January 17, 2023

Office of the Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203

RE: Joint Ad Trade Letter – Comments on Colorado Privacy Act Regulations

Dear Office of the Colorado Attorney General:

On behalf of the advertising industry, we provide input on the proposed regulations to implement the Colorado Privacy Act ("CPA").[1] We and the companies we represent, many of whom do substantial business in Colorado, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies.

We understand that our goal of harmonizing the CPA implementing regulations with other state approaches to privacy is shared by your office, as a key principle defined at the outset of the CPA rulemaking process was to "facilitate interoperability and help situate the CPA alongside the competing protections and obligations created by other state, national, and international frameworks."[2] As a result, in this comment letter, we provide input and suggested changes to discrete proposed regulatory provisions to help ensure the CPA implementing regulations are consistent with the law, aligned with other state approaches to privacy regulation, and protective of consumers while remaining workable for businesses.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.[3] Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We welcome the opportunity to engage with you in this process to develop regulations to implement the CPA.

---

[1] Colorado Attorney General, *Version 2 of Proposed Colorado Privacy Act Rules*, located at https://coag.gov/app/uploads/2022/12/CPA_Version-2-Proposed-Draft-Regulations-12.21.2022.pdf (Dec. 21, 2022).
[2] Colorado Attorney General, *Pre-Rulemaking Considerations for the Colorado Privacy Act* at 2, located at https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf.
[3] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf (hereinafter, "Deighton & Kornfeld 2021").

I. Colorado Should Take Steps to Harmonize Its Approach to Privacy with Other States When Such Harmonization Would Benefit Consumers and Controllers

We and our members support a national standard for data privacy at the federal level. In the absence of such a national standard, it is critical for regulators to seriously consider the costs and confusion to both consumers and businesses that will accrue from a patchwork of differing privacy standards across the states. Harmonization with existing privacy laws is essential for creating an environment where consumers in Colorado and other states have a consistent set of expectations, while minimizing compliance costs for businesses. Compliance costs associated with divergent, and oftentimes conflicting, privacy laws are significant. To make the point: one report found that privacy laws could impose costs of between $98 billion and $112 billion annually, with costs exceeding $1 trillion dollars over a 10-year period and small businesses shouldering a significant portion of the compliance cost burden.[4] Below we identify regulatory provisions that should be amended to harmonize the proposed regulations to implement the CPA with the approach to privacy in other states.

A. Proposed Regulations Create New Categories of Personal Data Beyond the Scope of the CPA

In line with the goal of harmonizing the implementing regulations with the CPA itself and other state laws, updates to the definitions section of the proposed rules should be made to foster uniformity. For example, the CPA already defines "Personal Data" and "Sensitive Data," but the proposed regulations would create entirely new categories of information such as "Sensitive Data Inferences" and define new concepts such as "Revealing" that go beyond the scope of the CPA and are out-of-step with other states.[5] The implementing regulations should effectuate the CPA as passed by the legislature and should not expand the scope of the law. Rule 2.02 should consequently be updated to remove the definitions of "Sensitive Data Inferences" and "Revealing."

The draft rules' approach to biometric information is another example of the proposed rules extending beyond the scope of what is covered in the CPA and diverging from other state approaches to privacy. The proposed regulations would define "Biometric Data" to include a subset of biometric information deemed to be "Biometric Identifiers."[6] These dual definitions in the proposed CPA regulations are confusing and could result in creating opt-in consent requirements for biometric information that is not actually used for identification purposes. Rule 2.02 should be updated to align the definition of "Biometric Data" with other state law definitions of the term and to remove the concept of "Biometric Identifiers" from the draft rules.

B. Pop-Up Banners and Other Methods of Obtaining Consent Should Be Permitted

The proposed regulations suggest that controllers may not obtain consent from consumers through a pop-up banner, but rather may only obtain consent via a link at the top of a webpage.[7] The proposed rules also suggest that certain effective methods of obtaining consent, such as just-in-time requests, may be prohibited. This approach is overly restrictive and in conflict with other approaches in the U.S. and EU, which do not place prescriptive limitations on how controllers may present consent requests to consumers. Companies operating in U.S. and EU jurisdictions use consent banners widely

[4] Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws (finding that small businesses would bear approximately $20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).
[5] Colorado Privacy Act Rules, 4 CCR 904-3 at Rule 2.02 (proposed Dec. 21, 2022).
[6] *Id.*
[7] *Id.* at Rule 7.05(B), (E) & (F).

as a method of obtaining consumer consent. This proposed regulation does not further consumer protection, but instead would unreasonably restrict controllers' ability to communicate with consumers. As a result, the proposed regulations' prohibition on regularly used consent request methods in Rule 7.05 should be removed.

II. Consumers Should Be Required to Take An Affirmative Step to Turn On Universal Opt-Out Mechanisms

The proposed regulations would consider a consumer's decision to adopt *any* mechanism, tool, or product "marketed as a tool that will exercise a user's rights to opt out" as the consumer's affirmative, freely given, and unambiguous choice to turn on a Universal Opt-Out Mechanism ("UOOM").[8] Consumers download and adopt various Internet-enabled tools and products for myriad reasons. The proposed regulations assume consumers prioritize an ancillary feature like a UOOM or understand the implications of such tools and choose to download or purchase them specifically to stop particular processing purposes. In reality, consumers' decisions to use specific Internet-enabled products, services, or mechanisms—such as browsers, routers, plug-ins, or other tools—very well may be for another purpose (*e.g.*, speed, WiFi coverage, password management features, etc.) and *not* specifically to enable a UOOM. For example, merely using a browser or a Bluetooth-enabled "smart product" like a lightbulb that automatically transmits a do-not-sell signal should not suffice to indicate a choice to turn on a UOOM—even if the lightbulb's opt-out features are advertised—because the main purpose of the tool is to provide light, not to send opt out signals. To be clear, if part of the aim of CPA is to provide transparency about data uses to consumers, then this provision undercuts that goal, instead replacing it with greater opaqueness by having a constellation of consumer products all sending signals without the consumer ever knowing anything about the impact or meaning of those actions.

Understanding a consumer's choice to merely *use* a mechanism, tool, or product with a primary feature that is *not* a UOOM as an affirmative, freely given, and unambiguous choice to enable a UOOM contravenes the spirit of the CPA. The CPA requires UOOMs to clearly represent the consumer's "affirmative, freely given, and unambiguous choice to opt out."[9] A consumer's use of a mechanism or product, such as a lightbulb, that has a primary use *entirely extrinsic* to the opt-out signal carried with the product does not signify that the consumer is affirmatively or unambiguously choosing to opt out. To the contrary: the consumer likely chooses to use the given lightbulb for the primary use for which it is intended. The CPA also plainly prohibits a consumer's acceptance of "general or broad terms of use that contain descriptions of personal data processing along with other, unrelated information" to constitute valid consent,[10] and the proposed regulations state that consent is not freely given when it is bundled with other terms and conditions.[11] Given these provisions, it is unclear why a consumer's choice to use a product or tool that simply contains a UOOM as a subsidiary feature should be understood as an affirmative and unambiguous choice to enable that feature when the consumer is not required to take a specific and separate action to turn on the UOOM. Rule 5.04(B) of the proposed regulations should thus be updated to require an affirmative action by a consumer, such as the clicking of a button or checking of a box, to turn on a UOOM, regardless of how a given product containing a UOOM is marketed.

[8] *Id.* at Rule 5.04(B).
[9] Colo. Rev. Stat. § 6-1-1313(2)(c).
[10] *Id.* at § 6-1-1303(5)(a).
[11] Colorado Privacy Act Rules, 4 CCR 904-3 at Rule 7.03(C)(2)(a) (proposed Dec. 21, 2022).

III. Authorized Agents Should Be Prohibited From Submitting Opt-Out Requests Through UOOMs

The proposed regulations do not clarify how authorized agents may submit opt-out requests on behalf of consumers.[12] In particular, the rules do not explain how a controller should or could verify that an agent has authority to act on behalf of the consumer when the agent submits a request through a UOOM. Rules 4.02 and 4.03 should consequently clarify that authorized agents may submit opt-out requests on behalf of consumers to controllers through methods that involve direct communication with a controller, such as through an email or an opt-out link or webform on a controller's website, but agents may not submit opt-out requests via UOOMs on behalf of consumers.

IV. The Term "Substantive" Should Be Struck From Notification Requirements Because It Is Ambiguous and Would Create Confusion

According to the proposed rules, if any "substantive or material" change to a processing purpose disclosed in a revised privacy notice constitutes secondary use, a controller must obtain consent from the consumer for such processing.[13] Of note, the term "substantive" does not appear in the CPA. While the proposed regulations provide certain examples of which changes may qualify as "substantive or material," they do not set forth an exhaustive list. Likewise, the Federal Trade Commission ("FTC") does not use the term "substantive" in its guidance on activity that could constitute a "material" privacy policy change. However, neither the FTC nor the proposed CPA regulations provide any meaningful information regarding what constitutes a "substantive" edit to a privacy notice. Rule 6.04 should be updated so only "material" changes to a processing purpose that will be applied retroactively (*i.e.*, to previously collected personal data) constitute secondary use requiring consent. Such a change will help avoid confusion and ease controllers' ability to understand when consent is required.

V. Dark Pattern Rules Should Not Force Controllers to Provide Content or Services

The proposed regulations would set forth prescriptive rules dictating how controllers may interact with their customers.[14] These mandates extend beyond requirements for methods of obtaining consumer consent. For example, the regulations prohibit consumers from being redirected away from content or services they are attempting to access because they declined a consent choice offered to them.[15] This kind of prescriptive requirement is not a "user interface" requirement, but rather serves to functionally force controllers to provide all content or services they offer to everyone regardless of the consent choices received from the consumer. Many online services are powered by consumer data and simply cannot be fully funded, exist, or function absent the ability to process such information. Rule 7.09 should be updated so controllers may stop offering services or access to information if the consumer does not provide the consent necessary for the controller to provide such offerings.

VI. Dark Pattern Rules Should Provide Clear and Reasonable Requirements for Consumer Communications

The proposed regulations' dark pattern mandates would place overly prescriptive, unclear, and subjective requirements on controllers to avoid "emotionally manipulative language or visuals to

[12] *Id.* at Rule 4.02 & 4.03.
[13] *Id.* at Rule 6.04.
[14] *Id.* at Rule 7.09.
[15] *Id.* at Rule 7.09(6)(b).

coerce or steer Consumer choice."[16] The draft regulations do not make clear what constitutes such "emotionally manipulative" communications, and given the subjective nature of the requirement, it would be infeasible to operationalize for interactions with all consumers. The proposed regulation could have the unintended effect of deterring businesses and nonprofits from communicating helpful information about products and services to consumers. The proposed regulation may also raise First Amendment concerns by unreasonably hindering commercial speech. Businesses and organizations have a constitutionally-protected First Amendment right to present truthful information to consumers, and the proposed overly restrictive requirements on speech interfere with this right. The requirement to avoid "emotionally manipulative" communications with consumers in Rule 7.09(2) should be removed from the draft rules rather than set forth a blanket rule with little to no explanation or contextual limits.

VII. Documentation and Disclosures Should Require Categories of Entities Rather Than Specific Names of Entities

In several sections of the proposed regulations, the rules would require controllers to document or disclose the names of third parties, affiliates, and processors to whom they disclose personal data.[17] The CPA itself provides no such requirement, instead opting to require documentation or disclosure of the categories of such entities rather than the names of the entities themselves.[18] Requiring documentation or disclosure of the names of entities would be operationally burdensome, as controllers change business partners frequently, and companies regularly merge with others and change names. Additionally, such a requirement could force controllers to abridge confidentiality terms they may have in place with their customers in contracts. To align with the CPA, simplify compliance, and avoid forcing controllers to violate contractual confidentiality provisions, all requirements to disclose or document names of third parties, affiliates, or processors should be removed from the draft rules and should be substituted with a requirement to disclose or document the categories of such entities.

VIII. Consumer Rights Should Clearly Exclude Pseudonymous Data To Align With The Text of the CPA

The proposed regulations would require controllers to return "all the specific pieces of Personal Data" collected and maintained about a consumer in response to a consumer access request.[19] Similarly, the proposed regulations would require correction, deletion, and portability of *all* consumer personal data.[20] The CPA itself makes clear that pseudonymous data, as defined, is exempt from all consumer rights except for the right to opt out.[21] However, as drafted, the proposed regulations do not recognize this statutorily provided exclusion, which would cause confusion for consumers and companies. Regulations promulgated by the Colorado Attorney General ("CO AG") must align with the directives set forth in law. The CO AG should, therefore, update Rules 4.04, 4.05, 4.06, and 4.07 to make clear that consumer rights requests are subject to certain exemptions provided by the CPA to ensure the proposed regulations do not directly contravene CPA.

---

[16] *Id.* at Rule 7.09(2).
[17] *See, e.g.*, *id.* at Rule 6.05(E)(1)(d) & 7.03(E)(1)(e).
[18] Colo. Rev. Stat. § 6-1-1308(1)(a)(V).
[19] Colorado Privacy Act Rules, 4 CCR 904-3 at Rule 4.04(B) (proposed Dec. 21, 2022).
[20] *Id.* at Rule 4.05, 4.06, & 4.07.
[21] Colo. Rev. Stat. § 6-1-1307(3) ("The rights contained in Section 6-1-1306(1)(b) to (1)(e) do not apply to pseudonymous data if the controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.")

IX. Sensitive Data Consent Requirements Should Align With the CPA

The proposed regulations' examples related to consent for sensitive data processing suggest consent is required for each individual processing action.[22] For instance, the regulations state consent is required to process sensitive data for a consumer-requested service, and a separate consent is required to share sensitive data for advertising purposes.[23] Coupled with the regulations' requirements related to "refreshing" consent, requiring consumer consent for each individual sensitive data processing action would inundate consumers with an unreasonable number of consent requests without providing meaningful consumer protection.[24] The CPA itself states that consent is required for sensitive data processing generally. The regulations should be amended to align with the law to require consent for sensitive data processing generally instead of requiring separate consents for each individual processing action.

X. Controllers Should Not Be Forced to Provide Loyalty Programs to Consumers Who Opt Out

The proposed regulations state that if a consumer exercises their right to delete, making it impossible for the controller to provide a bona fide loyalty program benefit to the consumer, the controller is not obligated to provide that benefit.[25] We agree. This clarification should be extended to the opt-out right in addition to the deletion right. Loyalty programs depend on the ability to use and transfer personal data. Without this ability, the utility and feasibility of offering a loyalty program is diminished. Controllers should not be forced to offer loyalty programs if the data they need to provide such programs is inaccessible. Rule 6.05 should clarify that controllers are not required to provide loyalty program benefits to consumers that exercise rights that remove the controller's ability to use personal data to power a loyalty program.

XI. Controllers Should Be Permitted to Exercise Reasonable Discretion For Correction Requests

The proposed regulations include certain requirements for personal data correction that are overly rigid and do not align with business practices. For example, the proposed rules would require controllers to correct personal data "across all data flows and repositories" and implement measures to "ensure" personal data remains corrected.[26] These standards are unreasonably high and would require constant updates and refreshes of datasets to maintain perfectly accurate information at all times. Additionally, the proposed correction rules would require controllers who do not have documentation vouching for the accuracy of the personal data they maintain to take any consumer's allegation of inaccuracy as fact.[27] Such correction rules could inadvertently enable fraudulent requests. Rule 4.05 should be updated to permit controllers to exercise reasonable discretion for correction requests and to provide a less rigid standard than the present requirement to "ensure" accuracy across all databases.

[22] Colorado Privacy Act Rules 4 CCR 904-3 at Rule 7.03(C)(3), (D)(4) & 7.08(C).
[23] *See id.* at Rule 7.03(D)(4).
[24] *See id.* at Rule 7.08.
[25] *Id.* at Rule 6.05(B).
[26] *Id.* at Rule 4.05(A).
[27] *Id.* at Rule 4.05(H).

XII. The Regulations Should Provide Flexibility to Accommodate IoT Devices and Different Kinds of Channels Through Which Consumers and Controllers Interact

The proposed regulations would require disclosures, notifications, and other communications to consumers to be "[r]eadable on all devices through which Consumers interact with the controller…."[28] This language would require entities that offer IoT devices or interact with consumers through different kinds of channels to provide notices and consent fields in an overly restrictive manner. The requirement ignores the fact that some IoT devices, such as smart speakers, smart doorbells, smart cameras, smart locks, smart vacuums, and myriad other devices may not contain a field where text can be presented to a consumer. Requiring controllers to provide notices through those devices could be impractical and hinder consumer education about the privacy features of the device. Instead, the proposed rules should permit companies that engage with consumers through novel avenues to provide required notices through other means, such as account settings if maintained, or interfaces that are regularly used in conjunction with the controller's product or service, such as companion apps or other similar tools.

XIII. Similar Symmetry of Steps for Consent Choices Should Be Required

The proposed regulations would require a controller to permit a consumer to refuse or revoke consent "within the same number of steps" as the initial consent was affirmatively provided.[29] This rule is overly prescriptive and places too much emphasis on the "number of steps" for the consent path rather than the quality of the communication with the consumer. This requirement also ignores the fact that consent and revocation of consent may need to be achieved through different channels, and certain devices may not permit revocation of consent to be achieved in the same number of steps as consent may be provided. For example, a smart phone may send just-in-time consent prompts before rendering an app, but may require revocation of consent through the user's navigation to the privacy preferences menu in the device settings. Revocation of consent thus may need to involve more "steps" than the initial just-in-time consent. Rule 7.09(B)(5) should consequently be updated so controllers must enable consumers to make choice options within a "similar" number of steps, thereby mirroring the change the CO AG already made to Rule 7.07(A) with respect to symmetry of steps for consent.

XIV. Required Disclosures Should Cover Online, Rather than Offline, Practices

The proposed regulations would require privacy notices to include information about offline data processing practices. This regulation exceeds the scope of the CPA, which does not require disclosures related to offline practices. In addition, this requirement is not inherent in the overwhelming majority of other states' privacy-related laws and regulations. Requiring disclosures about offline data collection and processing practices would be a stark departer from existing privacy policy requirements, which are tied to online practices related to personal data. Rule 6.03(A)(1) should be updated to remove the requirement to cover offline practices in a privacy notice.

XV. The Data-Driven and Ad-Supported Online Ecosystem Benefits Colorado Residents and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A recent 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 between two to three percent per year.[30] In 2020 alone, it contributed $2.45 trillion to the U.S.'s $21.18 trillion

[28] *Id.* at Rule 3.02(A)(5).
[29] *Id.* at Rule 7.09(B)(5).
[30] Deighton & Kornfeld 2021 at 5.

GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of $300 billion.[31] Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.[32] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.[33] The same study found that the ad-supported Internet supported 154,403 full-time jobs across Colorado, more than double the number of Internet-driven jobs from 2016.[34]

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulations that significantly hinder certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.[35] One recent study found that "[t]he U.S. open web's independent publishers and companies reliant on open web tech would lose between $32 and $39 billion in annual revenue by 2025" if third-party tracking were to end "without mitigation."[36] That same study found that the lost revenue would become absorbed by "walled gardens," or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.[37] 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.[38] According to one study, "[b]y the numbers, small advertisers dominate digital advertising, precisely because online advertising offers the opportunity for low cost outreach to potential customers."[39] Absent cost-effective avenues for these smaller advertisers to reach the public, businesses focused on digital or online-only strategies would suffer immensely in a world where digital advertising is unnecessarily encumbered by overly-broad regulations.[40] Data-driven advertising helps to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Coloradans' 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 cutting-edge information. Advertising revenue is an important

---

[31] *Id*.
[32] *Id*.
[33] *Id*. at 6. *See also* Digital Adverising Alliance, *Summit Snapshot: Data Drives Small-and Mid-sized Business Online, It's Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located at https://digitaladvertisingalliance.org/blog/summit-snapshot-data-drives-small-and-mid-sized-business-online-it%E2%80%99s-imperative-regulation-not.
[34] *Compare* Deighton & Kornfeld 2021. at 123 (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 67,895 full-time jobs to the Colorado workforce in 2016 and 154,403 jobs in 2020).
[35] *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 (hereinafter, "Deighton 2020")
[36] *Id*. at 34.
[37] *Id*. at 15-16. *See also* Damien Geradin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech*, EUROPEAN COMPETITION JOURNAL (Dec, 18, 2020), located at https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1848059.
[38] Deighton 2020 at 28.
[39] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 9 (2022), located here.
[40] *See id*. at 8.

source of funds for digital publishers,[41] and decreased digital advertising budgets directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[42] And, consumers tell us that. In fact, consumer valued the benefit they receive from digital advertising-subsidized online content at $1,404 per year in 2020—a 17% increase from 2016.[43] Another study found that the free and low-cost goods and services consumers receive via the ad-supported Internet amount to approximately $30,000 of value per year, measured in 2017 dollars.[44] Regulatory frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such regulatory frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media

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.[45] Additionally, in a 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.[46] Indeed, as the Federal Trade Commission noted in its 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.[47]

Laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and 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

---

[41] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00117/544506-00117.pdf.

[42] *See* John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located at https://www.ipc.be/~/media/documents/public/markets/the-value-of-data-consequences-for-insight-innovation-and-efficiency-in-the-us-economy.pdf.

[43] Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at $1,400/Year; Annual Value Jumps More Than $200 Since 2016* (Sept. 28, 2020), located at https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200.

[44] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), located here.

[45] 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.

[46] 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.

[47] 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.

therefore respectfully ask you to carefully consider the proposed regulations' potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing them through the regulatory process.

* * *

We and our members support protecting consumer privacy. We thank you for considering our comments on the proposed regulations to implement the CPA and the need for harmonization across state privacy standards. We look forward to continuing to work with you as your office further develops the proposed regulations to implement the CPA.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
202-296-1883

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

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
212-380-4700

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