409 7th Street, NW Suite 250
Washington, DC 20004

June 22, 2022

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

Dear Attorney General Weiser,

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide preliminary comments on proposed rulemaking under the Colorado Privacy Act ("CPA").

I. Introduction and Overview of the NAI

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to our FIPPs-based, privacy-protective Code of Conduct (the "NAI Code"), which underwent a revision in 2020 to keep up with changing business practices and consumer expectations. Member compliance with the NAI Code is backed by a strong accountability program, which includes a comprehensive annual review by NAI staff of member companies' business models, policies and practices to ensure their compliance with the NAI Code, even as their individual businesses, and the industry as a whole, evolves. The NAI also educates and empowers consumers to make meaningful choices about their experience with digital advertising through its easy-to-use, industry-wide opt-out mechanism.

The NAI supports the Office of the Attorney General ("OAG") in its principle-guided rulemaking approach outlined in its April preliminary rulemaking document, including harmonizing, encouraging innovation, clarifying ambiguities, and streamlining compliance. The NAI respectfully makes the below recommendations for the OAG's consideration in drafting implementing regulations.

II. Universal Opt-Out

"Universal opt-out mechanisms," (UOOMS) generally refer to HTTP-based signals (either deployed natively or via plugins), device settings, or other mechanisms that communicate or signal to a business a consumer's choice to exercise his or her rights to opt out as provided by the CPA and potentially similar state laws. These are also often referred to as "global privacy controls," or "opt-out preference signals."

The NAI has a long history of promoting consumers' ability to exercise choice over uses of their data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use choice mechanisms is a foundational element of tailored advertising that we have championed for decades. To that end, we believe that the adoption of UOOMs, under effective legal guidelines, can be a valuable tool for both consumers and businesses alike. However, it is imperative that UOOMs not be offered in a way by technology or platform providers that unfairly disadvantage other businesses. Ensuring that UOOMs are not activated by default by technology intermediaries, but rather reflect a clearly expressed choice by a consumer, is essential.

Consistent deployment and recognition of these signals, not just in Colorado but across the U.S. more broadly, would help to minimize confusion among consumers who deploy such mechanisms. We therefore appreciate the protections established by the CPA to provide for rulemaking to accomplish these important goals, and we appreciate your thoughtful questions on this topic posed in your Pre-Rulemaking Considerations. Please see below our answers to those questions.

A. ***Should the rules point to specific protocols or proposed specifications?***

The rules should refrain from promoting specific UOOMs, and instead should allow for various platforms and technology providers to develop signals that work effectively on their platforms and for their users. Given the wide range of devices and platforms, as well as the evolving nature of information technology services and platforms, it would be imprudent to identify specific technologies in a formal rulemaking process.

Instead, the rules should establish a set of basic operational standards or criteria establishing guidelines around what constitutes a UOOM activated with the consent of a user. This set of standards and guidelines should be developed through an open and transparent review process that provides for stakeholder input, to evaluate any mechanisms proposed to be recognized by businesses covered by the law. The review process should be ongoing, providing the OAG with the opportunity to periodically evaluate and test approved UOOM to ensure that they continue to be administered fairly. To assist in the review process, the OAG should seek input from stakeholders, particularly those businesses to which the signals are directed.

B. ***Should the rules discuss specific considerations tailored for different categories of tools that might serve as UOOMs, such as browsers, operating system settings, and browser add-ons, or should our rules remain strictly technology neutral?***

As noted above, the NAI concurs with OAG's stated objectives to provide a principles-based approach to rules to facilitate broad compliance. To that end, the NAI believes that the rules should be flexible and technology neutral, and they should therefore refrain from developing prescriptive technical guidelines for any particular platform or technology.

C. ***A "technical specification" suggests the need to engage with the technical details of products and services. How can the Department best provide these details while leaving an opportunity for future technical innovation?***

We appreciate the goal of promoting continued technical innovation, as well as your objective to develop rules that enable this goal. The NAI has long believed that privacy laws and regulations should seek to remain technology neutral, in order to prevent the outcome of selecting "winners and losers" among the broader marketplace. Therefore, with respect to the reference to a "technical specification" we recommend that implementing regulations avoid the development or identification of a prescriptive technical standard while still providing minimum requirements for a qualifying

standard, such as sufficient information to determine geographic applicability or granularity of choice mapping to the law's opt-out intent. However, as part of the UOOM review process that we propose above, it would be helpful for the rules to provide a requirement that any signal activated by consumers is clearly communicated to businesses as a Colorado citizen's opt-out request, consistent with the opt-out rights established by the law, rather than a broader privacy signal that may not be consistently understood by consumers or businesses or be in conflict with other state laws.

D. ***The "rules must not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data." How should the rules elaborate on this requirement, if at all? Would a tool that is marketed for its privacy features suffice to satisfy this requirement? Would a privacy-focused version of a tool offered in multiple versions suffice?***

This question raises the most important considerations for effectively implementing UOOMs to the benefit of both consumers and businesses. Businesses that process personal data cannot be sure of the integrity of UOOMs if technology companies that serve as intermediaries are enabled to utilize default settings that seek to represent decisions about other businesses processing of personal information. While the NAI supports the goal of making it easier for consumers to utilize easy-to-use choice mechanisms, leaving it up to technology intermediaries to make such decisions that presume user preferences risks creating market imbalances driven by the limited number of companies that are in a position to control consumers' access to internet-based products and services.

The requirement in the CPA that seeks to prevent such intermediaries from unfairly disadvantaging other processors is consistent with the requirement for UOOMs to represent a consumer's affirmative choice. In considering these two parallel requirements, the OAG should be mindful of potential market externalities that may result from technology intermediaries that seek to make a proactive choice on behalf of consumers, supposedly with the best intentions of the consumer in mind.

According to a 2019 NAI survey, 60% of consumers prefer to have online content sponsored by advertising, rather than paying subscription fees for individual websites and apps.[1] The vast majority of this advertising is data-driven, utilizing consumer data to make marketing decisions that provide greater value to publishers and digital service providers. Therefore, on-by-default settings that seek to limit consumer data processing for these purposes broadly across all businesses, extends a singular conclusion and preference to all users of that technology, and therefore establishes a preference (or, alternatively, a significant disadvantage) for competing–data-driven–business models. This is particularly concerning in cases where the technology intermediaries stand to benefit from these "privacy" settings. This is true in the case of the two dominant web browser and mobile platforms that have adopted product changes in the name of promoting consumer privacy, but that also are often cited by businesses and policymakers as posing threats to competition across the digital media ecosystem.

As an example of this complex dynamic, Apple actively markets its technology products and services as privacy-friendly, but what is not widely recognized is that this marketing campaign is consistent with Apple's business model, which relies on substantial revenue derived from charging consumers

[1] Network Advertising Initiative, *NAI Consumer Survey on Privacy and Digital Advertising*, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/.

and other businesses fees for using their services or operating on their platforms, respectively.[2] Apple has also been increasing their use of first-party advertising. A choice by Apple to market a "privacy-centric" browser or mobile operating system is therefore entirely consistent with their objectives to increase revenues derived from fee-based apps and first-party advertising, rather than third-party ad-supported apps that comprise the majority of apps used by consumers today. This approach should be viewed by policymakers holistically, seeking to balance privacy objectives with the need to maintain a robust, competitive marketplace.

A company like Apple, with substantial market share across a range of IT products and services, is in a unique position to promote its own web browser and mobile operating system. Considering that, we urge the OAG to recognize that on-by-default privacy controls that seek to portray a consumer's choice should not be the basis or requiring legal compliance for businesses. Enabling technology intermediaries to determine, by default, consumer decisions about processing of consumers' data by other businesses risks creating a major market imbalance and further reduces competition in the marketplace for innovative, data-driven products and services.

This is not to say that products and services cannot, or should not, compete on the merits of protecting consumers. Rather, competition is a desired outcome. To best achieve both consumer protection and healthy competition, policymakers, in crafting policies regarding collection and processing of consumer data, should be particularly mindful of these marketplace realities and should resist the opportunities for any market player who looks to impose legal compliance obligations on other businesses.

The regulations can play a valuable role in encouraging businesses to honor opt-out preference signals by ensuring that they reflect actual consumer choices, while also ensuring that these tools are readily accessible for consumers who wish to utilize them. The process highlighted above for review and approval of recognized UOOMs is a critical step to achieving these goals, as it would provide for an open, fair and consistent method of evaluating the terms through which UOOMs are offered and deployed by consumers.

E. ***The "rules must adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States." What other similar mechanisms have been required?***

The NAI strongly supports this objective established by the CPA to help provide for consistent consumer protections and experiences, as well as consistent and streamlined compliance requirements for businesses that operate across the United States. Similar legal requirements for businesses to comply with UOOMs have been established in California and Connecticut, though each of these laws have varying approaches to the potential implementation of automated signals. The NAI encourages the OAG to work collaboratively with other state regulators to seek harmonization to the greatest extent possible, while also championing the strong marketplace protections put in place by the CPA.

[2] Apple's service business, which includes revenues from its advertising (and specifically App Store search ads) grew by 24% in the 2021 fiscal year, for a record $19.5 billion in revenue. Such growth has been possible in part because of Apple's App Tracking Transparency privacy changes, which forced advertisers running mobile app ads to recalibrate and shift spending to the App Store—where Apple can directly collect money. *See* Nina Goetzen, *Apple Ad Revenues Skyrocket Amid Its Privacy Changes*, INSIDER INTELLIGENCE (Jan. 31, 2022), https://www.emarketer.com/content/apple-ad-revenues-skyrocket-amid-its-privacy-changes/.

F. ***The "rules must permit the controller to accurately authenticate the consumer as a resident of this state." What kind of mechanisms should our rules acknowledge to satisfy this requirement?***

Authentication of consumers as residents of specific states is one of several areas where large platforms have an advantage in compliance due to the significant amount of data they collect on each of their users, and their ability to implement new controls for consumers to efficiently verify state residence if they choose. NAI member ad-tech companies, as well as smaller publishers and advertisers, often cannot easily determine a consumer's state of residence. Therefore, it is important that the implementing regulations recognize this model and the challenges it presents for compliance with CPA and similar state laws. As with various other technical elements that the CPA and implementing regulations touch on, it is important that the regulations not be overly prescriptive with respect to specific technologies or practices.

For digital advertising uses of personal information, it is often quite difficult for businesses to know whether a particular consumer is a resident of Colorado or other states. The most common practice for businesses in responding to the existing state-specific requirements established by the California Consumer Privacy Act ("CCPA") is to rely on IP addresses, which often are not representative of a household's residency. The regulations should allow the processing of IP addresses and recognize the legitimate implementation of more accurate tools or mechanisms that rely on limited uses of personal data necessary to perform state-residence authentication.

G. ***Other recommendations regarding application of UOOMs***

The NAI makes two additional recommendations for implementing regulations to provide benefits to both consumers and businesses that honor these mechanisms.

First, clarify that application of choices conveyed via UOOMs apply only to the browser or device from which such choice is made for as long as the signal continues to be present in the browser or device. In some cases an UOOM signal could be applied more broadly to a consumer, if that consumer readily identifiable to the business without the business needing to combine or request additional data that they would not otherwise do. The regulations should clarify that businesses are neither required to collect additional data from consumers to apply the opt out more broadly, nor require steps to tie pseudonymous identifiers to known consumers in cases where they do not already perform such practices.

Second, the regulations should clarify how a business may be able to prompt a user to disregard or override a signal, for instance, in cases where that business has obtained an opt-in consent to share the consumer's data in accordance with clear terms provided by the business to the consumer. These circumstances will be very common as more publishers and advertisers seek opt-in consent to collect and share consumer data for advertising and marketing, among other purposes. Businesses need an effective opportunity to reconcile these conflicting signals, and this can be done efficiently and fairly.

III. Audit

The OAG should ensure companies subject to audits are permitted to provide their own annual audit completed by a qualified and independent auditor. The NAI believes that processors are best suited to select auditors, and so the auditor selection process should be done by the processor with the controller's consent. Many processors have retained the services of auditors already, and have established business relationships and familiarity with the processors' individual business practices.

IV. Consent and Dark Patterns

The CPA requires consent when processing certain information, such as sensitive data or the personal data concerning a known child.[3] *Consent* means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, and cannot be obtained through the use of dark patterns.[4] A dark pattern is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.[5]

The NAI's industry-leading self-regulatory program was founded with the mission to promote transparency and user choice, as well as establishing use limitations to protect consumers from unexpected and harmful outcomes. The NAI has long promoted—and even required through our Code and self-regulatory program—notice and choice interfaces that are presented to consumers regarding their data collection that should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain elections. In our 2020 Code of Conduct the NAI developed an industry-leading requirement, along with detailed guidance, that directs companies seeking the collection of consumer location data and other sensitive data to present clear and meaningful disclosures about the sharing and uses of the data for advertising and marketing purposes in conjunction with obtaining a user's consent.[6]

As industry norms and legal obligations change, the NAI published a resource on Best Practices for User Choice and Accountability in April 2022.[7] The NAI developed these best practices in consultation with member companies after surveying state law and Federal Trade Commission ("FTC") enforcement actions. The resource represents an effort to illustrate how compliance with the NAI Code positions member companies to be compliant with state and federal legal obligations as well. The below answers draw significantly from the NAI's Best Practices.

A. *What is a "clear, affirmative act?" What should be required to create "freely given," "specific," or "unambiguous" consent? What constitutes "informed" consent?*

The NAI Code does not define *consent* on its own, but it does offer guidance on opt-in consent: an affirmative action taken by a user that manifests the intent to opt-in to an activity described in a clear and conspicuous notice.[8] In general, the more sensitive the data collected is, the more disclosure the Code requires.[9] In providing our aforementioned Best Practices, the NAI suggests the following factors should be considered when designing clear user choice interfaces:

- Clearly include all material terms or conditions when obtaining consumer consent.

---

[3] COLO. REV. STAT. § 6-1-1308(7) (2022).

[4] COLO. REV. STAT. § 6-1-1303(5) (2022).

[5] COLO. REV. STAT. § 6-1-1303(9) (2022).

[6] *See Guidance for NAI Members: Opt-In Consent*, NETWORK ADVERTISING INITIATIVE (2019), https://thenai.org/wp-content/uploads/2021/07/nai_optinconsent-guidance19.pdf.

[7] *See Best Practices for User Choice and Transparency*, NETWORK ADVERTISING INITIATIVE (2022), https://thenai.org/wp-content/uploads/2022/04/NAI-Dark-Patterns-Final-1.pdf.

[8] THE NETWORK ADVERTISING INITIATIVE, 2020 Code of Conduct (hereinafter "NAI Code") § I.I (2020).

[9] The NAI Code's definition of "sensitive information" includes Social Security numbers, insurance plan or financial account numbers, information about any past, present, or potential future health or medical conditions or treatment, information and inferences about sensitive health or medical conditions or treatment, and information and inferences about a user's sexual orientation. NAI Code § I.O.

- State terms and conditions about not only the collection of data but its use and sharing in an easily understandable way, not likely to deceive consumers.
- Visually display choices in a way that clearly presents options and alternatives.
- Avoid opt-out processes that are onerous or that prompt users to fill out a time-consuming form.

The NAI encourages its member companies to consider including concise language in notice statements that avoids double negatives, and fully disclosing all information about the company's policies and personal data collection practices and all material information. For choice options presented to consumers, the NAI encourages its member companies to avoid pressuring language that could potentially manipulate consumers and avoid limitations with those choice mechanisms.

In drawing these conclusions and recommendations, the NAI carefully reviewed enforcement actions from the FTC over the last decade. While the FTC's definition of unfair or deceptive acts or practices is capacious, the NAI believes these best practices create clarity for consumers while ensuring consumer choice is truly informed and freely given.

B. *Are there specific frameworks, guidance documents, or court decisions from similar legal regimes which help articulate these standards for consent?*

In developing its own best practices for user choice and transparency, the NAI looked to the FTC enforcement actions in order to determine what could constitute a best practice. As the federal administrative body that oversees consumer protection, the FTC has produced a body of enforcement actions, guidance, and rules that should guide the OAG in how it defines and regulates consent and dark patterns. In particular, the OAG should be mindful of the FTC's standards and guidelines regarding deceptive acts or practices, and whether any omissions or misrepresentations are material. Under well-established FTC standards, an act or practice is deceptive if it (1) is *likely* to mislead the consumer; (2) is one a *reasonable* consumer would consider misleading; and (3) is a *material* misrepresentation.[10] For a misrepresentation to be material, it must be one that is likely to affect a consumer's choice or conduct regarding a product.[11]

These are practices and regulations businesses in Colorado—and the entire United States—have been adhering to for decades. Businesses are familiar with the requirements and have modeled their best practices around them. Importantly, in recent years the FTC has considered dark patterns to be an example of a deceptive act or practice and has been pursuing enforcement actions accordingly.[12] By following the FTC's standards, the OAG can ensure its regulations are consistent with federal law.

C. *What standards or principles would best guide design choice to help avoid the inadvertent use of dark patterns?*

While there is no "one size fits all" approach to defining a dark pattern, the NAI has recommended to its member companies the following in considering design choices for consumer opt outs:

- Avoid confusing sentence structure.

---

[10] Letter from James C. Miller, Chairman, Federal Trade Commission, to the Hon. John D. Dingell, Member of Congress (Oct. 14, 1983) (https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

[11] *Id.*

[12] *See, e.g., In re Zoom, Inc.*, F.T.C. No. C-4731 (2021) (complaint).

- Ensure the opt out link is on the same page as the accept button.
- Ensure that any toggles or sliders clearly explain which selection results in which outcome.
- Ensure just-in-time-notices are clear and distinct.
- Avoid inferring a user's choice or consent based on closing a pop-up window.
- Avoid displaying a custom message that mirrors the functionality of a system alert.
- Avoid designs or techniques that may be blocked by standard browser settings.
- Use notice/choice font sizes that are readable to a reasonable standard and consistent with other site or page content; use font colors that contrast from the respective background of the page and/or respective action buttons.
- Notify consumers of the ability to change their selection and how to do so.

D. *Should the rules outline specific types of dark patterns which are prohibited?*

The OAG should be mindful of the positions taken by the FTC and the State of California, which have not taken a prescriptive approach to defining dark patterns or how choices should be offered. Instead, the office should take a totality-of-the-circumstances approach, rather than seeking to develop or prohibit specific user interfaces. Ultimately, what could constitute a dark pattern in one circumstance, such as a multi-click interface on a website, could actually serve consumers more effectively if offered on small screen devices that ease consumer choice through clear interfaces.

V. Guidance on Data Protection Assessments

The NAI supports the requirement for businesses that process personal information to conduct regular cybersecurity audits and data privacy risk assessments. These risk assessments are also required by new privacy laws in California, Virginia, and Connecticut—commonly referred to as Data Protection Assessments ("DPAs")—and are essential for responsible data processing that minimizes risk posed by the collection and processing of personal information.

The NAI's long-standing Code and self-regulatory program predate both these legal requirements and those established in Europe under Article 35 of the European General Data Protection Regulation ("GDPR"). The Code is in essence a program to identify and minimize privacy risks surrounding the collection and use of consumer data for digital advertising purposes. The NAI's compliance team actively works with companies to assess practices, and as these practices evolve and new privacy risks are identified, we regularly update our Code and associated guidance documents, raising the bar to ensure that NAI members are upholding the highest standards among industry.[13] In response to the new state legal requirements for risk assessments around various types of data and practices, the NAI has begun a process of mapping the requirements to digital advertising practices, with the goal to help companies tailor their own assessments building from core NAI compliance requirements as the foundation.

These new state requirements for risk assessments will ultimately help expand heightened privacy efforts, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. However, a set of disparate requirements across multiple states threatens to create an environment where businesses are overwhelmed in their efforts to comply, with no discernable privacy benefit to consumers.

---

[13] *See* NETWORK ADVERTISING INITIATIVE, 2020 ANNUAL REPORT (2020), https://www.networkadvertising.org/sites/default/files/nai_annualreport-20_nolivetype_final.pdf; NETWORK ADVERTISING INITIATIVE, 2019 ANNUAL REPORT (2019), https://www.networkadvertising.org/sites/default/files/nai_annualreport_19_no-live_type_final.pdf.

Therefore, the NAI urges the OAG to develop and implement regulations that seek to harmonize, to the greatest extent possible, with the other state laws, and clarify that a company need not create a Colorado-specific data protection assessment, provided that the pre-existing assessment meets Colorado substantive requirements. The NAI supports the goal for businesses to perform these risk assessments, but we are concerned about the creation of an environment where businesses need to perform multiple assessments, or to tailor their assessments specifically to meet differing state legal requirements.

A. *In what circumstances should the Department request a DPA? How much and what type of guidance should the rules provide with respect to form and content of DPAs?*

The CPA requires that a controller "shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities."[14]

The NAI supports the CPA's approach to DPAs, which includes maintaining the confidentiality and attorney-client privilege of such records as well as ensuring such records are available to regulators upon request but not subject to public disclosure laws standard.[15] This approach will maintain the integrity of such risk mitigation practices.

Each organization may have its own approach to data governance and development of appropriate records. Therefore, the NAI encourages the OAG to clarify essential content but not be overly prescriptive on form or specific content. This is an essential step to ensure DPAs are not duplicative. Where some external standards may provide efficiencies for larger multinational organizations, the NAI would recommend that such standards could be an accepted alternative DPA but not required, so as to avoid being overly burdensome for smaller companies that may not already be subject to such requirements. As many standards may change or evolve over time the NAI would recommend stipulating to other legal standards such as those developed by the FTC.

In establishing criteria for when DPA are required, the Attorney General should seek heightened risk triggers that address real and quantifiable harms to consumers. While unfair treatment is one such statutory trigger, it is unclear what other "substantial injury" is covered by the CPA. The OAG should carefully evaluate other potential triggers that are not tied to unfair acts or practices and seek input on these during the rulemaking process.

B. *What information should DPAs contain with respect to processing for the purpose of profiling?*

With respect to DPAs related to profiling, the NAI would recommend that such analysis be focused on types of use and harm to consumers to best protect consumers. For example, the NAI Code prohibits marketing information to be used for employment eligibility, credit eligibility, healthcare eligibility, insurance eligibility, underwriting and pricing, tenancy eligibility and education admissions. Identifying if profiling data is used to make eligibility purposes may be a helpful distinction to assess the risk and harms of a profiling activity.

[14] COLO. REV. STAT. § 6-1-1309 (2022).

[15] COLO. REV. STAT. § 6-1-1309(4) (2022).

C. *The CPA allows for a single data protection assessment to address "a comparable set of processing operations that include similar activities." What makes processing operations comparable? What makes activities similar?*

In regard to the CPA allowance for a single Data Protection Assessment to address "a comparable set of processing operations that include similar activities," the NAI recommends the method of collection, data points collected, and purpose of collection as criteria to determine similar activities.

The NAI also encourages the OAG to clarify that the requirement to complete DPAs shall be required for activities conducted after July 1, 2023. This is our interpretation of the intent of the CPA, but additional clarity would be helpful for companies to ensure effective compliance. Further, providing for a six-month grace period following finalization of implementing regulations would be most effective to enable businesses to tailor DPAs to the forms and functions required by the regulations.

VI. Consumer Right to Opt-Out from Targeted Advertising and the Sale of Personal Data

A. *The right to opt-out of targeting, sale, and profiling should include specific exceptions for reporting, measurement, and legitimate business purposes.*

The NAI recommends that the OAG clarify in implementing regulations that the exception explicitly provided in the definition of Targeted Advertising for measurement and attribution also applies to the broader opt-out requirements for the sale of personal data and profiling. Specifically, the CPA provides "[a] consumer has the right to opt-out of the processing of personal data concerning the consumer for purposes of: Targeted Advertising; [t]he sale of personal data; or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[16] The CPA's definition of Targeted Advertising notably excludes "processing personal data solely for measuring or reporting advertising performance, reach, or frequency." While we believe it is the goal of the CPA, it does not specifically provide the same practical exclusion in the definition of the definition of sale or profiling.

The NAI considers Ad Delivery and Reporting to be distinct from Tailored Advertising activities, particularly the use of this data for drawing inferences or creating user profiles.[17] Given that the CPA clearly recognizes the importance of this information for statistical analysis, frequency reporting, and other valuable business functions by creating an explicit exception within the definition of Targeted Advertising, it seems practical that the regulations modify the consumer's right to opt-out to clarify that the exception for measuring and reporting applies to sales and profiling, in addition to targeted advertising.

VII. Consumer Right of Access

The NAI supports a consumer's right to access their personal data, as authorized by the CPA.[18] The NAI urges the OAG to be mindful of two key issues in promulgating and implementing regulations around the right to access: the risks associated with releasing personal data to third parties purporting to make access requests on behalf of individual or multiple consumers, and how service providers should respond to access requests.

---

[16] COLO. REV. STAT. § 6-1-1306(1)(a)(I).

[17] NAI Code § I.A; *see also* https://thenai.org/glossary/ad-delivery-and-reporting-adr/.

[18] COLO. REV. STAT. § 6-1-1306(1)(b) (2022).

The CPA permits controllers to refrain from complying with a request to access if the controller is unable to authenticate the request using commercially reasonable efforts.[19] In promulgating regulations the OAG should be mindful of the need for businesses to exercise caution when access requests come from third parties purporting to act as an agent on behalf of a consumer or groups of consumers. Controllers must have flexibility to rigorously authenticate such requests to ensure that personal data is not being disclosed to bad faith actors. Additionally, the OAG should take special care in addressing how service providers–as opposed to controllers, as defined by Colorado law–respond to requests to access.

VIII. Enforcement

A. *Maintain a 30-day cure period for businesses' first offense when demonstrating a reasonable effort to comply.*

The NAI appreciates the authors of the CPA including a 60-day cure period, recognizing the challenges businesses are likely to have coming into compliance with the Act, and seeking to provide for leniency in enforcement. However, the authors of the CPA also established a sunset for this provision after two years. The NAI interprets this sunset provision to reflect the recognition that compliance with the CPA will become easier after this period, and to prevent companies from not making efforts to comply until enforcement notices. However, while the NAI recognizes and supports the goal of ceasing enforcement leniency for companies that do not make reasonable efforts to comply with the Act after two years, a reasonable cure period provides a valuable tool for companies that take reasonable efforts to comply with the Act, enabling well-intentioned companies from being penalized, particularly for first-time offenses.

The NAI therefore recommends that the OAG utilize its enforcement discretion to provide for a reasonable cure period after January 1, 2025, with a particular business, particularly in cases where the business has demonstrated a reasonable attempt to comply with the CPA and implementing regulations and is not a repeat offender.

Specifically, the Connecticut Data Privacy Act ("CTDPA"), provides detailed examples of where the OAG could choose to utilize a cure period, post sunset.[20] The NAI recommends the OAG establish in rulemaking the intent to follow the approach found in the CTDPA:

> *(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider: (1) The number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; and (6) whether such alleged violation was likely caused by human or technical error.*[21]

The NAI believes that utilization of Connecticut's language for a cure period, post sunset, will strengthen Colorado's implementation regulations and promote consistent interpretations of data privacy laws to allow for harmonized regulations across the states.

IX. Duties of Controllers

---

[19] COLO. REV. STAT. § 6-1-1306(2)(d) (2022).

[20] Connecticut Data Privacy Act ("CTDPA"), S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022).

[21] *Id.* § 11(c).

The NAI appreciates the recognition by the CPA of the value of consumers' personal data in providing for enhanced products and services. As established under the CPA, controllers are explicitly permitted to provide for differing prices and levels of service, dependent on a consumer's voluntary participation in such an arrangement.[22] However, while the CPA recognizes the essential needs of businesses to offer varying levels of products and services, and to provide premium services for a fee, the Act does not sufficiently recognize that many content publishers and digital service providers offer their content and services on the basis of data-driven advertising and marketing services. In such cases, a company's provision of services is not free of cost to the company since they cannot monetize through advertising if consumers choose not to share their data.

Given the economic impact, a business should not be forced to provide a free service without a reasonable form of compensation. This concept of non-retaliation is also addressed by the CCPA, where the law provides for companies, in cases where a consumer has opted out, to charge a reasonable fee commensurate with the value of the consumer's data.[23] This approach allows for businesses to establish a reasonable fee in lieu of ad-supported provision, and it leaves for the business to determine on a case-by-case basis.

The NAI believes this is a practical approach which effectively balances the need to protect consumers from unreasonable demands for their personal data, while also providing many ad-supported businesses the opportunity to monetize their services in cases where they cannot perform data-driven advertising and marketing. Therefore, consistent with the spirit of the CPA, we urge the OAG to clarify that it is within a business' duty, particularly for web and app publishers, to charge a reasonable fee for services, related to the value of a consumer's data, if consumers choose not to share their data.

X. Conclusion

The NAI is grateful for the opportunity to comment on the Regulations for the CPA. If we can provide any additional information, or otherwise assist the OAG as it engages in the rulemaking process, please do not hesitate to contact Leigh Freund, President & CEO (leigh@thenai.org), or David LeDuc, Vice President, Public Policy (david@thenai.org).

*****

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

[22] COLO. REV. STAT. § 6-1-1308(1)(d)
[23] CAL. CIV. CODE § 1798.125(a)(2) (2022).