June 23, 2020

Honorable Gavin Newsom
Governor, State of California
State Capitol
Sacramento, CA 95814

Dear Governor Newsom:

The Association of National Advertisers ("ANA") writes to express a significant concern about the California Office of the Attorney General's ("CA AG") process of drafting regulations to implement the California Consumer Privacy Act of 2018 ("CCPA") as well as the CA AG's authority to promulgate those regulations. While we fully support the goal of creating strong and meaningful privacy protections for Californians, certain provisions in the implementing rules could hinder consumer privacy and choice rather than advance it. ANA is the advertising industry's oldest and largest trade association. ANA's membership includes nearly 2,000 companies, marketing solutions providers, charities and nonprofits, with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than $400 billion in marketing and advertising annually. Nearly every advertisement you'll see in print, online, or on TV is connected in some way to ANA members' activities.

As we explained in our comments to the CA AG on the content of the CCPA regulations,[1] the final rules fail to provide businesses with needed clarity and time to comply, and they contain unconstitutional requirements that exceed the CA AG's authority and could frustrate consumers. Although the CCPA will become enforceable on July 1, 2020, the state government has not yet finalized the regulations that will implement this landmark law. Even as your office extended state regulatory deadlines in recognition of the impact of the COVID-19 pandemic, the CA AG has indicated it will commence CCPA enforcement in July without any delay to account for the present lack of final rules and the significant disruption to business operations caused by COVID-19. Consumers, businesses, and the public health would benefit from a reasonable forbearance of enforcement during this pandemic.

In addition, instead of instituting a blanket requirement for businesses to honor browser signals and other intermediary controls, a proposal that goes beyond the law's intent and scope, the law should provide that businesses may honor these browser controls or offer consumers another, equally effective method of opting out of personal information sale. This clarification would avoid the constitutional concerns inherent in the requirement and would better enable businesses to abide by consumers' expressed choices. As it stands, the requirement impinges on constitutionally protected speech under the First Amendment to the United States Constitution and Article I, Section 2(a) to the California Constitution by impermissibly burdening businesses' commercial speech. Further, the requirement contravenes the separation of powers doctrine, as the CA AG exceeded its authority to regulate under the CCPA statute itself. Updating the regulatory requirement so businesses may permissibly offer consumers another, equally effective method of opting out of personal information sales instead of obeying browser signals would help prevent intermediaries from setting default signals that do not align with consumer preferences. An excerpt of our comments explaining the challenges surrounding the timing of the CCPA enforcement date, as well as raising legal and procedural issues about the regulations' loyalty programs

[1] *ANA Comments on the Second Set of Modifications to the Proposed CCPA Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set2.pdf, CCPA_2ND15DAY_00003 – 00019.

terms, browser mandate, and application to internally-generated business inferences, is attached hereto as **Exhibit A**.

Our members through advertising underwrite the vast majority of free or subsidized content that Californians and all consumers access and read online. They are well-intentioned and eager to receive final CCPA implementation guidance from the state government. However, we are concerned that they will not have enough time to implement the CCPA rules once they do become final. Moreover, the regulations as currently drafted are unclear and extend beyond the CA AG authority to regulate pursuant to the law. We therefore ask you to take action to ensure that businesses have the opportunity to operationalize constitutional and procedurally sound CCPA regulations before they can be subject to enforcement actions for allegedly violating the law's terms.

* * *

Thank you for your attention to this important matter. We urge you to take any action in your power to remedy the constitutional and procedural defects inherent in the CCPA regulations, as well as provide needed time for businesses to implement the final rules before enforcement begins.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

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

California Office of Administrative Law
300 Capitol Mall, Suite 1250
Sacramento, CA 95814

Anthony Williams, Cabinet Secretary

Melissa Immel, Deputy Legislative Secretary

EXHIBIT A

I. Delay Enforcement Until January 2, 2021

With less than four months before CCPA enforcement is scheduled to begin, the regulations implementing the law have not yet been finalized. In the face of this uncertainty, businesses have been forced to implement brand new processes for the CCPA based on incomplete regulatory requirements, and these processes must change with each update to the draft rules. Current events have also placed significant strain on businesses in their earnest efforts to comply with the CCPA and its regulations. The recent outbreak of COVID-19 has brought normal business operations and typical consumer interactions to a halt, as California's governor has instituted a mandatory stay-at-home order, which has paused or dramatically altered day-to-day activities. The health crisis, coupled with the unfinished nature of the draft CCPA rules, has significantly impacted businesses' ability to create processes and procedures to keep up with the continuously evolving proposed regulations. We therefore ask you to forbear from enforcing the CCPA until January 2, 2021.

COVID-19 has substantially encumbered businesses' ability to operationalize the draft rules implementing the CCPA prior to July 1, 2020. The World Health Organization has proclaimed the virus to be a global pandemic.[2] President Trump has also declared a national state of emergency due to its rapid spread and its potentially deadly effects,[3] and declared California a "major disaster."[4] Governor Gavin Newsom has declared a state-wide order for Californians to shelter in place, ordering them to "stay in their homes unless they are accessing essential services, such as pharmacies, grocery stores and banks."[5] The disruption to daily life and business operations presented by the virus cannot be overstated.

On March 20, 2020, in the midst of the spreading COVID-19 pandemic, over sixty-five trade associations, organizations, and companies sent your office a letter asking you to delay the effective date of the rules as well as enforcement until January 2, 2021.[6] We renew that request in these comments, as our members employ millions of individuals who are faced with this unprecedented health emergency. Employees who are responsible for CCPA compliance are being forced to divert resources to provide timely responses to consumer requests given the current state of affairs. The law gives businesses forty-five days to respond, but many of the same employees responsible for responding to requests are now working remotely or not at all or are seeking to support workforces working remotely. Moreover, for many businesses, available resources have been diverted to efforts to respond to COVID-19. Entities are in talks with the U.S. government about substantially realigning their daily operations to produce necessary medical equipment and supplies to aid the fight against the virus.[7] Given the unparalleled

---

[2] World Health Organization, *WHO characterizes COVID-19 as a pandemic* (Mar. 11, 2020), located at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

[3] White House, *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak* (Mar. 13, 2020) located at https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/.

[4] Office of Governor Gavin Newsom, *California Secures Presidential Major Disaster Declaration to Support State's COVID-19 Emergency Response* (Mar. 22, 2020), located at https://www.gov.ca.gov/2020/03/22/california-secures-presidential-major-disaster-declaration-to-support-states-covid-19-emergency-response/.

[5] *Californians ordered to shelter in place*, CALMATTERS (Mar. 20, 2020), https://calmatters.org/newsletter/california-coronavirus-homeless/.

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

[7] David Shepardson, *GM, Ford in talks with Trump administration on medical equipment production*, REUTERS (Mar. 18, 2020), located at https://www.reuters.com/article/us-health-coronavirus-gm-equipment/gm-ford-in-talks-with-trump-administration-on-medical-equipment-production-idUSKBN2153W5; Jeffery Martin, *Trump Signs Emergency Bill to Make Companies Manufacture Medical Supplies to Fight Coronavirus*, NEWSWEEK (Mar. 18,

present situation and the unique realities facing consumers and businesses alike, we urge your office to delay enforcement so businesses can allocate crucial funds, labor, and time to supporting their employees as well as California's and the national response to COVID-19.

Additionally, conduct undertaken now during the emergency should not be the subject of CCPA enforcement actions. Businesses are understandably focused on ensuring the health and safety of their workers and maintaining economic viability in the face of immense challenges. Businesses should not be penalized under the CCPA for current conduct or activities when their attention is rightfully focused on the dire and important matter of managing the novel coronavirus. Relevant authorities in other jurisdictions, such as the United Kingdom Information Commissioner's Office ("UK ICO"), have suspended data protection regulatory actions during the outbreak.[8] The California Attorney General should follow the UK ICO's approach by refraining from using activities undertaken during this exceedingly difficult present period as a hook for enforcement actions.

Developing needed processes to comply with the CCPA necessarily has taken a backseat to the urgent and pressing health crisis. Business efforts to build CCPA compliance mechanisms based on the most up-to-date draft rules have been delayed. Threatening businesses with the prospect of extremely burdensome and resource-intensive litigation in the present catastrophic economic and health emergency will cause increased stress in an already precarious state of affairs. Many businesses who employ millions of Californians are simply trying to keep their doors open without going under during these dire times.[9] Small businesses and startup entities will be particularly impacted by the economic impacts of the health crisis.[10] A forbearance in enforcement would provide much needed time for businesses to continue to bring their operations into compliance with the regulations once the health emergency is under control.

Although companies have already taken steps to facilitate compliance, the lack of finalized regulations has left our members and thousands of other California businesses uncertain concerning their ultimate obligations. On March 11, 2020, your office released a third iteration of the draft rules, thereby

---

2020), located at https://www.newsweek.com/trump-signs-emergency-bill-make-companies-manufacture-medical-supplies-fight-coronavirus-1493142; Jeremy B. White, *Newsom says California enlisting Elon Musk, Tim Cook for coronavirus help,* POLITICO (Mar. 21, 2020), located at https://www.politico.com/states/california/story/2020/03/21/newsom-says-california-enlisting-elon-musk-tim-cook-for-coronavirus-help-1268647; Arjun Kharpal, *US tech CEOs from Tim Cook to Elon Musk pledge to help coronavirus fight with masks and ventilators,* CNBC (Mar. 23, 2020), located at https://www.cnbc.com/2020/03/23/coronavirus-apple-ceo-tim-cook-teslas-elon-musk-pledge-donations.html.

[8] UK ICO, *Data protection and coronavirus: what you need to know*, located at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/covid-19-general-data-protection-advice-for-data-controllers/. In response to a question asking if the regulator would take action against companies for conduct during the pandemic, the UK ICO wrote: "No. We understand that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work. We won't penalise organisations that we know need to prioritise other areas or adapt their usual approach during this extraordinary period."

[9] Roland Li, *Coronavirus closes many Bay Area hotels: 'Worse than 9/11 or 2008'*, SAN FRANCISCO CHRONICLE (Mar. 19, 2020), located at https://www.sfchronicle.com/business/article/Coronavirus-puts-San-Francisco-s-hotels-in-15141953.php?cmpid=gsa-sfgate-result; Ali Wunderman, *How to keep restaurants afloat amidst the coronavirus lockdown*, SFGATE (Mar. 21, 2020), located at https://www.sfgate.com/food/article/restaurants-bars-help-coronavirus-gift-cards-merch-15138978.php.

[10] The economic impact study the CA AG completed on the impacts of the CCPA regulations indicate that small businesses will incur $50,000 in compliance costs in getting ready for the CCPA. In the best of times that would be crippling to cash strapped small business. Given today's realities, it is a death sentence for small businesses owners and its employees. *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 10 (August 2019), located at http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/CCPA_Regulations-SRIA-DOF.pdf (hereinafter "*SRIA*").

updating the regulatory scheme with new nuances that now need to be built into already-existing compliance strategies.[11] Continuing to change the regulations so close to the law's enforcement date of July 1, 2020 will make it difficult if not impossible for businesses to conform their new procedures to the final rules by July 1, 2020. Furthermore, the rules will not be final until they are approved the California Office of Administrative Law, which adds to the increasingly likely possibility that the draft rules will become effective only a short time before your office could commence enforcement.

The CCPA is a first-of-its-kind, complex statute that has imposed entirely new requirements on businesses and has caused them to incur significant costs. The CCPA suggests that the CA AG may begin enforcing the law on July 1, 2020, but your office has discretion to provide a reasonable period of additional time for businesses to understand and implement the final rules before you start bringing enforcement actions. We therefore respectfully ask you to postpone your enforcement efforts until January 2, 2021. This limited deferral will give businesses the time they need to understand and effectively implement the final rules and will help lessen the blow to the economy caused by the coronavirus outbreak.

II. Clarify Financial Incentive Terms to Enable the Continued Existence of Loyalty Programs

Guidance provided on financial incentive terms remains unclear.[12] According to the draft rules, businesses that offer "financial incentives" or "price or service differences" related to the collection, retention, or sale of personal information must ensure that such incentives and differences are "reasonably related to the value of the consumer's data."[13] Additionally, businesses must disclose "a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference" and "a description of the method used" to calculate such value.[14] As articulated in the proposed modified regulations, businesses that do not adequately comply with these requirements may not offer financial incentives or price or service differences to consumers.[15] The unclear nature of these burdensome rules coupled with significant confusion regarding how businesses must operationalize them could force many entities to stop offering loyalty and rewards programs to California consumers altogether. We therefore ask the CA AG to clarify or remove the draft rules' ambiguous financial incentive and price or service difference terms to ensure Californians may continue to receive the benefits of the loyalty and rewards programs they enjoy, value, and expect.

Brands and marketers offer various loyalty and rewards programs to California consumers, such as clothing VIP points programs, tiered ride-sharing programs, grocery rewards, credit card cash back benefits, and myriad others. Consumers have long enjoyed participating in these programs because they receive offers and better deals for the products and services that are most relevant and important to them. Businesses also have benefited from the loyalty, brand trust, and word-of-mouth marketing they accumulate through consumers' participation in these programs. The draft rules could impede or completely eradicate the existence of loyalty and rewards programs in California due to their requirements to tie the "value of the consumer's data" to the financial incentive or price or service difference offered to consumers. It is consequently extremely important for the CA AG to clarify the

[11] 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?.
[12] Cal. Code Regs. tit. 11, §§ 999.336, 337 (proposed Mar. 11, 2020).
[13] *Id*. at §§ 999.301(j), (o); 336(b).
[14] *Id*. at § 999.307(b)(5).
[15] *Id*. at § 999.336(b).

draft rules' uncertain financial incentive and price or service difference terms so Californians can have the same access to loyalty programs as consumers residing in other states.

The proposed rules offer nearly no information about how a business may show that a price or service difference offered through a loyalty or rewards program is "reasonably related to the value of a consumer's data." Notably, there is no reference in the draft rules to how a business can account for the value it receives in fostering goodwill and consumer loyalty for a brand. This intangible value is difficult if not impossible to quantify, so, showing a direct relationship between a financial incentive and this value in numerical terms might be an unachievable task. Moreover, the value a business attributes to personal information associated with a consumer might vary from situation to situation. Such value might depend, for example, on the particular discount offered at a specific time or in a specific place.

Adding to the confusion is the fact that businesses might offer several different financial incentives or price or service differences to consumers through loyalty and rewards programs at one time. For example, a grocery store might offer consumers discounts through a loyalty card when the consumer signs up for the card with the store. By signing up for the program, consumers might receive discounts on select food items and beverages when they shop. Simultaneously, the very same grocery store might offer consumers a loyalty program that takes the form of a sweepstakes, providing consumers with necessary pieces to complete the game as they make continuous purchases at the store. It is unclear how the grocery store could show that both the loyalty card and the game are "reasonably related to the value of the consumer's data," especially if "the value of the consumer's data" is to remain a constant number. The draft rules are unclear on this point, and they could consequently cause businesses to stop offering loyalty programs in California due to confusion in regard to how to follow the proposed regulations' mandates. Given the vagueness of the terms and requirements, we do not see how the CA AG could enforce these requirements consistent with constitutional requirements of fair notice and due process.

The revised proposed rules also require businesses to provide a "notice of financial incentive" for each incentive or price or service difference offered that discloses an estimate of "the value of the consumer's data" and the method of calculating that value.[16] Requiring a business to make such disclosures could reveal business trade secrets and proprietary information that could jeopardize the business's competitive position in the marketplace. Forcing businesses to reveal their confidential, internal valuations and methods of calculating such value in this way could detrimentally impact competition and risk the exposure of protected business proprietary information. Revealing such data would also provide little to no value to consumers, as the required disclosures would be meaningless from a consumer's point of view. Moreover, consumers would be overwhelmed and inundated with an excessive number of financial incentive notices, as businesses typically offer several incentives to consumers at one time. Consumers would therefore likely not digest or understand meaningful information about business practices by receiving such notices. Finally, compelling the surrender of legally protected, highly proprietary information could raise numerous constitutional problems, ranging from a regulatory taking to dormant Commerce Clause issues given the negative impact on interstate commerce.

For the foregoing reasons, we urge the CA AG to clarify or remove the unreasonably onerous price or service difference and financial incentive terms in the proposed rules. In particular, we ask the CA AG to remove or clarify the provisions requiring businesses to disclose an estimate of "the value of consumer data," the method of calculating such value, and ensure that financial incentives offered through loyalty and rewards programs are reasonably related to "the value of the consumer's data." We also request that clarification be given to ensure that businesses are not required to disclose internal data, calculations, and inferences. Without such clarification and corrections, these requirements are

[16] *Id*. at § 999.307(b)(5).

exceptionally onerous if not impossible for businesses to implement and could result in the end of loyalty programs in California.

III. Allow Businesses to Choose to Honor Global Privacy Controls *or* Offer Another, Equally Effective Method for Consumers to Opt Out of Personal Information Sale

According to the draft rules, a business that collects personal information from consumers online must "treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information" as a valid request to opt out of sales.[17] This requirement raises constitutional concerns, as it is wholly divorced from the text of the CCPA itself, is an arbitrary and capricious exercise of the CA AG's authority to issue regulations according to law, and impinges on constitutionally protected speech under the First Amendment to the United States Constitution and Article I, Section 2(a) to the California Constitution. The requirement will also impede consumer choice and the digital economy by casting a single, default opt-out signal to all entities in the online marketplace instead of enabling consumers to make individualized, business by business selections about which entities may and may not sell personal information as the law requires. The requirement consequently violates both constitutional rights as well as consumers' rights to exercise robust and specific choices in the marketplace.

Instead of instituting a blanket requirement for businesses to honor browser signals and privacy controls, we ask the CA AG to clarify that businesses *may* honor global privacy controls *or* offer consumers another, equally effective method of opting out of personal information sale. This clarification would avoid the constitutional concerns inherent in the requirement and would better enable businesses to abide by consumers' expressed choices. It would also prevent intermediaries from setting default signals that do not align with consumer preferences.

A. The Draft Rules' Browser Mandate Exceeds the CA AG's Authority and Raises Serious Constitutional Concerns

The draft rules have instituted an entirely new requirement for businesses to honor browser signals and global privacy controls that is nowhere present in the text of the CCPA. This requirement is arbitrary and capricious, exceeds the scope of the CCPA, falls outside of the CA AG's authority to issue regulations as set forth in Section 1798.185 of the law, and impedes free speech as protected by the First Amendment to the United States Constitution and Article I, Section 2(a) to the California Constitution.[18] Businesses have had no meaningful opportunity to anticipate or prepare for this brand-new obligation, and it represents a broadly applicable rule that does not advance the state's interest in protecting consumer privacy. We therefore request that this requirement be removed from the regulations or that your office alternatively adopt a less restrictive means to effectuating consumer choice.

1. The Browser Mandate Contradicts the Text of the CCPA and Therefore Exceeds the CA AG's Authority

In passing the CCPA, the California Legislature purposefully did not include a mandate to respect default signals set by browsers that send a single opt-out signal to the entire Internet ecosystem. The CA

[17] *Id*. at § 999.315(d).

[18] As Professor Grodin has commented, "California may have broader protection for commercial speech than the First Amendment provides, at least as to compelled speech." Joseph R. Grodin, *Freedom of Expression under the California Constitution*, 6 *California Legal History* 214 (2011), available at http://repository.uchastings.edu/faculty_scholarship/1067.

AG's proposed regulation requiring businesses to respect global privacy controls set through browsers effectively turns the CCPA's opt-out regime into an opt-in regime. The present text of the draft rules empowers browsers and other intermediaries to set such signals by default, allowing for opt-out signals to be sent to businesses even if they do not align with consumers' actual preferences or desires. Upon the receipt of such a default global opt-out signal through a browser, businesses will be forced to contact consumers directly to ascertain whether such consumers would like to opt-in to sales of personal information. This structure thwarts legislative intent by converting the opt-out right in the CCPA into an opt-in system.

The Legislature specifically created a right for consumers to opt out of personal information sales, enabling consumers to submit granular choices directly to businesses rather than requiring a single online signal to trump all other signals set in the marketplace.[19] It was not the goal of the Legislature to force consumers to opt in to every business's sale of personal information associated with them. 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.[20] More than five years ago, when it amended the California Online Privacy Protection Act, the California Legislature considered global privacy controls and elected to refrain from enshrining them into law.[21] The CCPA similarly took the approach of refraining from requiring businesses to honor global browser settings or privacy controls. The CA AG was empowered by statute only to "adopt regulations to further the purposes of [the CCPA]."[22] Thus, as the CCPA does not authorize or contemplate an opt-in regime, the CA AG lacks statutory authority to promulgate the browser mandate.

By imposing a *de facto* opt-in regime that the California Legislature has previously rejected and again declined to adopt in the CCPA, the draft regulation would usurp legislative authority and violate the separation of powers required by the California Constitution.[23] Transforming the legislative directive for an opt-out system to an opt-in system is not within the scope of the delegated legislative authority, nor is it reasonably necessary to implement the CCPA, nor is it a reasonable interpretation of the CCPA's terms.[24] It therefore violates multiple aspects of the separation-of-powers doctrine.[25]

2. The CA AG's Economic Impact Analysis Neglected to Consider the Unique Impacts of the Browser Mandate

The CA AG failed to comply with California's Administrative Procedure Act ("APA") when it neglected to consider the unique economic costs associated with the browser mandate at the initial proposal stage. Agencies are required by law to consider the economic impacts of proposed regulations

---

[19] Cal. Civ. Code § 1798.120.
[20] *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)).
[21] *See Assembly Committee on Business, Professions and Consumer Protection*, Hearing Report on AB 370 (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.'")
[22] Cal. Civ. Code § 1798.185.
[23] Cal. Const. Article III, Section 3 ("The powers of state government are legislative, executive, and judicial. Persons charged with the exercise of one power may not exercise either of the others except as permitted by this Constitution.").
[24] *See Yamaha Corp. v. State Bd. of Equalization*, 19 Cal. 4th 1, 6 (1998).
[25] *See id.*

prior to submission.[26] The CA AG's economic impact assessment did not separately consider the effective opt-in regime created by the browser mandate, which will prevent regulated businesses from selling data from a class of consumers who have not expressed specific data-sharing preferences.[27] It also did not consider the costs consumers could incur from default opt-out signals expressed through browsers without their express permission or buy-in. Thus, the impact analysis erroneously counted as a benefit what should have been counted as a cost—loss of value to consumers when opt-out signals are cast without their permission, and lost revenue for businesses that otherwise would have been able to sell personal information about parties who do not oppose the sale of personal information and thus derive no benefit from this prohibition. A substantial failure to comply with the APA is grounds for a regulation's invalidation,[28] and California courts have invalidated regulations in cases where an agency's economic impact analysis was "materially deficient."[29] We therefore urge the CA AG to either reexamine the economic impacts of the browser mandate or remove it from the final regulation.

3. The Browser Mandate Violates the First Amendment

By turning the opt-out regime into an opt-in regime through the requirement to honor global privacy controls set through browsers, the CA AG's proposal violates the First Amendment to the United States Constitution, as applied to California through the Fourteenth Amendment, and Section 2(a) to the Declaration of Rights within the California Constitution (Article I). The dissemination of data collected by a business is constitutionally protected commercial speech.[30] In order for a regulation restricting commercial speech to pass constitutional muster, (1) the state must assert a substantial interest in restricting this speech, (2) the regulation must directly advance that interest, and (3) the regulation must be narrowly tailored to serve that interest.[31] There is a substantial state interest in the protection of consumer privacy in business relationships.[32] But, this proposal neither directly advances a substantial governmental interest, nor is it narrowly tailored to advance such an interest. Therefore, it violates the First Amendment and Art. 1, Sec. 2(a).

Regulations that provide only "'ineffective or remote support for the government's purpose'" do not satisfy the constitutional protections afforded to commercial speech.[33] As is further explained below, forcing businesses to defer to global privacy controls is less effective and less direct than the opt-out methods employed by the rest of the CA AG's regulations. The comprehensive opt-out system devised by the CA AG and the California Legislature directly addresses a consumer's relationship with an individual business, allowing consumers to express their privacy preferences in the context of their unique relationships with individual entities. The global privacy controls proposal, on the other hand, requires businesses to infer nuanced attitudes toward data disclosure from a one-size-fits-all device setting. Thus, if the State's interest is in preventing the spread of specific data that a consumer wishes to withhold, the global privacy controls proposal falls short—it provides no indication that a consumer desires to withhold information particular to a specific business relationship, instead forcing businesses to infer disclosure preferences from a remote and indirect signal which might not accurately reflect a consumer's attitude towards the data at issue in a given transaction.

---

[26] Cal. Gov. Code § 11346.3(a)(2).
[27] *SRIA*, supra note 10.
[28] *Western States Petroleum Assn. v. Bd. of Equalization*, 304 P.3d 188, 203 (Cal. 2013).
[29] *See, e.g., John R. Lawson Rock & Oil, Inc. v. State Air Resources Bd.*, 20 Cal. App. 5th 77 (Cal. App. 5th 2018).
[30] *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).
[31] *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).
[32] *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1192 (W.D. Wash.).
[33] *Id*. (quoting *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980)).

Moreover, the proposal is not narrowly tailored to serve the state's interest; it needlessly restricts the commercial speech of regulated businesses without bolstering the effectiveness of the existing opt-out framework. In order to be narrowly tailored, a regulation must not be disproportionately burdensome and must "signify a careful calculation of the costs and benefits associated with the burden on speech imposed."[34] The existing opt-out regime provides businesses with precise information about the informed preferences of individual consumers. The global privacy controls rule, though serving no additional purpose not already served by the opt-out rules, has the potential to restrict speech by requiring businesses to defer to potentially inaccurate information about a consumer's individual preferences. Section 999.315(d)(2) of the CA AG's proposed regulation provides that, if global privacy controls conflict with the individual user preferences logged into a business's privacy settings, a business must defer to the global privacy controls by default or must seek out separate approval from the consumer. Thus, businesses are required by default to defer to a general and imprecise expression of user preference at the expense of specifically expressed preferences, and businesses must bear the cost of clearing up these indeterminacies. The standard opt-out regime is both more precise and less burdensome, as it allows businesses to assess the specific preferences of users in the context of each unique consumer relationship and restricts commercial speech only inasmuch as that speech is known to interfere with consumer preferences.

The global privacy controls rule does nothing to enhance the existing opt-out regime, while needlessly restricting speech. Thus, the global privacy controls rule unconstitutionally imposes burdens on commercial speech without offsetting those burdens with benefits.

B. The Browser Mandate Hinders Consumer Choice and Allows Intermediaries to Block Consumer Preferences

As we have explained in prior submissions, the unprecedented requirement to honor global privacy settings and browser controls does not further the purposes of the CCPA. Instead, it threatens to impede consumers' ability to make choices about specific entities that can and cannot sell personal information. Because global privacy controls cast a single opt-out signal to every business across the entire Internet ecosystem, the ability to make granular choices that the California Legislature meant to confer on consumers would be rendered nonexistent.

Additionally, such a requirement would be poised for intermediary tampering, as businesses would have no way to verify whether a signal is a genuine consumer-set preference. In the March 11, 2020 second set of modifications to the draft rules, the CA AG removed the requirement for consumers to "affirmatively select" such browser signals or privacy controls to clearly indicate a choice to opt out.[35] The CA AG also removed a provision stating that "[t]he privacy control… shall not be designated with any pre-selected settings."[36] The result of striking these important terms is that intermediaries will be able to set *default* opt-out signals through browsers that may have absolutely no connection to a consumer's actual preferences. The proposed regulations therefore take choice away from consumers by inserting the choice of intermediaries in place of those consumers. In departing so far from the legislative intent, the requirement would be arbitrary and capricious.

[34] *Id*. at 1194.
[35] *Compare* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Feb. 10, 2020) *with* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Mar. 11, 2020).
[36] *Id*.

C. The Draft Rules Offer No Clarity Regarding How Conflicting Privacy Controls or Signals Should Be Managed

It also is unclear in the most recent draft how default browser signals should interact with a consumer's previously expressed desire to allow a business to sell personal information. If, for example, a consumer has enabled an individual business to sell personal information, a browser's subsequent institution of a default global opt out would cut directly against the choice the consumer expressed directly to the business. Any subsequently instituted default global privacy control would effectively block the particularized choice that the consumer set with the individual business. The requirement to honor browser signals and global privacy controls would allow intermediaries to interfere with consumers' individual choices by using cookies, plugins, JavaScript and other technologies to set a single signal to the marketplace. Consumer preferences cannot be respected if such interference is permitted. As a result, the obligation to honor browser signals and global privacy controls coupled with intermediaries' capability to set such controls by default has the potential to obstruct consumers' expressed choices.

Additionally, the browser signal requirement advantages consumer-facing businesses over others in the marketplace and entrenches incumbents who regularly interface with consumers. Third party entities, for example, might not have a direct touchpoint with consumers through which they could ascertain whether a consumer intends to opt in or opt out of personal information sale. Moreover, it is not clear how, or at what frequency, companies would be able to communicate with consumers in regard to default privacy settings. Businesses would be forced to ask consumers to opt in to the sale of personal information every time the consumer interacts with that business. However, the CCPA limits a business's ability to seek "opt-in" consent to once every twelve months.[37] The lack of clarity on this issue will impede the expression of consumers' actual choices and will hinder their ability to express preferences in the marketplace.

D. The CA AG Should Amend its Approach To Browser Settings So It Is Less Restrictive and So It Passes Constitutional Muster

Instead of requiring businesses to honor browser settings and global privacy controls, the CA AG should update the draft rules to allow businesses that sell personal information to *either* (1) honor user-enabled privacy controls as valid requests to opt out, *or* (2) offer another effective mechanism for the consumer to submit a request to opt out, such as a "Do Not Sell My Info" link and an interactive form that enables the consumer to opt out of personal information sale. This is a better approach that will enable consumers to express individualized choices about specific entities' use of data. This approach would also avoid the constitutional concerns inherent in the browser signal requirement. There is no privacy-enhancing reason to require businesses to respect user-enabled privacy controls over choice provided by a business. Updating the draft rules to give businesses the ability to respect such controls or offer another, equally effective opt-out mechanism would allow consumers to make granular opt-out choices instead of concentrating control and power in the hands of intermediaries such as browsers.

IV. Clarify that Internally-Generated Inferences and Derived Data Are Not Subject to a Consumer Request to Know

In the course of developing the draft rules, the CA AG helpfully aligned the regulations with the text of the CCPA by clarifying that a "request to know" means a consumer request that a business disclose personal information that it has *collected* about the consumer, including the specific pieces of

[37] Cal. Civ. Code § 1798.135(a)(5).

personal information *collected* about the consumer.[38] The draft rules do not, however, state whether internally-generated data, such as inferences and derived data, must be returned in response to a consumer request to know. We ask the CA AG to issue additional updates to the draft rules to clarify that internally-generated inferences and derived data need not be returned in response to a consumer request to access specific pieces of personal information because such data is not collected.

For most businesses, providing access to personal information is both an important and costly aspect of complying with the CCPA. Providing access presents challenges because many businesses do not maintain information about an individual in a centralized way, so complying with access requests often involves a manual process of searching through various storage locations to build a centralized collection of data that can be provided to a consumer. Additionally, in today's day and age, nearly every entity processes information about individuals in some manner and generates internal data, like internal inferences, that would be both time-consuming to collect and of little privacy value to consumers. Against this backdrop, it is critical that businesses have clarity around what data should be disclosed under CCPA. The draft rules should require a business to return to the consumer the specific pieces of personal information it has collected about the consumer, but not the personal information it independently generated or derived from such data. This approach reflects a logical reading of the law and aligns with consumer expectations as to the types of data that could be "collected" from and sold about them.

This interpretation also protects the intellectual property of businesses in their inferences and provides clear guidance that allows them to practically provide information about consumers that is readily understandable. Significantly, a broader interpretation that would require the disclosure of inferences or decisions made tied to a consumer would in many cases infringe on the intellectual property of businesses. Companies compete on providing consumers with the best consumer experience, including through pricing, customer support, product offering scope, and many other factors. In the digital age, consumer experience is driven by trade secrets regarding computing and efficiencies. The CCPA specifically recognizes and enumerates that information that amounts to intellectual property or a business's trade secrets should be exempt from the law. The statute instructs your office to "establish… any exceptions necessary to comply with state or federal law, including but not limited to those relating to trade secrets and intellectual property rights."[39]

Pursuant to Section 1798.110 of the CCPA and the draft regulations, a consumer may request that a business disclose to them personal information that the business has collected about the consumer.[40] The final rules should clarify that the duty to disclose information that a business collects does not apply to *internally-generated* data such that business are not required to disclose such data in response to a consumer access request for specific pieces of personal information. Such information was not "collected" consistent with the law's definition of the term. However, this is distinguishable from instances where a business receives or buys inferred data from another entity. In such cases the business *has* collected this data and would be subject to a verified consumer access request.[41] Additionally, if a business sells its proprietary inferences to a third party or discloses such inferences for a business purpose, the business would disclose that it has sold and/or disclosed the category of "inferences" pursuant to the CCPA requirement to provide the categories of personal information that the business sold and disclosed about the consumer for a business purpose.[42] This reading of the CCPA is supported by the text of the law itself as well as your office's recent revisions to the regulations implementing the CCPA.

---

[38] *Id*. at § 1798.110(a)(1); *see also* Cal. Code Regs. tit. 11, § 999.301(q) (proposed Mar. 11, 2020).
[39] Cal. Civ. Code § 1798.185(a)(3).
[40] *Id*. at § 1798.110(a)(5).
[41] *Id*.
[42] *Id*. at §§ 1798.115(a)(2)-(3).

Compelled disclosure of proprietary information would have significant legal consequences. Not only would it exceed the scope of the legislative delegation (and thus implicate separation of powers), it also could constitute a regulatory taking prohibited by the Fourteenth Amendment to the U.S. Constitution and Article 1, Sections 1, 7(a). 15, and 19(a) to the California Constitution. Inasmuch as it would have substantial effects on interstate commerce, it also could violate the dormant Commerce Clause, Article 1, Section 8 to the U.S. Constitution.

The CCPA appropriately limited the scope of the access obligations to "collected" data to avoid imposing undue burden on California businesses and ensure the data provided to consumers is meaningful and intelligible. If the CCPA were to require businesses to return *all* generated data, including inferences in response to a consumer access request, consumers would be burdened by the delivery of excessively detailed and potentially incomprehensible information, including internally-generated inferences—basic computing connections, like validating a name, that businesses must undertake in order to sustain day-to-day operations. Businesses ultimately would have difficulty or impossibility in complying. A business's provision of this data to a consumer would hinder the consumer's ability to access meaningful information about the information collected from or about the consumer, thereby thwarting the aim of the CCPA to provide consumers with enhanced transparency. For these reasons, ANA urges the CA AG to update the draft rules to clarify that a business should return to a consumer the specific pieces of personal information it has *collected* about the consumer, but not the personal information it independently generated, inferred, or derived from such data.