From: Christopher Oswald [redacted]
Sent: 11/8/2021 11:38:47 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Ad Trade Response to CPPA Invitation for Preliminary Comments on Proposed CPRA Rulemaking
Attachments: FINAL Joint Ad Trade Comments - CPRA Preliminary Rulemaking Request for Comment.pdf

[EXTERNAL]: [redacted]

To: regulations@cppa.ca.gov

Subject: PRO 01-21 Ad Trade Response to CPPA Invitation for Preliminary Comments on Proposed CPRA Rulemaking

To Whom It May Concern:

Please find attached comments from the following advertising trade associations in response to the California Privacy Protection Agency's request for preliminary comments on proposed rulemaking under the California Privacy Rights Act: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the Network Advertising Initiative, the American Advertising Federation, and the Digital Advertising Alliance. We appreciate your consideration of these comments.

If you have any questions about these comments, please feel free contact me.

Regards,
Christopher Oswald
Senior Vice President, Government Relations
ANA – Association of National Advertisers
[redacted] | ana.net | @ANAGovRel
2020 K Street, NW, Suite 660, Washington, DC 20006

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
[redacted]

Dave Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[redacted]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[redacted]

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

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[redacted]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[redacted]

CC: Mike Signorelli, Venable LLP