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

September 30, 2024

The Hon. Letitia James
Office of the New York State Attorney General
The Capitol
Albany, NY 12224

Submitted electronically via ChildDataProtection@ag.ny.gov

RE: Advanced Notice of Proposed Rulemaking on the NY Child Data Protection Act (CDPA)

Dear Attorney General James:

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide comments on the Office of the New York State Attorney General ("OAG") Advanced Notice of Proposed Rulemaking ("ANPRM") to assist the office in crafting rules to protect children's privacy pursuant to the New York Child Data Protection Act ("CDPA") (New York General Business Law § 899-ee *et seq.*). The NAI shares the OAG's goal of protecting children's privacy online, and appreciates the opportunity to provide more guidance and clarity for digital advertisers and other actors operating primarily online.

These comments provide an overview and an introduction to the NAI as well as our historical approach to protecting children's privacy while still allowing for websites and apps directed to children to fund themselves through advertising. In addition, we provide responses to questions in four key categories for OAG's consideration: (1) the definition of "primarily directed to minors," (2) the treatment of personal data, (3) permissible processing without consent, and (4) methods of obtaining parental consent. The NAI's goal is to harmonize disparate state and federal laws and regulations to provide clarity for digital advertisers seeking to comply with the law, while promoting a robust, ad-supported internet that keeps kids' data safe and prevents its misuse.

I. Introduction and Overview of the NAI

As a self-regulatory body, the NAI has been involved in developing higher standards and practices for digital advertisers, advancing privacy-protective policies that work for businesses and can be operationalized and adopted throughout the industry. The NAI has long supported enhanced safeguards for children's privacy online. In our 2020 Code of Conduct, we prohibited NAI members from creating advertising segments targeting children under the age of 16

without verified parental consent, a step further than current federal law goes.[1] Within the digital advertising ecosystem, NAI members (with a few exceptions) are distinct from publishers (the websites and apps that display advertisements) and consumer-facing brands (the companies that pay for advertisements).[2] Instead, NAI members provide the technology that facilitates the selection, delivery, and measurement of advertisements between publishers and brands. NAI members will therefore usually not be in the position of operating websites or other digital properties that are directed to children within the meaning of the definition under the Children's Online Privacy Protection Act ("COPPA") or the CDPA. They may in some instances be considered operators as the term is used in the CDPA–and in all instances will be impacted directly or indirectly by the requirements placed on operators.[3] Nonetheless, NAI member companies routinely assess the websites and apps they engage with in an effort to avoid collecting advertising data related to children, even when they do not know the age of a given user.

While the NAI is proud of its efforts and their demonstrable results, there are limitations inherent in the self-regulatory model. Public policies that apply seamlessly across the entire digital media industry are critical, particularly when it comes to protecting children. The NAI believes that heightened standards need to be applied evenly across the entire industry, rather than merely to those companies that voluntarily embrace higher standards.

Additionally, the effort by states to increase protections for children online beyond COPPA, which was enacted more than two decades ago, has created a patchwork of inconsistent requirements, particularly regarding minors and teenagers. As a result, uniform compliance is increasingly difficult for online advertisers. For instance, tailored advertising directed to teenagers is permissible in some states, but not others.[4]

The NAI has been a leading proponent of an updated federal privacy law that will create a national standard for the protection of consumer data, including an expansion on protections for children's data. The NAI is pleased that Congress has recently made significant progress towards enacting additional protections for children's data.[5] Regardless of whether Congress enacts a uniform national standard for children's privacy, the NAI is committed to working with federal and state policymakers to enact and implement a consistent set of protections, and we

---

[1] 15 U.S.C. § 6501(1) (2024) (defining "child" as an individual under the age of 13).
[2] The NAI's member list is public, and our members range in size from smaller startups to some of the largest tech companies in the world. While some of the larger members have parts of their businesses that function as a publisher, their NAI membership is limited to their company's ad tech business lines.
[3] *See* N.Y. Gen. Bus. Law § 899-ee(3) (2024).
[4] *Compare* Cal. Civ. Code § 1798.120(c)(1) (2024) (permitting cross-context behavioral advertising with affirmative consumer consent) *with* Md. Code Ann. § 14-4607(A)(4) (2024) (prohibiting the processing of personal data for targeted advertising when the controller knows or should know a consumer is under the age of 18).
[5] Press Release, Network Advertising Initiative, NAI Applauds House Committee on Passage of Strong Children's Privacy Legislation (Sept. 18, 2024) (https://thenai.org/press/nai-applauds-house-committee-on-passage-of-strong-childrens-privacy-legislation/); Press Release, Network Advertising Initiative, NAI Applauds Senate Passage of Strong Children's Privacy Legislation (July 30, 2024) (https://thenai.org/press/nai-applauds-senates-passage-of-strong-childrens-privacy-legislation/).

applaud New York's efforts to develop regulations that seek to align implementation of the CDPA with COPPA, while also being mindful of other disparate state requirements.

II. Comments to Specific Proposals

The comments below reflect our assessment of the OAG's questions on areas specific to digital advertisers.

A. CDPA's Definition of "Primarily Directed to Minors"

The CDPA differs from COPPA and most state privacy laws because it contains provisions about websites or apps primarily directed to minors.[6] The Federal Trade Commission ("FTC" or "Commission") has, historically, used its authority under COPPA to issue regulations allowing companies to know with reasonable certainty which websites or online services are considered directed to children.[7] The CDPA's definition differs from COPPA's definition because it is applied more broadly to cover "*minors"* including all users under the age of 18, whereas COPPA's definition applies only to children under the age of 13. This distinction creates inconsistency for businesses in determining the audience to which their sites and services are directed.

i. Factors for Websites Directed to Children

The NAI encourages the OAG to clarify in its regulations that the CDPA's determination of sites and services directed to children will be consistent with the approach created by the FTC under the COPPA Rule and implementing regulations; a multi-factor, "totality of the circumstances" test that relies on a number of factors, where no one factor is dispositive.[8]

The current COPPA Rule provides an established precedent that has proven workable for regulators and operators alike for decades. Deviating from this precedent would not only create unnecessary confusion for operators without any clear benefit, but it would also likely present a conflicting set of requirements that would be preempted by COPPA.

ii. Factors for Websites Directed to Teenagers/Minors

As noted above, New York is unique in that no other jurisdiction in the United States is considering the determination of specific factors to assess if websites or apps are primarily directed to teenagers. The NAI therefore supports the OAG adopting a modified set of factors when determining whether a website or online service is primarily directed to *teenagers* (*i.e.*,

---

[6] *Compare* N.Y. GEN. BUS. LAW § 899-ee(6) (definition of primarily directed to minors) *with* 16 C.F.R. § 312.2 (2024) (definition of web site or online service directed to children). The CDPA is also unique in that it refers to covered sites and services as "*primarily* directed to minors," while COPPA only refers to websites and services "directed to children" (emphasis added). Nonetheless, the NAI interprets both provisions to be consistent in their intent, if not their wording.

[7] *See* 16 C.F.R. § 312.2 (2024) (definition of web site or online service directed to children).

[8] *Id.*

users between the ages of 13 and 17), than when determining whether a website or online service is primarily directed to *children* (*i.e.*, users under the age of 13).

There is a substantial difference between sites and services directed to children under the age of 13, and those intended for teenagers. However, there is substantially less difference between what interests a covered 17-year-old and a non-covered individual between 18 and young adulthood. Many of the factors the FTC uses in the COPPA rule could potentially be more broadly applied to teenagers, but some factors are inappropriate and could potentially lead to general audience websites being considered "directed to teenagers" when they did not specifically direct their content to teenagers. This could impair those websites' ability to continue operations.

The NAI therefore supports a more limited set of factors when assessing whether or not a website or app is directed to teenagers or minors. Importantly, these factors continue to mirror those from the COPPA Rule, to promote consistency and ease of compliance, and all remain within the control of individual operators. These factors include: subject matter (provided that the subject matter is specific to teenagers and not general audience content that might appeal to teens as well as adults); use of teenager-oriented activities and incentives (provided that the subject matter is specific to teenagers and not a general audience); age of models; presence of teenage celebrities[9]; and language or other characteristics of the website or app that indicate it is directed to teenagers.

iii. Websites and Apps with Incidental Appeal to Minors

As noted, the CDPA covers websites and apps that are *primarily* directed to minors. This wording indicates that there is a clear distinction between these and the separate, distinct websites and apps that are only *incidentally* directed to minors. The NAI recommends that the implementing regulations clarify the intent of the CDPA, consistent with the intent of COPPA, to avoid application to sites and services merely with incidental or secondary appeal to minors. Websites or online services that do *not* have an intended audience of children or teenagers should not be covered by the CDPA.

For instance, an article on a general audience website, such as CNN.com, about Taylor Swift's latest concert tour, could potentially be appealing to children, but children are not CNN.com's intended audience. From a compliance perspective, it becomes difficult (if not impossible) to anticipate and manage every instance of when children *might* be attracted to content on a website or app. If a digital media platform has a vertical that appeals to children but the platform overall is for a general audience, the presence of that children's-oriented vertical should not make the entire platform directed to children.

[9] Here, we limit this factor when compared to celebrities that appeal to children in part because there is more overlap with celebrity appeal to teenagers and adults. Celebrities like LeBron James or Taylor Swift have significant crossover appeal with adults, while there are fewer child-oriented celebrities that also appeal to adults.

This approach is consistent with the statutory language in the CDPA, that is limited to websites or online services *targeted to minors*, not those that are *incidentally* (but not purposefully) appealing to children or teenagers, or have a significant number of child or teen users despite not specifically targeting these audiences. This is also consistent with the COPPA Rule's analysis focusing on "competent and reliable empirical evidence" regarding audience composition and evidence regarding the intended audience.[10]

B. Treatment of Personal Data

The ANPRM asks about how regulations concerning the definition of personal data should account for anonymized or de-identified data that could potentially still be re-linked to specific individuals. The CDPA defines personal data as "any data that identifies or could reasonably be linked, directly or indirectly, with a specific natural person or device."[11]

Nearly twenty states have passed comprehensive privacy laws that explicitly exempt de-identified data from their varying definitions of "personal data."[12] The CDPA is an outlier by not similarly explicitly exempting de-identified data from its definition of personal data. To better ensure the CDPA's treatment of personal data accounts for the different risks to minors' privacy associated with different types of data and in line with widely established data privacy principles in the United States, the implementing regulations should specify that personal data does not include de-identified data, and it should also provide guidance on what is considered an acceptable standard for when data is de-identified, taking into considerations what other jurisdictions have determined and what is technologically feasible for operators within the state of New York to adopt.

A subset of data that is often included in the definition of personal data under federal and state privacy laws includes pseudonymous identifiers–identifiers that can be used to recognize a consumer over time and across different services, such as Internet Protocol ("IP") addresses, cookies, beacons, pixel tags, or mobile advertising identifiers. As a general matter, under state privacy laws, data can only be considered pseudonymous if it is not reasonably capable of being attributed to specific individuals without the use of additional information.[13]

COPPA allows for certain uses of pseudonymous data when processing personal information in order for websites and apps to function properly, through its exemptions for the support for internal operations of websites and online services.[14] The NAI recommends that the OAG recognizes the role of pseudonymous data in regulation and permit limited processing provided

[10] *See* 16 C.F.R. § 312.2 (2024) (definition of web site or online service directed to children).
[11] N.Y. Gen. Bus. Law § 899-ee(4).
[12] *See*, e.g., Cal. Civ. Code § 1798.140(v)(3) ("'Personal information' does not include consumer information that is deidentified or aggregate consumer information"); Colo. Rev. Stat. § 6-1-1303(17)(b) ("'Personal data'... does not include de-identified data or publicly available information"); Va. Code Ann. § 59.1-575 (2024) ("'Personal data' does not include de-identified or publicly available information").
[13] *See, e.g.,* Colo. Rev. Stat. § 6-1-1303(22) (2024) (definition of pseudonymous data).
[14] 16 C.F.R. 312.2 (definition of "support for the internal operations of the web site or online service").

that certain technical and legal safeguards are in place, as discussed in greater detail below regarding Permissible Processing.

C. Permissible Processing and Contextual Advertising

The ANPRM asks about permissible processing, which the CDPA defines as processing that is strictly necessary for a certain enumerated list of activities.[15] This is an important question, and the NAI appreciates the OAG's further consideration of the application of the CDPA in this area.

As noted above, current federal regulations under COPPA permit the collection and processing of persistent identifiers for a limited set of advertising practices that are essential to child-directed websites and services, but that do not entail retention of children's personal information or use in targeting advertisements.[16] COPPA's internal operations exception also provides for the use of these identifiers to measure and cap the frequency of ad serving on a specific device, as well as enabling necessary security measures, such as preventing ad click-fraud. In its notice of proposed rulemaking to update the COPPA Rule, the FTC recently reaffirmed the interpretation of COPPA as permitting contextual advertising and ad measurement as internal operations.[17]

Further, legislation passed by the U.S. Senate and the House Energy and Commerce Committee recently to strengthen COPPA and extend its coverage to teens addresses this issue.[18] Specifically, the legislation would amend the COPPA statute to clarify those functions permissible as processing for internal business operations, including contextual advertising and related measurement.

However, the CDPA's enumerated list of permitted permissible practices explicitly states that activities related to marketing and advertising are not to be considered strictly necessary for conducting internal business operations.[19] As this approach conflicts with COPPA today, and would also conflict with legislation updating COPPA in this Congress, the NAI recommends that the OAG takes a similar approach to the FTC, developing implementing regulations that allow for these limited advertising purposes. In order to accomplish this while also prohibiting invasive collection and processing of children's data, the NAI also recommends that the OAG define "ad serving and measurement" in its regulations, in order to provide clarity and guidance for digital advertisers of what is not included. The NAI proposes the following definition:

---

[15] *See* N.Y. GEN. BUS. LAW § 899-ff(1)(b).
[16] See 16 C.F.R. § 312.2 (definition of support for the internal operations of the website or online service).
[17] Federal Trade Commission, Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034, 2043 (proposed Jan. 11, 2024).
[18] Kids Online Safety and Privacy Act, 118th Cong. (2024) (amended by S. Amdt. 7891); House Energy and Commerce Committee, Amendment in the Nature of a Substitute to H.R. 7890, 118th Cong. (2024) (https://docs.house.gov/meetings/IF/IF00/20240918/117432/BILLS-118-HR7890-A000370-Amdt-7-U6.pdf).
[19] *See* N.Y. GEN. BUS. LAW § 899-ff(2)(b).

> "Ad serving and measurement means processing covered data to serve an ad on a website or app, and for the purpose of measurement and reporting of frequency, and performance of advertising, but not for purposes of targeted advertising or the development of user profiles, including, but not limited to: statistical reporting, traffic analysis, analytics, optimization of ad placement; ad performance, reach, and frequency metrics (including frequency capping); sequencing of advertising creatives; billing; and logging the number and type of ads served on a particular day to a particular website, application, or device."

If implementation of the CDPA ultimately does not provide a limited exception for ad serving and measurement, as well as contextual advertising on sites and services directed to children and minors, this would deprive those sites and apps of needed revenue, limiting the ability to prevent necessary security functions, such as ad verification and click-fraud prevention. Again, we appreciate the OAG's careful consideration of this issue, and how the CDPA interacts with other relevant policy frameworks and existing practices.

D. User Signals and Consent

In this section we address several issues related to the application of user signals and "flags" under the CDPA. These terms are used interchangeably in the statute, but user signals and flags used by sites and ad-tech providers are different.

i. User Signals

The CDPA requires operators to treat users as covered minors if the user's device signals that the user is a minor through a browser plugin, privacy or device setting, or another mechanism.[20] This approach is similar to multiple state privacy laws that provide for the use of a technical signal to send consumer opt-out choices to businesses administered through browsers or other connected devices.[21] However, this approach would extend the application of a user signaling mechanism to also provide for transmission information about the user's age, not their opt-out preferences.

In general, the NAI supports the use of easy-to-use mechanisms for consumers to exercise control over the use of their data, and the alignment of these signals with legal requirements. We believe the adoption of these types of signals under effective legal guidelines can be a useful tool for consumers and businesses alike, and could potentially help to protect the personal data of children and minors.

However, such signals have not yet been adapted for purposes of minor's privacy, and the NAI is concerned about the CDPA's approach to signaling insofar as it would involve broadcasting to all websites that a user is a child or a minor. This approach could lead to unintended and harmful

[20] *Id.* § 899-ii(1).
[21] See, e.g., COLO. REV. STAT. § 6-1-1306(1)(a)(IV)(A).

results, such as enabling malicious sites and services to identify children and target them for illegal or harmful purposes. Additionally, signals that collect and share a user's age require collecting and sharing more user data than is necessary and could conflict with the data minimization goals and legal restrictions under certain laws.

The ANPRM asks what standards regulations should set for acceptable device communications or signals that a user is a minor or consents or refuses to consent to data processing. This is a very important question, as there are no such signals available today to achieve this goal, and, as noted above, there are serious risks associated with adopting any such signal. The most commonly utilized universal opt-out mechanism in use today is the Global Privacy Control ("GPC"), which was recently recognized as a valid signaling mechanism by Colorado and California.[22] However, the GPC technical specification does not provide for communicating additional information about the user, such as their age, as provided for by the CDPA, or their state of residency. And, as noted above, GPC would put users at risk if it did include information about their age. Further, GPC is intended to indicate a user's preference to opt out of sales, sharing, and use of personal data targeted advertising, not to limit all processing of personal data that isn't "strictly necessary." Therefore, while the GPC is the most widely recognized universal opt-out mechanism in use today, it is not equipped to address the requirements under the CDPA.

Given that the CDPA provides little detail on how these signals should work, criteria by which they should be administered, or how they can address risks posed to minor users, the NAI recommends that the OAG apply a process and set of criteria similar to the rigorous process and criteria established by the Colorado Privacy Act ("CPA") and Colorado Department of Law to recognize valid user signals under the CPA. That process was very thorough, including a call for proposals for qualifying universal opt-out mechanisms, and a review period by stakeholders to help evaluate a subset of proposals that were deemed to meet the requirements established by the CPA and implementing regulations.[23] In particular, Colorado required certain key safeguards in the development of such a signal, refusing, for example, a signal or mechanism that is a default setting on a browser or device, and not permitting manufacturers of such signals to unfairly disadvantage other businesses.[24] Colorado also established that they will continue to periodically review approved universal opt-out mechanisms to ensure their continued adherence to the CPA and established regulatory criteria.

The OAG should refrain from enforcing against CDPA's signal requirements while undertaking its process to recognize valid user signals; this will ensure that companies have the legal certainty they need to continue operations. The NAI remains committed to engaging with the OAG, as well as other policymakers and stakeholders, to promote implementation of and compliance with an effective provision of consumer signals.

---

[22] California Office of the Attorney General, *California Consumer Privacy Act FAQs*, (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa; Colorado Office of the Attorney General, *Universal Opt-Out Shortlist*, https://coag.gov/uoom.

[23] *See* Colo. Code Regs. § 904-3 Rule 5.07 (2024).

[24] *See* Colo. Code Regs. § 904-3 Rule 5.06 (2024).

ii. COPPA Flags and Consideration of Additional Advertising Flags for Minors

One signaling function that is used today in digital advertising is the deployment of "COPPA flags," an attribute of an advertising bid request that is part of the IAB TechLab's OpenRTB specification. The COPPA flag indicates that the bid request is associated with a child protected by COPPA.[25] These flags currently comply with federal COPPA requirements and therefore are only utilized on sites and services directed to children under 13. They do not indicate when a site or app would be directed to teenagers. However, the CDPA creates a new, separate age category of users, "minors," and it seeks to identify a new category of websites and services "directed to minors," so at a minimum these flags would need to be added to sites directed to teenagers.

Neither the CDPA nor the ANPRM make reference to this operational consideration. Instead the CDPA refers to the term "flag" as a signal directly from a user, as discussed above. If the implementation of the CDPA creates the need for companies to distinguish between sites and services directed to children from sites and services distinguished to teenagers, there would be a need for industry to develop a new standardized signal for sites and services directed to teenagers. Given that existing signaling functions are currently only used in the narrow context of digital advertising conducted through the Open Real-Time Bidding protocol, and were not designed with the requirements of the CDPA in mind, this would be a significant task with the potential for unintended consequences. This is an area the NAI is actively discussing with members and other stakeholders of the digital advertising industry, including publishers and advertisers.

While the use of COPPA flags, which are already in place, could provide a useful avenue for CDPA compliance, we encourage the OAG to proceed cautiously and to solicit specific inquiries about this method. Currently, here is no method of "aging out" of COPPA flags (*i.e.*, a flag cannot communicate when a user is 17 or when a user is 18), and given the CDPA's distinctions between children and teenagers, the OAG should determine how best to operationalize its requirements.

We welcome the opportunity to further discuss whether such an approach would be necessary in the implementation of the CDPA's new requirements, but we note that this technology is not readily available today and that existing signals and flags are ill-equipped to address the requirements of the CDPA and must address the risks associated with sharing additional user data and over-restricting access to content and services.

[25] Interactive Advertising Bureau, *Guide to Navigating COPPA*, (Oct. 2019),, https://www.iab.com/wp-content/uploads/2019/10/IAB_2019-10-09_Navigating-COPPA-Guide.pdf.

iii. Consent Mechanisms

The NAI encourages the OAG to align the CDPA regulations relating to consent with COPPA and the COPPA Rule. Additionally, for platforms that are directed to children or minors, the regulations should allow operators to empower parents and teens to provide consent through the use of control settings. This level of granularity would allow for age assurance, while also ensuring that older teenagers and adults are not prohibited from making choices they are legally entitled to make. These affirmative choices are in many cases the most effective and efficient means to impute consent from a parent or teen about their choices. For example, if a parent is able to change settings to allow for a child's data to be collected and processed by a site or service a child is interacting with directly, the decision to change the setting to permit such sharing should constitute consent. This is an approach that we have also proposed to the FTC in response to their COPPA Notice of Proposed Rulemaking published in December 2023.[26]

III. Conclusion

The NAI appreciates the opportunity to submit comments to the Commission on this important topic. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at leigh@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

*****

Respectfully Submitted,

Leigh Freund
President & CEO
The NAI

[26] Network Advertising Initiative, Comment Letter on Proposed Amendments to the Children's Online Privacy Protection Rule (Mar. 11, 2024), https://www.regulations.gov/comment/FTC-2024-0003-0235.