent communication between consumers, businesses, the Agency Board, staff, and others involved in the CPRA regulatory process will be crucial to develop regulatory provisions that further the goal of advancing consumer privacy. We welcome future opportunities to respond directly to the regulatory provisions the Agency drafts. We hope to have a meaningful two-way dialogue on these important topics.

Thank you for your consideration of these comments. We look forward to working further with you on developing implementing regulations under CPRA.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

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

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

EXHIBIT A

December 6, 2019

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

Dear Attorney General Becerra:

As the nation's leading advertising and marketing trade associations, we provide the following comments to offer input on the California Office of the Attorney General's ("OAG") proposed regulations implementing the California Consumer Privacy Act ("CCPA"). We and our members support the objectives of the CCPA and believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, we have certain concerns about negative consequences the proposed regulations could create for consumers and businesses alike. Additionally, we are concerned that many of the proposed rules' provisions impose entirely new requirements on businesses that are outside of the scope of the CCPA and do not further the purposes of the law.

The undersigned organizations collectively represent thousands of companies in California and across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. Locally, our members help generate some $767.7 billion dollars for the California economy and support more than 2 million jobs in the state.[1] The companies we represent desire to comply with the CCPA by offering consumers robust privacy protections while simultaneously continuing to be able to do business in ways that benefit California's employment rate and its economy.

We provide the following comments to draw the OAG's attention to certain parts of the proposed regulations that are unsupported by statutory authority and other provisions that may have detrimental consequences for consumers and businesses alike. Below we provide a list of suggested updates to the proposed rules to bring them into conformity with the text of the CCPA and to rectify certain negative results they could cause for consumers and businesses. We also highlight certain provisions in the proposed regulations that we support for providing helpful clarity to the advertising and marketing industry. Some of the undersigned trades will file additional comments to the OAG.

[1] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), *located at* https://www.ana.net/magazines/show/id/rr-2015-ihs-ad-tax.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.[2] Calculating against those figures, the interactive marketing industry contributed $1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.[3]

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the FTC noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[4] It is in this sprit–preserving the ad supported digital and offline media marketplace while helping to design privacy safeguards–that we provide these comments.

---

[2] John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf.

[3] *Id*.

[4] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

II. The OAG Should Ensure the Proposed Regulations' Definitions Conform with the Text of the CCPA and Are Given Consistent Meaning

Although the OAG has provided definitions for several new terms in the proposed regulations, some of the definitions contradict the text of the CCPA itself and others are used inconsistently throughout the proposed regulations, thereby obscuring the meaning of the defined terms. For example, the OAG defined "request to know" in a way that departs from the text of the CCPA. In addition, the use of the defined term "request to delete" in at least one section of the proposed regulations is at odds with its definition in the proposed regulations as well as the text of the CCPA. We respectfully ask the OAG to update the proposed regulations so that the defined terms conform with the text of the CCPA and are given consistent meaning throughout the entirety of the draft rules.

The OAG defined "request to know" as "a consumer request that a business disclose personal information that it has about the consumer… [including] [s]pecific pieces of personal information that a business has about a consumer…."[5] This definition differs from the text of the CCPA, which states that "[a] consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer…" the categories and specific pieces of personal information "it has *collected about the consumer*."[6] To reduce business and consumer confusion and align the proposed regulations with California legislators' intent and the text of the CCPA, the OAG should update the proposed rules so a "request to know" is defined as "a consumer request that a business disclose personal information that it has collected about the consumer… [including] [s]pecific pieces of personal information that a business has collected about a consumer."

In addition, the OAG defined "request to delete" as "a consumer request that a business delete personal information about the consumer that the business has collected from the consumer…."[7] This definition aligns with the deletion right as it is set forth in the CCPA, which states that "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[8] However, in the section of the proposed regulations discussing the information that must be included in a privacy policy, the draft regulations note that a business must "[e]xplain that a consumer has a right to request the deletion of their personal information *collected or maintained* by the business."[9] The expression of the right to delete in the privacy policy section of the proposed regulations therefore contradicts with the CCPA's stated expression of the right and the proposed regulations' defined term "request to delete." The OAG should update the privacy policy section of the CCPA so it states that a business must explain that consumers have the right

[5] Cal. Code Regs. tit. 11, § 999.301(n)(1) (proposed Oct. 11, 2019).
[6] Cal. Civ. Code §§ 1798.110(a)(1), (5) (emphasis added).
[7] Cal. Code Regs. tit. 11, § 999.301(o) (proposed Oct. 11, 2019).
[8] Cal. Civ. Code §§ 1798.105(a).
[9] Cal. Code Regs. tit. 11, § 999.308(b)(2)(a) (proposed Oct. 11, 2019) (emphasis added).

"to request personal information about the consumer that the business has collected from the consumer" to align the section with the defined term "request to delete" and the CCPA.

As described above, we suggest that the OAG take steps to alter certain definitions in the proposed regulations so that they match and support the text of the CCPA and are used consistently throughout the draft rules. Such updates would help create certainty for businesses and consumers and would ensure that the text of the CCPA and the proposed regulations interpreting its terms are not in conflict.

III. Allow Flexibility for Businesses that Do Not Collect Information Directly to Provide Notice of Sale and an Opportunity to Opt Out

The CCPA states that a "third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out…."[10] Through the proposed regulations, the OAG has provided that the business must: (1) contact the consumer directly to provide notice of sale and notice of the right to opt out, or (2) confirm the source provided a notice at collection to the consumer; obtain signed attestations from the source describing how it gave notice at collection, including an example of the notice given to the consumer; retain such attestations and sample notices for two years; and make them available to consumers upon request.[11] The OAG should change this provision of the draft rules so businesses are not required to maintain and make available examples of the notice provided to a consumer at the time of collection.

Requiring businesses to maintain sample notices creates a substantial new business obligation that was not contemplated by the legislature when it passed or amended the law. Requiring examples of the notice that was provided to a consumer at the time of collection constitutes a requirement that is beyond the text, scope, and intent of the CCPA, as the law itself only requires a third party to ensure a consumer has received explicit notice of sale and an opportunity to opt out. Second, little if any additional consumer benefit is provided through this new business duty to maintain example notices. The requirement to obtain attestations from data sources confirming that a notice at collection was given and describing how the notice was given provides consumers with the same transparency benefits as requiring businesses to obtain and maintain samples of the notice that was given to consumers.

Finally, mandating that businesses must maintain examples of notices provided to consumers at the time of collection is unreasonable, significantly burdensome, and could place a considerable strain on normal business operations. For example, it is possible the proposed regulations could be interpreted to require businesses to pass example notices from original sources of data to third party businesses who may later receive personal information. This obligation would impose significant new recordkeeping obligations on third party businesses and could stifle the free flow of information that powers the Internet. We therefore ask the OAG to

[10] Cal. Civ. Code § 1798.115(d).
[11] Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).

remove the requirement for businesses to obtain examples of the notices at collection that were given to consumers to enable more flexibility for businesses to comply with the requirements the CCPA places on third parties who engage in personal information sale.

IV. Remove the Requirement to Respect Browser Signal Opt Outs so Consumers' Are Provided with Consumer Choice

The draft rules require businesses that collect personal information from consumers online to "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…."[12] This requirement is extralegal and goes beyond the text and scope of the CCPA by imposing a substantive new requirement on businesses that was not set forth by the legislature and does not have any textual support in the statute itself. For this reason and others we describe below, we ask the OAG to eliminate this requirement, or, at a minimum, give businesses the option to either honor browser plugins or privacy settings or mechanisms, or decline to 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 the sale of personal information.

The browser-based signal requirement in the proposed rules has no textual support in the CCPA itself. The California legislature could have included a browser-based signal mandate when it initially passed the CCPA, or when it amended it via multiple bills thereafter,[13] but the legislature never chose to impose such a requirement. Moreover, the California legislature already considered imposing a similar browser setting requirement in 2013 when it amended the California Online Privacy Protection Act.[14] The legislature ultimately decided against imposing a single, technical-based solution to enabling consumer choice and instead chose to offer consumers multiple avenues through which they may communicate their preferences. Together, these decisions reveal that the California legislature had the opportunity to enact a browser-based signal requirement on multiple occasions, but never chose to do so, and as such, the proposed regulation mandating that such signals be treated as verifiable consumer requests does not further legislative intent and is outside the scope of the CCPA.

If the OAG ultimately maintains this requirement, we suggest that the OAG modify 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. The latter approach is more consistent with the spirit of the CCPA and the intentions of the legislature, as it affords consumers with robust choice and control over the sale of personal information. In contrast, browser-based signals or plugins would broadcast a single signal to all businesses opting a consumer out from the entire data

[12] *Id*. at § 999.315(c).
[13] *See* AB 1121 (Cal. 2018); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).
[14] AB 370 (Cal. 2013).

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. Furthermore, 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.

In addition, certain intermediaries in the online ecosystem stand between consumers and businesses and therefore have the ability to interfere with the data-related selections consumers may make through technological choice tools. These intermediaries, such as browsers and operating systems, can impede consumers' ability to exercise choices via the Internet that may block digital technologies (*e.g.*, cookies, javascripts, and device identifiers) that consumers can rely on to communicate their opt out preferences. This result obstructs consumer control over data by inhibiting consumers' ability to communicate preferences directly to particular businesses and express choices in the marketplace. The OAG should by regulation prohibit such intermediaries from interfering in this manner.

We ask the OAG to eliminate the requirement to honor browser plugins or privacy settings or mechanisms, or, alternatively, revise the draft rules so that businesses have the option of honoring such settings or providing a "Do Not Sell My Personal Information" link along with another method for consumers to opt out of the sale of personal information by the business. We also ask the OAG to update the proposed rules to prohibit intermediaries from blocking or otherwise interfering with the technology used to effectuate consumer preferences in order to protect the opt out signals set by consumers via other tools.

V. Enable Effective Opt Out Mechanisms for Businesses that Do Not Maintain Personally Identifiable Personal Information

The proposed regulations require businesses to offer consumers a webform through which they may opt out of the sale of personal information.[15] However, webforms may not work to facilitate opt outs for online businesses that do not maintain personally identifiable information about consumers. Many businesses in the online ecosystem may maintain personal information that does not identify a consumer on its own, for example, IP addresses, mobile advertising identifiers, cookie IDs, and other online identifiers. For businesses that maintain this non-identifying information, webforms may not work to facilitate consumer requests to opt out, because the consumer's submission of identifying information such as a name, email address, or postal address may not be easily matched to the non-personally identifiable information the business does maintain. This provision could undermine the privacy-protective elements of the CCPA by forcing companies to attempt re-identification techniques which are widely avoided by industry in its efforts to enhance consumer privacy.[16] Consequently, the proposed rules should provide businesses with flexibility to offer mechanisms for consumers to opt out of personal information sale. The OAG has indicated it may issue another button or logo to enable a

[15] Cal. Code Regs. tit. 11, § 999.315(a) (proposed Oct. 11, 2019).
[16] *See* Fix CCPA, *Don't Force Companies to Connect Online Identities to Real Names*, *located at* https://www.fixccpa.com/.

consumer to opt out of the sale of personal information.[17] We encourage the OAG to consider industry leading implementations that already have consumer recognition in crafting another acceptable opt out mechanism. We also ask the OAG to clarify that online businesses that do not maintain personally identifying information may use an effective method to enable a consumer to opt out other than a webform.

VI. Clarify Businesses Are Not Required to Collect or Maintain More Personal Information to Verify a Consumer

Pursuant to the draft regulations, "[a] business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes."[18] The AG should clarify by regulation that businesses are not required to collect data they do not maintain or collect in the regular course of business in order to verify a consumer's identity.

Some businesses may maintain personal information in a manner that is not associated with a named actual person. For example, IP addresses and cookie IDs are kinds of personal information that could be associated with or linked to information from many consumers rather than information from a single consumer. Moreover, businesses often keep information that could identify a consumer's identity separate from other information that may not be identifying on its own. This practice is privacy protective, as it separates consumer identities from certain information collected about the consumer. The draft rules' current text could require businesses that do not maintain information that is associated with a named actual person to collect additional information from consumers in order to verify their identities. While the draft regulations acknowledge that "fact-based verification process[es]" may be required in such circumstances,[19] this provision of the proposed regulations could force businesses to investigate consumer identities by procuring more data than they normally would in their normal course of business in order to verify consumers.

A business should not be required to obtain additional information from consumers in order to comply with the CCPA. The purpose of the law is to enhance privacy protections for consumers, and forcing businesses to collect data they would not otherwise collect, maintain, or normally associate with a named actual person has the potential to undermine consumer privacy rather than enhance it.[20] The OAG should clarify that while businesses *may* collect additional

[17] Cal. Code Regs. tit. 11, at § 999.306(e) (proposed Oct. 11, 2019).
[18] *Id*. at § 999.323(c).
[19] *Id*. at 999.325(e)(2).
[20] For example, this mandate would force businesses to collect more information from consumers than they typically do in their normal course of business. Reports on the General Data Protection Regulation ("GDPR") in Europe have revealed that unauthorized individuals can exploit the law to access personal information that does not

information from a consumer to verify the consumer's identity, the business does not need to do so to comply with the law.

VII. Ensure that Businesses May Provide User-Friendly Privacy Policies to Consumers

The proposed regulations set forth certain requirements for businesses in providing privacy-related notices to consumers. Some of these requirements, such as the obligation to provide relevant disclosures with respect to *each category of personal information collected*, represent new obligations that are not expressly included in the text of the CCPA and may force businesses to produce excessively long and confusing privacy notices that would do little to further consumers' understanding of business data practices. Other notice-related requirements in the draft rules are unclear. For example, the draft regulations do not clearly state whether the required notice at collection, notice of right to opt out, and notice of financial incentive may be provided to consumers in a privacy policy. We urge the OAG to update the draft rules so that consumers may receive understandable privacy notices and so that businesses may provide all required privacy-related notices in a single privacy policy disclosure.

According to the proposed regulations, in privacy policies business must list the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information "[f]or *each category of personal information collected*…."[21] However, the terms of the CCPA itself do not require businesses to make disclosures relevant to each category of personal information collected, but rather require businesses to make disclosures with respect to all personal information collected. As such, requiring granular, category-by-category disclosures for each type of personal information collected imposes a significant new substantive requirement on businesses that has no textual basis for support in the CCPA.

Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from ensuring privacy policies are "written in a manner that provides consumers [with] a meaningful understanding of the categories listed."[22] If businesses must make disclosures about sources, purposes, and third parties for each category of personal information collected, privacy notices could be excessively complicated, lengthy, and incomprehensible for consumers, thereby impeding the purpose of providing an informative and understandable consumer privacy notice. Moreover, consumers would be less likely to read and understand such lengthy notices, which could impede the CCPA's goal of enhancing the transparency of business data practices. The OAG should align the regulations with the text of the CCPA by removing the "for each category of personal information collected" language. This change would enable consumers to receive meaningful privacy policies that sensibly disclose

---

belong to them, causing risks of identity theft. *See* BBC News, *Black Hat: GDPR privacy law exploited to reveal personal data* (Aug. 9, 2019), *located at* https://www.bbc.com/news/technology-49252501.

[21] Cal. Code Regs. tit. 11, § 999.308(b)(1)(d)(2) (proposed Oct. 11, 2019).

[22] *Id.*

required information in an undaunting and clear format and would advance California legislators' aim of enabling comprehensible, workable consumer notices more effectively than requiring disclosures pertaining to each category of personal information collected.

VIII. Allow Businesses to Satisfy All CCPA-Related Notice Requirements in a Privacy Policy

Pursuant to the proposed rules, businesses must provide a privacy policy and certain other particular notices to consumers. Specifically, in addition to a privacy policy, businesses must provide a notice at collection, a notice of the right to opt out of the sale of personal information, and a notice of financial incentive.[23] However, the proposed rules do not clearly state whether the notice at collection, notice of the right to opt out of the sale of personal information, or notice of financial incentive may be offered to consumers through the privacy policy. The OAG should clarify that all required notices may be provided in a privacy policy.

The draft rules state that a notice at collection may be provided through a conspicuous link on the business's website homepage, mobile application download page, or on all webpages where personal information is collected, which represent typical methods through which privacy policies are normally offered to consumers.[24] However, the draft rules do not expressly confirm that a notice at collection may be provided through the privacy policy. Similarly, while a notice of the right to opt-out must include certain particular information or link to the section of the business's privacy policy that contains such information, there is no explicit confirmation that the opt out notice requirement may be satisfied by providing the necessary information in a privacy policy.[25] Finally, if a business offers a financial incentive or price of service difference online, the business must link to the section of the business's privacy policy that contains the required information, but it is unclear whether making such a disclosure counts as the required notice of financial incentive that must be offered to consumers.[26]

We ask the OAG to update the proposed rules so they remove the requirement to provide disclosures with respect to each category of personal information collected, and so that they explicitly state that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy. These updates would lessen the possibility for consumer notice fatigue by enabling more concise, readable notices. They would also be consistent with consumer expectations and would enable more effective and less confusing consumer disclosures, as all privacy-related information could be housed in a unified location. Moreover, such a rule would help businesses in their efforts to meet the CCPA's requirements, because business would be able to focus on reviewing and updating one notice as needed instead of multiple notices. The OAG should clarify that all required notices may be

[23] *Id*. at §§ 999.305, 306, 307.
[24] *Id*. at § 999.305(a)(2)(e).
[25] *Id*. at § 999.306(b)(1).
[26] *Id*. at § 999.307(a)(3).

provided in a privacy policy, because such a clarification would reduce confusion for consumers and better enable CCPA compliance for businesses.

IX. Clarify that Requesting Verifying Information from a Consumer Pauses the Time Period Within Which a Business Must Respond to the Request

The proposed regulations set forth a risk-based process by which businesses may engage in efforts to verify consumers before acting on their requests to delete and requests to know.[27] We support the non-prescriptive, risk-based framework for verifying consumer requests that is outlined in the proposed regulations. It provides businesses the flexibility they need to create verification mechanisms that fit their business models while being robust enough to accurately identify consumers submitting CCPA requests. However, despite the beneficial nature of the risk-based approach for verifying consumer requests that is outlined in the proposed rules, we are concerned that the draft rules do not provide businesses with enough time to verify consumers before they are responsible for effectuating CCPA requests.

The draft rules require a business to comply with requests to know and delete within 45 days of receiving the request regardless of the period of time it takes for the business to verify the request.[28] We ask the OAG to reconsider this requirement and update the draft rules so 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. Such a result could have two distinct consumer harms: first, it would fail to fulfill the wishes of the consumer who actually submitted the request, and second, it could impact personal information about a consumer that did not make the request. Consequently, we urge the OAG to update the proposed rules so a business's request for verifying information tolls or pauses the 45-day period within which the business must respond to consumer requests to know and delete.

X. Clarify that a Business May Provide a General Toll-Free Number for Receiving CCPA Requests

According to the draft rules, a business must enable consumers to submit requests to know via a toll-free number and may provide a toll-free number to receive requests to delete and opt out of personal information sale. The proposed rules as currently drafted do not clarify if a business may offer its general toll-free number to receive CCPA requests or if a business must create a separate, CCPA-specific number through which it should receive consumer requests under the law. We ask the OAG to clarify that a business may offer consumers its general toll-free number to receive consumer CCPA requests and does not need to create or staff an entirely new phone number for such requests. Such an update to the proposed rules would decrease consumer confusion by funneling all business-related inquiries through one contact phone

[27] *Id*. at §§ 999.323, 324, 325.
[28] *Id*. at § 999.313(b).

number. It would also help businesses by refraining from imposing an unnecessary cost on them to staff and maintain a separate number for CCPA requests. Consequently, we urge the OAG to update the draft rules to clarify that a business can provide its general consumer telephone number as the toll-free phone number through which it may receive consumer CCPA requests.

XI. Remove the Requirement to Flow Down Opt Out Requests to Third Parties to Whom the Business has Sold Personal Information in the Prior 90 Days

The proposed rules would require businesses to pass on the opt out requests they receive to third parties. Specifically, a business must "notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt out and instruct them not to further sell the information."[29] This requirement does not further meaningful consumer choice, as it takes a consumer's opt out selection with respect to one business and propagates it throughout the ecosystem without the consumer's express consent to do so. Furthermore, it represents a departure from the text of the CCPA by imposing a brand-new requirement on businesses that was not contemplated by the text of the law itself.

Requiring businesses to pass on opt out requests to third parties that received the consumer's personal information in the prior 90 days could impede a consumer's ability to exercise specific choices that are effective against particular businesses. A consumer's choice to opt out of one business's ability to sell personal information does not mean that the consumer meant to opt out of every business's ability to sell personal information. This proposed rule has the potential to cause consumers to lose access to online offerings and content that they did not expect or choose to lose by submitting an opt out request to a single business. The law should not require businesses to understand a consumer's opt out choice as a decision that must apply throughout the entire Internet ecosystem. In addition, requiring businesses to communicate opt out requests to third parties is a substantial new obligation that does not give businesses enough time to build processes to comply with the requirement before January 1, 2020.[30] The CCPA, as passed by the Legislature, already provides a means for consumers to control onward sales by third party businesses. The law requires that consumers be provided explicit notice and opportunity to opt out from sale.[31] The new obligation to pass opt out requests on to third parties that received the consumer's personal information within the past 90 days moves beyond the text and intent of the CCPA by imposing material and burdensome new obligations on businesses

[29] *Id*. at § 999.315(f).

[30] The Standardized Regulatory Impact Assessment ("SRIA") analyzing the proposed regulations' economic effect on the California economy 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 that the requirement to pass opt out requests on to third parties that have received a consumer's personal information in the past 90 days would have throughout the Internet ecosystem and the economy. Under the draft rules, a consumer's single opt out of sale request would restrict beneficial uses of personal information, including those generally occurring subsequent to the initial sale. The OAG should consider how restricting the sale of personal information by third parties in this way can "increase or decrease… investment in the state." *See* Cal. Gov. Code § 11346.3(c)(1)(D).

[31] Cal. Civ. Code § 1798.115(d).

without textual support in the CCPA. We therefore encourage the OAG to update the proposed rules so businesses are not required to pass opt out requests along to third parties. Alternatively, the OAG should limit the requirement to information the business actually sold to third parties in the previous 90 days.

XII. Align the Draft Rules with Consumer Choices by Removing the Requirement to Convert Unverifiable Requests to Delete into Requests to Opt Out

If a business cannot verify a consumer who has submitted a request to delete, the proposed rules would require the business to "inform the requestor that their identity cannot be verified and… instead treat the request as a request to opt out of personal information sale.[32] Compelling businesses to convert unverifiable consumer deletion requests into opt out requests could hinder or even completely impede meaningful consumer choice in the marketplace. This mandate has the potential to force a result that the consumer neither intended nor approved. Consequently, we ask the OAG to update the proposed rules so that businesses are not forced to transform unverified deletion requests into opt out requests unless the consumer specifically asks the business to do so.

The CCPA provides separate consumer rights for deletion and opting out of personal information sale because these two rights achieve different policy aims and consumer goals. While deletion is structured to erase the consumer's personal information from the databases and systems *of the business to which the consumer communicates the request*, the opt out right empowers consumers to stop the transfer of data to *other businesses* in the chain. Because these two rights achieve two different objectives, the law should not compel consumers to opt out of personal information sale if a business cannot verify their request to delete. This outcome, which would be legally required by the proposed regulations, it is not likely to reflect the consumer's desires in submitting a deletion request.

To illustrate this point, the OAG's proposed rule requiring businesses to communicate opt out requests to third parties to whom they have sold personal information in the prior 90 days and instruct them not to further sell personal information could cause a consumer's unverified deletion request to be transformed into an opt out request that is imposed on many other parties other than the business that is the recipient of the request. As a result, a business may be required to transform a deletion request a consumer may have thought she served on one business alone into an opt out request by that business and pass that opt out request along to other businesses without obtaining the consumer's consent to take this action. This obligation therefore has the potential to unknowingly expose the consumer to potential loss of products and services she did not wish to lose. This result deprives consumers of the ability to make particularized selections about businesses who may and may not sell personal information. We therefore respectfully ask the OAG to align the draft rules with consumer choices by removing the requirement to convert unverifiable requests to delete into requests to opt out unless the consumer affirmatively requests that the business take such an action.

[32] Cal. Code Regs. tit. 11, § 999.313(d)(1) (proposed Oct. 11, 2019).

* * *

Thank you for the opportunity to submit input on the content of the proposed regulations interpreting the CCPA. We look forward to continuing to engage with your office as it finalizes the draft rules. Please contact us with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-296-2359

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

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-296-2359

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's
202-355-4564

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

CC: Mike Signorelli, Venable LLP

February 25, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Revised Proposed Regulations Implementing the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the content of the February 10, 2020 release of revised proposed regulations implementing the California Consumer Privacy Act ("CCPA").[1] We appreciate the opportunity to continue to engage with the OAG on the important subject of consumer privacy and the implementing regulations that will help shape privacy protections in the state of California.[2]

We and our members strongly support protecting the privacy of Californians, and we believe consumer privacy deserves meaningful protection. We are encouraged by several updates the OAG made to the CCPA implementing regulations that will enhance consumer privacy and provide more clarity for businesses in their efforts to operationalize the law's terms. However, certain specific issues, which we address below in this letter, could be further clarified to help preserve consumers' ability to exercise meaningful choice in the marketplace and businesses' ability to provide products and services that consumers expect and value. We are also concerned that the quickly impending CCPA enforcement date of July 1, 2020 will leave little to no time for businesses to implement the changes the OAG has made to the draft regulations as well as any additional updates the OAG may make to the regulations before July of this year.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Locally, our members are estimated to help generate some $767.7 billion dollars for the California economy and support more than 2 million jobs in the state.[3] Our members want to provide consumers with robust privacy protections while simultaneously maintaining their ability to do business in ways that benefit California's employment rate and its economy. We believe a regulatory scheme that enables strong individual privacy protections alongside continued economic development and advancement will best serve California consumers.

---

[1] *See* California Department of Justice, *Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File* (Feb. 10, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?.

[2] Our organizations submitted joint comments on the content of the OAG's original proposed rules implementing the CCPA. *See Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/priavcy/ccpa-public-comments.pdf at CCPA 00000431 - 00000442.

[3] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana.net/getfile/23045.

The requests we pose in this submission represent targeted suggestions to improve the CCPA implementing regulations for consumers and businesses alike. These comments are supplementary to filings that may be submitted separately and individually by the undersigned trade associations.

I. Afford Businesses Time to Update Their Practices in Light of Regulatory Revisions

Although the CCPA went into effect on January 1, 2020, the final regulations have not yet been promulgated, leaving our members and thousands of other California businesses uncertain concerning their ultimate compliance obligations. Given the extraordinary complexity of the law and the potential for other open issues to be clarified in subsequent updates to the draft rules, there will not be sufficient time for businesses to effectively implement the final regulations prior to the anticipated enforcement date of July 1, 2020. We therefore ask you to delay enforcement of the CCPA until January 2021 in order to provide businesses a sufficient time period to implement the new regulations before being subject to enforcement.

a. It Is Appropriate to Provide Businesses a Reasonable Period of Time to Implement the Regulatory Updates

As soon as the California Legislature passed the CCPA, it was clear that the law's requirements would evolve through both the legislative and rulemaking process. It was not clear, however, that key CCPA provisions would be substantially amended so close to its effective date, and that the rules implementing its terms would not be finalized until after the law became operative.

While we recognize that the amendments in the California Legislature delayed the development and formal release of draft regulations implementing the CCPA until October 11, 2019,[4] these draft rules presented significant new and unprecedented requirements, such as entirely new recordkeeping obligations, notice requirements, and verification rules, among many other novel obligations.[5] Then, on February 10, 2020, the rules changed again, altering the requirements businesses had used to build systems, processes, and policies for the CCPA. Businesses are contending with the proposed regulations' new mandates from both the October 11, 2019 and February 10, 2020 release of draft rules, and they are working earnestly to adjust their systems and build new processes to facilitate compliance.

Unfortunately, it is presently unclear when the rules will be finalized and whether they will be further amended. Just mere months before enforcement is scheduled to begin, companies that are subject to the CCPA are faced with the possibility that the draft rules could substantially change again and impose other entirely new requirements and nuances on businesses. If the rules change again, the OAG must issue a new notice in the California Regulatory Notice Register and provide for another comment period of 15 to 45 days.[6] The rules will not be effective until they are submitted and reviewed by the Office of Administrative Law, further reducing the time available to businesses to implement the regulations. This timeline increases the likelihood that the draft rules will not be finalized before, or only a short period prior to the law's July 1, 2020 enforcement date.

We and our members strongly support the underlying goals of the CCPA. The limited and quickly shrinking time before the existing enforcement deadline, however, will place businesses in a nearly untenable position. Without final regulatory requirements, businesses will be unable to make operational changes to their systems, further delaying finalization of their compliance programs. Businesses should be

---

[4] *See* State of California Office of Administrative Law, *Notice Publication/Regulations Submission* (Oct. 11, 2019), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std400a.pdf.
[5] Cal. Code Regs. tit. 11, § 999.305-308, 317, 323-325 (proposed Feb. 10, 2020).
[6] *See* Office of the Attorney General, California Department of Justice, *California Consumer Privacy Act (CCPA): Background on Rulemaking Process* at 3, located at https://oal.ca.gov/rulemaking_participation.

afforded an appropriate time period to implement the new regulations once they become final and before being subject to enforcement.

b. Providing a Reasonable Period of Time for Implementing the New Regulations Benefits Consumers

While the law instructs the OAG not to bring any enforcement action prior to July 1, 2020, there is no restriction on you providing a reasonable period of additional time for California businesses to review and implement the final regulations before your office initiates any enforcement actions.[7] Thus, in order to avoid consumer and business confusion with respect to the new rules, we request that you delay enforcement of the law to begin in January 2021. This short deferral will give businesses the time they need to understand and effectively operationalize the rules helping ensure consumers have access to the rights afforded under the new law.

Business attempts to comply with an incomplete legal regime risk causing significant consumer frustration and the implementation of inadequate or duplicative compliance tools. While we understand that your office is working expeditiously to provide clear rules for businesses to operationalize the CCPA, the clock is working against well-intentioned businesses in their compliance efforts. We urge you to give California business the opportunity to understand what is required under the law before they are at risk for being penalized for violating its terms.

While our members support California's intent to provide consumers enhanced privacy protections, the evolving nature of the CCPA and the draft nature of the proposed rules make the current enforcement date of July 1, 2020 a difficult deadline for businesses and consumers alike. Consumer privacy is best served when businesses that leverage data do so in accordance with clear and concrete laws and regulations that present them with adequate time to adjust their practices to come into compliance with new requirements.

We urge you to provide a moratorium on enforcement until January 2021, thereby giving businesses throughout the United States that operate in California adequate time to prepare to adhere to the law's final form. Delaying the CCPA's enforcement in this manner will help ensure that businesses can effectively provide consumers with the new protections and rights that the law and its implementing regulations require.

II. Enable Consumer Choice By Removing the Requirement to Honor Browser Settings and Global Privacy Controls

The revised proposed rules require businesses that collect personal information from consumers online to treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism that signals the consumer's choice to opt out of the sale of personal information, as a valid request submitted for that browser, device, or consumer.[8] In our prior submission to the OAG, we explained that this requirement robs consumers of the ability to exercise granular choice. This mandate would obstruct consumers' individualized, business-by-business decisions about entities that can and cannot engage in the sale of personal information. Moreover, this requirement represents an obligation that has no support in the text of the CCPA itself and extends far beyond the likely intent of the California Legislature in passing the law. For these reasons, we renew our request for the OAG to remove the requirement to respect user-enabled global privacy controls, or, at a minimum, to give businesses the

[7] Cal. Civ. Code § 1798.185(c).
[8] Cal Code Regs. tit. 11, § 999.315(d) (proposed Feb. 10, 2020).

option to honor user-enabled global privacy controls or decline to honor such settings if the business offers another, equally effective method for consumers to opt out of personal information sale.

The requirement to honor user-enabled global privacy controls is a substantive obligation that the California Legislature did not include in the text of the CCPA itself. Despite numerous amendments the legislature passed to refine the CCPA, none of them included a mandate to honor browser signals or global privacy controls. Additionally, the California Legislature considered a similar requirement in 2013 when it amended the California Online Privacy Protection Act, but it declined to impose a single, technical-based solution to address consumer choice and instead elected to offer consumers multiple ways to communicate their preferences to businesses.[9] The revised proposed rules' imposition of a requirement to honor user-enabled privacy controls would result in broadcasting a single signal to all businesses opting a consumer out from the entire data marketplace. This requirement would obstruct consumers' access to various products, services, and content that they enjoy and expect to receive.

Additionally, requiring businesses to honor global, single-signal privacy control opt out choices would effectively convert the CCPA's statutorily mandated opt out regime to an opt in regime. Because businesses would be required to respect a user-enabled global privacy control opt out setting under the draft rules, they would be forced to approach consumers on an individualized basis to ask them to opt in to personal information sale after receiving a user-enabled global privacy setting opt out through a browser. This outcome is certainly not the result the California Legislature intended in passing the CCPA, which clearly proposes an opt out approach to consumer data sales rather than an opt in approach.[10]

In the most recent iteration of the draft rules, the OAG added provisions to the requirement that allow a business to notify a consumer of a conflict between any business-specific privacy setting or financial incentive and a global privacy control.[11] According to the updated regulations, a business may give the consumer a choice to confirm the business-specific setting or the global privacy control.[12] However, the draft rules still require a business to "respect the global privacy control," thereby forcing businesses to act on global privacy settings before they can confirm whether the consumer actually wanted to make a choice to end beneficial transfers of data that occur via the Internet.[13] This option, therefore, does nothing to further a consumer's actual desired or expressed choices. The fact that the rules now allow for a business to confirm a consumer's intentions does little to save the consumer from unintentionally losing access to various products, services, and valuable content through the Internet. Additionally, this provision stands to advantage certain players in the market that have a direct relationship with consumers. Businesses that do not directly interact with consumers online, such as third-party entities, would not have the ability to confirm whether a consumer intended to apply a browser signal or privacy setting to the entire Internet or whether the consumer would rather abide by the choice the consumer made with respect to that particular business.

The revised proposed rules also note that a privacy control "shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings."[14] Although this new provision reduces the potential for default settings to miscommunicate consumers' actual preferences, it does not address the fact that intermediaries in the online ecosystem stand between consumers and businesses and have the ability to interfere with the data-related selections consumers may make through technological choice tools. Obligating businesses to honor user-enabled privacy settings

[9] *See* AB 370 (Cal. 2013).
[10] Cal. Civ. Code § 1798.120.
[11] Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Feb. 10, 2020).
[12] *Id.*
[13] *Id.*
[14] *Id.* at § 999.315(d)(2).

that are presented to consumers through an intermediary vests power in the hands of the intermediary and risks inhibiting consumers' ability to communicate preferences directly to particular businesses. It also makes intermediary meddling in consumers' expressed privacy choices harder to detect, especially if a consumer makes a choice directly with a business that conflicts with a global opt-out signal set by a browser.

To preserve consumers' ability to exercise granular choices in the marketplace, to keep the regulations' requirements in line with legislative intent in passing the CCPA, and to reduce entrenchment of intermediaries and browsers that have the ability to exercise control over user-enabled privacy settings, we ask the OAG to remove the requirement to honor user-enabled privacy controls. Alternatively, we ask the OAG to update the draft rules so a business may *either* honor user-enabled privacy controls or decline to honor such settings *if* the business provides another equally effective method for consumers to opt out of personal information sale, such as a "Do Not Sell My Personal Information" link.

III. Clarify Financial Incentive Terms So Californians May Continue to Benefit from Consumer Loyalty Programs

The OAG did not take steps to materially clarify the draft rules' financial incentive requirements in its revisions to the proposed regulations. Without additional clarity on this issue, loyalty programs offered in California could be significantly undermined due to business confusion regarding how to implement the regulatory mandates. We respectfully ask the OAG to clarify or remove the rules' ambiguous terms requiring businesses to ensure that financial incentives are reasonably related to the value of a consumer's data. We also ask the OAG to clarify or remove the requirement to disclose an estimate of the value of the consumer's data as well as the method of calculating such value in a notice of financial incentive.

According to the revised proposed rules, "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference."[15] Despite this mandate, the draft rules do not provide any helpful information regarding how a business may justify that a price or service difference is reasonably related to the value of a consumer's data. The revised proposed regulations also do not address how businesses may reasonably quantify nontangible value in terms of fostering consumer loyalty and goodwill.

Californians greatly benefit from loyalty and rewards programs and the price differences and discounts they receive for participating in those programs. Loyalty programs exist due to consumers' widespread participation in such programs. Without consumer data, loyalty programs would not be possible. Consumer data increases businesses' access to useful information as well as their ability to generate revenue by marketing their products and services. Allowing consumers to continue to participate in loyalty programs without providing personal information to the business would defeat the purposes of the programs. Consumers who opt out or delete personal information from the loyalty program would essentially be permitted a "free ride" on the program, reaping all of its benefits due to data provided by other consumers. Additionally, it is not immediately apparent how any business can ensure that the program is "reasonably related to the value of the consumer's data." The lack of clarity on this issue and the "free rider" problem enabled by the draft regulations could cause many businesses to decline to continue offering loyalty programs to California residents.

Moreover, the requirement to disclose an estimate of the value of the consumer's data as well as the method of calculating such value in a notice of financial incentive represents a particularly onerous

[15] *Id*. at § 999.336(b).

requirement that would engender consumer confusion and could have anticompetitive effects.[16] Businesses typically offer multiple discounts to consumers through loyalty programs at one time. Requiring businesses to disclose an estimate of the value of the consumer's data and the method of calculating such value would inundate and confuse consumers with multiple and potentially duplicative privacy notices and would provide no tangible consumer benefit. Additionally, disclosing such information in a privacy notice could reveal confidential information about a business and pose risks to the business's competitive position in the market. Forcing businesses to reveal internal and proprietary valuations of data could negatively impact competition and could impose significant risks to business proprietary information.

For the foregoing reasons, we respectfully ask the CA AG to clarify or remove the unreasonably onerous financial incentive requirements inherent in the revised rules. In particular, we ask the OAG to clarify or remove the provisions requiring businesses to disclose a good faith estimate of the value of the consumer's data, disclose their methods of calculating such value, and ensure that financial incentives offered through loyalty programs are reasonably related to the value of the consumer's data. These requirements are particularly unclear and therefore could be impossible to operationalize. Without additional clarity, the draft rules' financial incentive terms could inhibit or drastically reduce the availability of loyalty programs offered in the state.

* * *

Thank you for the opportunity to submit input on the content of the revised proposed regulations implementing the CCPA. We look forward to continuing to engage with the OAG as it takes steps to finalize the draft rules. Please contact Mike Signorelli of Venable LLP at 202-344-8050 with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

[16] *Id*. at § 999.307(b)(5).

March 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Second Set of Proposed Regulations Implementing the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the proposed regulation included in 999.315(d) of the March 11, 2020 release of the second set of modifications to the text of the proposed regulations implementing the California Consumer Privacy Act ("CCPA").[1] This requirement exceeds the scope of the OAG's ability to regulate in conformance with the CCPA, runs afoul of free speech rights inherent in the United States Constitution, and impedes the ability of consumers to exercise granular choices in the marketplace. We ask that it be struck or modified per the below comment.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Locally, our members are estimated to help generate some $767.7 billion dollars for the California economy and support more than 2 million jobs in the state.[2] We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous submissions and in the sections that follow below, the draft regulations implementing the law could be updated to better enable consumers to exercise meaningful choices and to help businesses in their efforts to continue to provide value to California's consumers and its economy.[3]

Despite businesses' best efforts to develop compliance strategies for the CCPA, current events coupled with the unfinalized nature of the draft rules stand in the way of entities' earnest work to facilitate compliance with the law. As we have discussed in our prior submissions, the draft rules' onerous terms concerning global controls and browser settings stand to impede consumer choices as well as access to various products, services, and content in the digital ecosystem. More urgently, the novel coronavirus known as COVID-19 has shaken businesses' standard operating procedures as well as the development of policies, processes, and systems for the CCPA. In this period of crisis facing the world-at-large, entities should be focused on dedicating funds, time, and efforts to supporting their employees and the response to

---

[1] *See* California Department of Justice, *Notice of Second Set of Modifications to Text of Proposed Regulations* (Mar. 11, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-second-mod-031120.pdf?.

[2] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana.net/getfile/23045.

[3] Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. *See Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/priavcy/ccpa-public-comments.pdf at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf at CCPA_15DAY_000554 – 000559.

the coronavirus outbreak rather than diverting resources to prepare for an ever-evolving set of regulations under the CCPA. Therefore, we support the request made earlier this month by a group of sixty-six (66) trade associations, organizations, and companies to your office asking you to delay enforcement until January 2, 2021.[4]

Our members are committed to offering consumers robust privacy protections while simultaneously maintaining their ability to support California's employment rate and its economy in these unprecedented times as well as access to ad-funded news. We believe a regulatory scheme that enables strong individual privacy protections alongside continued economic development and advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA implementing regulations for Californians as well as the global economy.[5]

I. Give Businesses the Option to Honor Browser Settings and Global Controls

The revised proposed rules require businesses that collect personal information from consumers online to treat user-enabled global controls, such as a browser plugin or setting, device setting, or other mechanism that purports to carry signals of the consumer's choice to opt out of the sale of personal information, as a valid request submitted for that browser, device, or consumer.[6] This requirement exceeds the scope of the OAG's authority to regulate pursuant to the CCPA, runs afoul of free speech rights inherent in the United States Constitution, and impedes consumers of the ability to exercise granular choices in the marketplace. For these reasons, we ask the OAG to remove this requirement, or, at a minimum, to give businesses the option to honor such controls or decline to honor such settings if the business offers another, equally effective method for consumers to opt out of personal information sale.

a. The Browser Setting and Global Control Mandate Exceeds the OAG's Regulatory Authority Pursuant to the CCPA

Requiring businesses to honor such controls and browser settings is an obligation that has no support in the text of the CCPA itself and extends far beyond the intent of the California Legislature in passing the law. Under California administrative law, when an agency is delegated rulemaking power, rules promulgated pursuant to that power must be "within the lawmaking authority delegated by the Legislature," and must be "reasonably necessary to implement the purposes" of the delegating statute.[7] The CCPA gives the OAG power to "adopt regulations to further the purposes of [the CCPA]," but not to adopt regulations that contravene the framework set up by the Legislature when it passed the law.[8]

The CCPA was plainly structured to provide consumers with the right to opt out of sales of personal information.[9] However, the requirement to respect the proposed controls and browser settings effectively transforms the CCPA's opt-out regime into an opt-in regime by enabling intermediaries to set opt-out signals through browsers that apply a single signal across the entire Internet marketplace. Individual businesses will consequently be forced to ask consumers to opt in after receiving a global opt-out signal set by an intermediary, thereby thwarting the granular opt-out structure the California Legislature purposefully enacted in passing the CCPA. The OAG's regulation mandating that businesses

---

[4] *Joint Industry Letter Requesting Temporary Forbearance from CCPA Enforcement* (Mar. 20, 2020), located at https://www.ana.net/getfile/29892.

[5] These comments are supplementary to filings that may be submitted separately and individually by the undersigned trade associations.

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

[7] *Western States Petroleum Assn. v. Bd. of Equalization*, 304 P.3d 188, 415 (Cal. 2013) (quoting *Yamaha Corp. of America v. State Bd. Of Equalization*, 960 P.2d 1031 (Cal. 1998)).

[8] Cal. Civ. Code § 1798.185.

[9] *Id*. at § 1798.120.

obey such controls and browser signals therefore exceeds the scope of the OAG's authority to issue regulations under the CCPA.

The requirement to obey such controls is a substantive obligation that the California Legislature did not include in the text of the CCPA itself. Despite numerous amendments the legislature passed to refine the CCPA, none of them included a mandate for browser signals or global controls. Additionally, the California Legislature considered a similar requirement in 2013 when it amended the California Online Privacy Protection Act ("CalOPPA"), but it declined to impose a single, technical-based solution to address consumer choice and instead elected to offer consumers multiple ways to communicate their preferences to businesses.[10] The Legislature did not intend to institute a requirement to mandate global controls or browser signals when it amended CalOPPA in 2013, and it similarly did not intend to do so when it passed the CCPA in 2018. The obligation to honor such signals in the draft rules therefore thwarts legislative intent and is an impermissible exercise of the OAG's ability to issue regulations under the law.

b. The Browser Setting and Global Control Mandate Contravenes Constitutional Rights to Free Speech

The OAG's proposed rule regarding such controls and browser signals violates the First Amendment to the United States Constitution by converting the CCPA's opt-out structure into a de facto opt-in structure and by improperly restricting free speech. Businesses' dissemination of the data they collect constitutes constitutionally protected commercial speech.[11] A regulation restricting commercial speech is unconstitutional unless the state has a substantial interest in restricting this speech, the regulation directly advances that interest, and the regulation is narrowly tailored to serve that interest.[12] While there may be a substantial state interest in protecting consumer privacy, [13] the OAG's directive to respect such controls and browser settings does not advance the government's substantial interest. Moreover, this rule is not narrowly tailored to advance such an interest. The regulatory requirement therefore violates the First Amendment.

Commercial speech is entitled to protections under the United States Constitution. Regulations that provide "'ineffective or remote support for the government's purpose'" impermissibly burden constitutional protections afforded to commercial speech.[14] The wide-ranging opt-out structure set forth by the California Legislature and the OAG particularly focus on a consumer's relationship with an individual business. This structure enables consumers to express opt-out preferences in the context of their unique relationships with individual entities. By contrast, the global controls mandate obligates businesses to figure out consumers' individual preferences regarding data disclosures from a singular browser setting. Moreover, requiring businesses to defer to such controls as a way to understand consumers' true preferences is less effective and less direct than the opt-out methods employed by the rest of the OAG's regulations. If the state's interest is in stopping the disclosure of specific data that a consumer wishes to restrict from sale, such a proposal does not adequately further this aim. It provides no way for businesses

---

[10] *See Assembly Committee on Business, Professions and Consumer Protection*, Hearing Report on AB 370 (Cal. 2013) (Apr. 16, 2013), located at https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140AB370# ("According to the California Attorney General's Office, 'AB 370 is a transparency proposal – not a Do Not Track proposal. When a privacy policy discloses whether or not an operator honors a Do Not Track signal from a browser, individuals may make informed decisions about their use of the site or service.')

[11] *See Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001); *Boetler v. Advance Magazine Publishers Inc.*, 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016).

[12] *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

[13] *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1192 (W.D. Wash.).

[14] *Id*. (quoting *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980)).

to divine that a consumer wishes to keep personal information within the confines of a specific business relationship, and instead compels businesses to guess at consumers' preferences from an indirect signal that may not accurately reflect a consumer's wishes.

In addition, the AG's proposed rule is not narrowly tailored to serve the state's interest. Instead, it senselessly restricts the commercial speech of businesses without supporting the efficacy of the existing opt-out framework. Narrowly tailored regulations are not disproportionately burdensome. Additionally, they must "signify a careful calculation of the costs and benefits associated with the burden on speech imposed."[15] The existing opt-out regime implemented by the California Legislature offers businesses more exact information about specific, granular preferences of individual consumers than the global controls mandate. The global controls requirement serves no purpose that is not already served by existing opt-out rules in the draft regulations and the law itself, and it could potentially restrict speech by requiring businesses to act on inaccurate information about a consumer's individual preferences.

The proposed regulations note that businesses may contact consumers to ascertain their true intent regarding personal information sales if a global control conflicts with a choice the consumer individually set with the business. However, the rules require the business to defer to the global controls in the meantime, thus mandating a potentially incorrect expression of user preferences at the expense of specific choices the consumer indicated to the contrary. In addition, businesses bear the burden of ascertaining the consumer's true intent after receiving a global signal that does not align with an individual consumer's preferences. In contrast, the opt-out privacy framework set forth in the CCPA itself and bolstered by the draft rules is both more precise and less burdensome. It enables businesses to assess specific preferences of users in the context of each unique consumer relationship, and it restricts commercial speech only if that speech is known to contravene consumer preferences. The global controls mandate consequently does not further the goals of the existing framework, but it does needlessly restrict commercial speech. The global controls rule therefore does not pass constitutional muster because it burdens commercial speech without appropriately balancing those burdens with benefits.

c. The Browser Setting and Global Control Mandate Impedes Consumer Choice

The revised proposed rules' imposition of a requirement to honor such controls would result in broadcasting a single signal to all businesses, opting a consumer out from the entire online ecosystem. This requirement would obstruct consumers' access to various products, services, and content that they enjoy and expect to receive, and it would thwart their ability to exercise granular, business-by-business selections about entities that can and cannot sell personal information in the digital marketplace.

In the March 11, 2020 updates to the draft rules, the OAG removed the requirement for a consumer to "affirmatively select their choice to opt-out" and the requirement that global controls "shall not be designed with any pre-selected settings."[16] The removal of these provisions entrench intermediaries in the system and will advantage certain business models over others, such as models that enable direct communications between consumers and businesses. It will also enable intermediaries to set *default* signals through browsers without consumers having to approve of them before they are set. This outcome risks causing businesses to take specific actions with respect to consumer data that the consumer may not want or intend. The OAG should take steps to ensure that default privacy signals may not be set by intermediaries without the consumer approving of the signals set and the choices they relay to businesses.

Moreover, the draft rules do not address how businesses should interpret potentially conflicting signals they may receive directly from a consumer and through a global control or a browser setting. For

[15] *Id*. at 1194.
[16] Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Mar. 11, 2020).

example, if a business directly receives a consumer's permission to "sell" personal information, but later receives a global control signal through a browser set by default that indicates the consumer has opted out of such sales, which choice should the business follow? The CCPA itself allows businesses to contact consumers asking them to opt in to personal information sales after receiving opt-out signals only once in every twelve month period.[17] As such, the business's ability to communicate with the consumer to ascertain their true intentions may be limited despite the draft regulations' statement that a business may notify consumers of conflicts between setting and give consumers the choice to confirm the business-specific setting.

To preserve consumers' ability to exercise granular choices in the marketplace, to keep the regulations' requirements in line with constitutional requirements and legislative intent in passing the CCPA, and to reduce entrenchment of intermediaries and browsers that have the ability to exercise control over settings, we ask the OAG to remove the requirement to obey such controls. Alternatively, we ask the OAG to update the draft rules so a business may *either* honor user-enabled privacy controls or decline to honor such settings *if* the business provides another equally effective method for consumers to opt out of personal information sale, such as a "Do Not Sell My Personal Information" link.

* * *

Thank you for the opportunity to submit input on the content of the revised proposed regulations implementing the CCPA. Please contact Mike Signorelli of Venable LLP at 202-344-8050 with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

[17] Cal. Civ. Code § 1798.135(a)(5).

October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Third Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the third set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.[1]

As explained in more detail below, the OAG's proposed modifications: (1) unreasonably restrict consumers from receiving important information about their privacy choices, (2) prescriptively describe how businesses must provide offline notices, and (3) unfairly fail to hold authorized agents to the same consumer notice standards as businesses. The OAG's potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses' right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG's proposed edits to Section 999.306 could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify the modifications per the below comments.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising expenditures. Locally, our members are estimated to help generate some $767.7 billion dollars for the California economy and support more than 2 million jobs in the state.[2] We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in the sections that follow below, the draft regulations implementing the law should be updated to better enable consumers to exercise informed choices and to help businesses in their efforts to continue to provide value to California consumers while also supporting the state's economy.[3]

---

[1] *See* California Department of Justice, *Notice of Third Set of Proposed Modifications to Text of Regulations* (Oct. 12, 2020), located at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-third-mod-101220.pdf?.

[2] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana.net/getfile/23045.

[3] Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. *See Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf at CCPA_15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California*

Our members are committed to offering consumers robust privacy protections while simultaneously providing access to ad-funded news, apps, and a host of additional online services. These are offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. The most recent modifications to the CCPA regulations set forth a prescriptive interpretation of the CCPA that could limit our members' ability to support California's employment rate and its economy in these unprecedented times. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as the economy.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

The U.S. economy is fueled by the free flow of data. Throughout the past three decades of the commercial Internet, one driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet by delivering new, innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this responsible advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.[4] This means that the interactive marketing industry contributed $1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.[5]

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.[6] The survey also found that consumers estimate the personal value of ad-supported content and services on an annual basis to be $1,403.88, representing an increase of over $200 in value since 2016.[7] Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored

---

Consumer Privacy Act, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf at CCPA_2ND15DAY_00309 - 00313.

[4] John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf.

[5] *Id*.

[6] Digital Advertising Alliance, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf.

[7] *Id*.

experience, and research demonstrates that they are generally not reluctant to participate online due to data-driven advertising and marketing practices.

Without access to ad-supported content and online services, many consumers would be unable or unwilling to participate in the digital economy. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[8] The ad-supported Internet therefore offers individuals a tremendous resource of open access to information and online services. Without the advertising industry's support, the availability of free and low-cost vital online information repositories and services would be diminished. We provide the following comments in the spirit of preserving the ad-supported digital and offline media marketplace that has provided significant benefit to consumers while helping to design appropriate privacy safeguards to provide appropriate protections for them as well.

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."[9] This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported Internet would be unduly hindered, thereby undermining a consumer's ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising. However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business' provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would

[8] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.
[9] Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet as described in Section I, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer to "to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request" the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses' ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt out choice while facilitating the consumer's request to opt out.

Additionally, the restrictions created by this proposed modification infringe on businesses' First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that "people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . ."[10] Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is "neither misleading nor related to unlawful activity" unless it has a substantial interest in restricting this speech, the regulation directly advances that interest, and the regulation is narrowly tailored to serve that interest.[11] The proposed regulation fails each part of the test:

- ***No substantial interest:*** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.

[10] *Virginia Pharmacy Board v. Virginia Citizens Consumer Council,* 425 U. S. 748, 770 (1976).
[11] *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York,* 447 U.S. 557, 564 (1980); *see also Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

- ***No advancement of the interest:*** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A "regulation may not be sustained if it provides only ineffective or remote support for the government's purpose."[12] This proposed regulation is both ineffective and provides no support for the government's purpose.

- ***Not narrowly tailored:*** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. "[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive."[13] As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. "As in other contexts, these standards ensure not only that the state's interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message." [14] The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The OAG should revise the text of the proposed modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.[15] Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,[16] those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable (and, in fact, could incentivize) some agents to give consumers misleading

[12] *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).
[13] *Id.*
[14] *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).
[15] Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).
[16] *Id*. at § 999.315(h)(3).

or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.[17] The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer.

The proposed modifications would require businesses that collect personal information when interacting with consumers offline to "provide notice by an offline method that facilitates consumers' awareness of their right to opt-out."[18] The proposed modifications proceed to offer the following "illustrative examples" of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.[19] While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer's interaction with the business.

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, "[w]hen a business collects… personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online."[20] The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in

[17] Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).
[18] Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Oct. 12, 2020).
[19] *Id*.
[20] Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).

over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications' illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer's ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications' addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, and inflexible. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

* * *

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at masignorelli@venable.com with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

December 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Fourth Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the fourth set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.[1]

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising expenditures. Locally, our members are estimated to help generate some $767.7 billion dollars for the California economy and support more than 2 million jobs in the state.[2]

For more than a year, our members have been communicating with consumers about their CCPA rights and how to effectuate them. As a result, our members have experience in operating under the CCPA and interacting with consumers. We have learned valuable insights about how to support consumer privacy rights under this new legal regime, including that operational flexibility is vital.

Not all interactions with consumers are the same nor are all business operations. There is no "one-size fits all" approach to the CCPA. We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in this letter, the draft regulations implementing the CCPA should be updated to provide greater clarity, better enable consumers to exercise informed choices, and help businesses in their efforts to continue to provide value to Californians and support the state's economy.[3]

---

[1] *See* California Department of Justice, *Notice of Fourth Set of Proposed Modifications to Text of Regulations and Addition of Documents and Information to Rulemaking File* (Dec. 10, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-4th-set-mods.pdf.

[2] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana.net/getfile/23045.

[3] Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. *See Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf at CCPA_15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California Consumer Privacy Act*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf at CCPA_2ND15DAY_00309 - 00313; *Third Set of Proposed Regulations Implementing the California Consumer*

Companies and consumers have been adapting to the "Do Not Sell My Personal Information" tagline for more than a year. This effort has included refashioning digital properties, as well as instituting backend processes to meet the compliance requirements of the CCPA even as a new ballot initiative, the California Privacy Rights Act (or "Proposition 24"), was moving forward. These most recent proposed modifications by the OAG to the CCPA regulations set forth ambiguous terms surrounding a proposed online button almost a full year after the law went into effect. Among other things, this round of modifications fails to clarify whether the button is optional or mandatory. The proposed changes also do not leave room for the deployment of alternative icons, such as the CCPA Privacy Rights Icon in market provided by the Digital Advertising Alliance ("DAA"),[4] or other methods, such as a text only link in applicable scenarios, to facilitate consumers' right to opt out of personal information sales. The OAG should reconsider these provisions, or at the very least clarify them so businesses can take steps to comply with the new terms as soon as possible.

Additionally, changes the OAG made during the third set of proposed modifications to the CCPA regulations set forth a prescriptive interpretation of the law that could limit businesses' ability to support employment in California and the state's economy during these unprecedented times. We reassert the issues we previously raised with those provisions in this submission. As explained in more detail in the sections that follow below, the OAG's potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses' right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG's proposed edits to Section 999.306 regarding offline notice of the right to opt out could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify these changes per the below comments.

Our members are committed to offering consumers robust privacy protections while simultaneously providing them with access to ad-funded news, apps, and a host of additional online services. These are offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content and services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as protect the economy.

I. The Regulations Should Clarify That the Proposed New Button is Discretionary and Not Preclude Use of Other Icons Presented in Conjunction with the Text Link

In the fourth set of proposed modifications to the CCPA regulations, the OAG reinserted terms setting forth a specific graphic for a button enabling consumers to opt out of personal information sales. The proposed modifications state that the proposed button "*may* be used" in addition to posting a notice of the right to opt-out online, but not in lieu of such notice or the "Do Not Sell My Personal Information" link.[5] In the very next subsection, the proposed rules state that when a business provides a "Do Not Sell My Personal Information" link, the proposed button "*shall* be added to the left" of the link.[6] The language describing the proposed button is thus unclear, as it does not adequately explain whether providing the

---

Privacy Act, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf at CCPA_3RD15DAY_00111 - 00118.

[4] DAA, *Opt Out Tools*, located at https://www.privacyrights.info/.

[5] Cal. Code Regs. tit. 11, § 999.306(f)(1) (proposed Dec. 10, 2020) (emphasis added).

[6] *Id*. at § 999.306(f)(2) (emphasis added).

button is discretionary or mandatory for businesses that sell personal information. We ask the OAG to confirm that the proposed button is discretionary as well as to provide flexibility for businesses to use alternative, industry-developed icons that signal the right to opt out of personal information sales to California consumers.

As the founding members of the DAA YourAdChoices program and corresponding icon,[7] we understand the benefits a widely recognizable icon can bring to provide transparency and choices to consumers. In fact, in November 2019, the DAA announced its creation of a tool and corresponding Privacy Rights Icon to provide consumers with a clear and recognizable mechanism to opt out of personal information sales under the CCPA.[8] Icons and corresponding privacy programs created by the DAA have a history of success. The YourAdChoices icon has been served globally at a rate of more than one trillion times per month, and its recognition continues to grow. In a 2016 survey, more than three in five respondents (61 percent) recognized the YourAdChoices icon at least a little, and half (50 percent) said they recognized it a lot or somewhat. For the CCPA, there is a need for flexibility in how this novel law is implemented in the market. The OAG should allow the marketplace to determine the best opt-out button approach, including allowing the option for use of an icon promulgated in relation to industry-driven opt-out mechanisms, rather than creating uncertainty by mandating a new graphic that businesses must use.

Moreover, adding the button as a requirement now, nearly a year after the CCPA became effective and more than five months after the OAG began enforcing the law, would create unnecessary new compliance costs for businesses to reconfigure websites and consumer-facing properties after they have already taken significant steps to update their practices per the CCPA's requirements. We therefore ask the OAG to clarify that the new opt-out button is discretionary rather than mandatory, and businesses that provide a "Do Not Sell My Personal Information" link are not required to also provide the proposed button. We also ask the OAG to provide flexibility for businesses to utilize other icons to signal a consumer's right to opt out of personal information sales, such as the DAA's CCPA Privacy Rights Icon. The OAG should reconsider the need to create new iconography and should instead partner with industry on the already existing DAA Privacy Rights Icon to help lead consumers to choices about how their personal information is used and shared.

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."[9] This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported

[7] Digital Advertising Alliance, *YourAdChoices*, located at https://youradchoices.com/.
[8] DAA, *Digital Advertising Alliance Announces CCPA Tools for Ad Industry* (Nov. 25, 2019), located at https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-ccpa-tools-ad-industry.
[9] Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

Internet would be unduly hindered, thereby undermining a consumer's ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising.[10] However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business' provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer "to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request" the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses' ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt-out choice while facilitating the consumer's request to opt out.

Additionally, the restrictions created by this proposed modification infringe on businesses' First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that "people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . ."[11] Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is "neither misleading nor related to unlawful activity" unless it has a substantial interest in restricting this speech, the regulation directly advances that interest,

[10] DAA, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located at https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance.
[11] *Virginia Pharmacy Board v. Virginia Citizens Consumer Council,* 425 U. S. 748, 770 (1976).

and the regulation is narrowly tailored to serve that interest.[12] The proposed regulation fails each part of the test:

- ***No substantial interest:*** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.

- ***No advancement of the interest:*** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A "regulation may not be sustained if it provides only ineffective or remote support for the government's purpose."[13] This proposed regulation is both ineffective and provides no support for the government's purpose.

- ***Not narrowly tailored:*** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. "[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive."[14] As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. "As in other contexts, these standards ensure not only that the state's interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message."[15] The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The U.S. Supreme Court has made clear that the burden is on the government to justify content-based restrictions on lawful speech, and the failure to even state a basis for this restriction fails to meet this requirement.[16] The OAG should revise the text of the proposed

---

[12] *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980); *see also Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).
[13] *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).
[14] *Id.*
[15] *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).
[16] *E.g., Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (citing *Arizona Free Enter. Club's Freedom Club PAC v. Bennett*, 564 U.S. 721 (2011)).

modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.[17] Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,[18] those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable some agents to give consumers misleading or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.[19] The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer. This sort of operational flexibility is necessary for businesses to convey important notices in context.

The proposed modifications would require businesses that sell personal information to "inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request" when interacting with consumers offline.[20] The proposed modifications proceed to offer the following "illustrative examples" of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a

[17] Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).
[18] *Id*. at § 999.315(h)(3).
[19] Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).
[20] Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Dec. 10, 2020).

brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.[21] While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer's interaction with the business.

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, "[w]hen a business collects… personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online."[22] The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications' illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer's ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications' addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, inflexible, and likely highly costly for many businesses. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores

[21] *Id.*
[22] Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

* * *

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at masignorelli@venable.com with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

July 28, 2021

California Office of the Attorney General
Attorney General Rob Bonta
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Response to CCPA FAQ Regarding User-Enabled Controls and Related Enforcement Letters

Dear Attorney General Bonta:

The undersigned trade associations and organizations collectively represent a broad cross-section of the Californian and United States business community spanning various industries including advertising and marketing, analytics, magazine publishing, Internet and online services, financial services, package delivery, cable and telecommunications, transportation, retail, real estate, insurance, entertainment, auto, and others. Our organizations have a long history of supporting consumers' ability to exercise choice over uses of data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use, user-enabled choice mechanisms is a foundational aspect of data privacy that we have championed for decades. However, we are concerned that the OAG's new FAQ response regarding user-enabled global privacy controls will cause confusion for consumers and businesses, rather than effectuating genuine user choices.

In particular, we maintain the following three concerns. First, the FAQ mandate directly conflicts with the approach taken in the California Privacy Rights Act of 2020 ("CPRA"), which becomes operative in less than 18 months. Second, there was no public process for evaluating or

considering the cited tools or the particular implementations by the browser referenced in the FAQ, and as a result there are diverging perspectives around what constitutes a tool that is "user enabled." Finally, the existence of the FAQ unnecessarily prejudices a subject matter on which the California Privacy Protection Agency ("CPPA") is directed by law to promulgate rules. These concerns are compounded by the recent publicly-reported enforcement letters sent by the OAG to companies on adherence to such signals.[1] We therefore ask you to retract this FAQ response, reconsider your enforcement approach to user-enabled global privacy controls, and defer to California's new privacy agency on the subject.

- **The FAQ response conflicts with the approach taken in the CPRA. This will lead to confusion for consumers and businesses.** Not only does the California Consumer Privacy Act of 2018 ("CCPA") not direct the Attorney General to create and mandate adherence to the controls described in Section 999.315(c) of the regulations implementing the law,[2] but the FAQ response stands in direct contrast to the approach to such controls taken in the CPRA. According to the CPRA, businesses "may elect" to either (a) "[p]rovide a clear and conspicuous link on the business's internet homepage(s) titled 'Do Not Sell or Share My Personal Information'" **or** (b) allow consumers to "opt-out of the sale or sharing of their personal information… through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]"[3] Despite this choice that will become available to businesses in a short time, the FAQ response and decision to send enforcement letters to businesses regarding user-enabled privacy controls that do not align with the CPRA is unnecessary and creates confusion in the market. The OAG consequently takes a position on such controls that does not reflect California law and is likely to be different from the approach spelled out by new regulations implementing the CPRA. This will result in confusion for consumers and businesses.

- **The FAQ statement directly conflicts with the CPRA mandate explicitly directing California's new privacy agency to issue specific rules governing user-enabled global privacy controls.** The CPRA tasks the CPPA to issue particularized regulations governing user-enabled global privacy controls to help ensure consumers and businesses are protected from intermediary interference. Given the lack of formal process employed with respect to the OAG's proposed application of global privacy controls and the FAQ response, it does not appear that these safeguards have been considered and addressed. For example, the CPRA instructs the CPPA to "ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal *cannot unfairly disadvantage another business*."[4] According to the CPRA, the CPPA must also ensure user-enabled global privacy controls "*clearly*

[1] *See State of California Department of Justice, Rob Bonta Attorney General*, California Consumer Privacy Act (CCPA) FAQ Section B, #7 and #8, available at https://oag.ca.gov/privacy/ccpa; *see also* Kate Kaye, *California's attorney general backs call for Global Privacy Control adoption with fresh enforcement letters to companies*, DIGIDAY (Jul. 16, 2021), available at https://digiday.com/marketing/californias-attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/.

[2] Cal. Code Regs. tit. 11, § 999.315(c); *see also* Joint Ad Trades Comments on the Second Set of Proposed Regulations Implementing the CCPA at CCPA_2ND15DAY_00310 - 00313, available here (noting California Administrative Procedural Act and constitutional concerns with Section 999.315(c) of the regulations implementing the CCPA) .

[3] CPRA, Cal. Civ. Code § 1798.135(b)(3).

[4] CPRA, Cal. Civ. Code § 1798.185(a)(19)(A) (emphasis added).

represent a consumer's intent and [are] free of defaults constraining or presupposing such intent."[5]

In contrast, the OAG's FAQ response does not ensure that any of the safeguards set forth in the CPRA's regulatory instructions are followed. For instance, the OAG's FAQ response lists a browser that sends opt-out signals by default without consulting the consumer, and such signals are unconfigurable.[6] The OAG's FAQ response therefore does not provide any means to enable businesses to determine whether a global privacy control signal, as implemented by particular browsers, is truly user-enabled, or if it is instead sent or communicated by an intermediary in the ecosystem without the consumer's consent. Moreover, the FAQ response contravenes the will of Californians, as expressed in passing the CPRA ballot initiative, that privacy regulation on the subject of user-enabled global privacy controls should come from the CPPA as opposed to the OAG.

- **New OAG guidance regarding user-enabled global privacy controls should be developed through a deliberative process that considers stakeholder input.** The OAG's FAQ response was posted to its website without any sort of formal deliberation or process prior to publication. Legal and material guidance such as those contained in the FAQ should only be issued after a carefully deliberated formal process that allows for public input. New rules or guidance regarding user-enabled global privacy controls should be afforded the benefit of a formal process, including public comment and thoughtful evaluation.

  Such process should also indicate how the OAG and/or CPPA will (i) ensure such controls are compliant with the CPRA, (ii) monitor control providers to ensure their compliance with law and the standards set forth in the CPRA, and (iii) set forth a system to ensure that modifications by browsers and other intermediaries remain compliant with law to avoid circumstances where changes "unfairly disadvantage another business" or no longer "clearly represent a consumer's intent and [are] free of defaults constraining or presupposing such intent." Issuing a rule on such controls without providing a deliberative process risks creating significant confusion and unworkable policy for consumers and businesses alike.

* * *

The undersigned trade associations and organizations fully support empowering consumer choice and advancing workable privacy protections for Californians. However, the position reflected in the OAG's recent FAQ response and enforcement letters was issued without formal process and contradicts the approach to user-enabled global privacy controls taken in the CPRA. We therefore respectfully ask you to reconsider the FAQ response, as well as your enforcement

[5] *Id.*

[6] *See* Brave, *Global Privacy Control, a new Privacy Standard Proposal, now Available in Brave's Desktop and Android Testing Versions*, available at https://brave.com/global-privacy-control/ ("Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.")

approach concerning user-enabled global privacy controls, and to instead defer to the CPPA on the issue. Please contact Mike Signorelli of Venable LLP at masignorelli@venable.com with questions on this letter.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

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

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Howard Fienberg
Senior VP, Advocacy
Insights Association
202-800-2545

Shoeb Mohammed
Policy Advocate
California Chamber of Commerce
916-879-7904

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

Cameron Demetre
Executive Director, CA & the Southwest
TechNet
916-903-8070

Anton van Seventer
State Privacy & Security Coalition
202-799-4642

CC: California Privacy Protection Agency

EXHIBIT B

PRINCIPLES FOR USER-ENABLED CHOICE SETTING MECHANISM

A Choice Setting should meet the following criteria:

1. **Accessing the Setting.** A Choice Setting shall be activated in the settings panel of a browser and/or device, which is accessible from a menu. Additional prompts or other means of accessing a Choice Setting may be offered in addition to the setting panel, but such additional prompts or means should not unfairly disadvantage an entity.

2. **Describe Setting & Effect.** A Choice Setting shall communicate the following:

    a. **Effect of Choice.** The effect of exercising such choice including that a Choice Setting signal is limited to communicating a preference to opt out from the sale of personal information, specific types of advertising, and/or any other legal right provided by law; and the fact that some data may still be collected and used for purposes not subject to the rights provided by law following the sending of a choice signal;

    b. **Scope of Opt Out.** Choice made via the Choice Setting applies to the browser or device from which such choice is made, or for the consumer, if known to the entity receiving the signal and required by law; and

    c. **Affirmative Direction to Sell.** The fact that if a consumer affirmatively allows a particular entity to collect, sell, or use personal information about interactions, viewing and/or activity from Web sites, devices, and/or applications, the activation of the Choice Setting will not limit that collection, sale, or use from such entity.

3. **Affirmative Step.** The consumer shall affirmatively consent to turn on or activate the Choice Setting via the settings panel of a browser and/or device. Such ChoiceSetting may not be preselected, turned on, or activated by default.

4. **Option to Withdraw Choice.** A Choice Setting shall provide a means for a consumer to turn off, deactivate, or revoke consent for the Choice Setting through the same means the consumer previously made the affirmative choice to turn on or activate the Choice Setting.

5. **Jurisdictional Signal.** The Choice Setting should indicate the jurisdiction(s) from which choice is made in a manner that the entity receiving the signal may determine the applicable legal requirement(s).

* * *