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

Submitted electronically via: https://www.regulations.gov/document/NTIA-2023-0008-0001

November 16, 2023

Stephanie Weiner
Chief Counsel
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Docket No. NTIA-2023-0008

Dear Ms. Weiner:

On behalf of the Network Advertising Initiative (NAI), thank you for the opportunity to provide comments on the National Telecommunications and Information Administration ("NTIA") Request for Comment ("RFC") on the initiative to protect youth mental health, safety, and privacy online.[1]

I. Introduction

The NAI appreciates the breadth of this RFC across the entire digital media ecosystem. While focusing most heavily on large social media and gaming platforms where there is substantial engagement among children and minors,[2] the RFC also explores the full range of digital platforms, including small and medium-sized apps and sites, as well as the range of e-commerce businesses that continue to drive U.S. economic growth. As the leading self-regulatory organization and trade association for digital advertising technology companies, the NAI's focus has historically been on the promotion of privacy-protective practices, with a particular focus on third-party collection and processing of consumer data to enable Tailored Advertising[3] and Ad

[1] National Telecommunications and Information Administration Initiative To Protect Youth Mental Health, Safety & Privacy Online, 88 Fed. Reg. 67733 (proposed Sept. 26, 2023).
[2] When we refer to children we mean individuals under the age of 13; when we refer to minors, we mean individuals under the age of 18.
[3] Within the context of the NAI's 2020 Code of Conduct, Tailored Advertising "is the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device." Network Advertising Initiative, 2020 NAI Code of Conduct (2020) [hereinafter "NAI Code"] § I.Q, https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf. This term is analogous to what many state laws define as "Targeted Advertising." *See, e.g.,* Va. Code Ann. § 59.1-575 (2023) (definition of "Targeted Advertising").

Delivery and Reporting.[4] Therefore, these comments do not seek to address all of the questions posed in the RFC; rather they focus more narrowly on these areas that are most relevant to the mission of NAI and our members.

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising technology companies. For over 20 years the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest industry standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust. The NAI Code of Conduct (the "NAI Code") has long promoted strong self-regulatory standards for its members and NAI membership requires annual privacy reviews by NAI staff attorneys.[5]

II. NAI-Led Efforts to Protect Children's Privacy

Like all other companies, NAI member companies must comply with the Children's Online Privacy Protection Act ("COPPA") (15 U.S.C. §§ 6501-6506), as well as multiple state privacy laws that put protections for children's data in place.[6] Because there are multiple state laws with varying requirements and restrictions, many NAI members take a "highest common denominator" approach and set their policies to comply with the strictest requirements.

Within the digital advertising ecosystem, NAI members (with a few exceptions) are distinct from publishers (the websites that display advertisements) and consumer-facing brands (the companies that pay for advertisements).[7] 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 established by the Federal Trade Commission ("FTC") in its COPPA rule (16 C.F.R. § 312.2). Nonetheless, NAI member companies routinely assess which 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.

---

[4] Within the context of the NAI 2020 Code of Conduct, Ad Delivery and Reporting is "separate and distinct from Tailored Advertising, and it refers to the collection or use of data about a browser or device for the purpose of delivering ads or providing advertising-related services." These services can include (but are not limited to) providing a specific advertisement based on a particular *type* of browser or device; statistical reporting; or ad performance, reach, and frequency metrics. NAI Code § I.A.

[5] *See generally* NAI Code, https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

[6] *See, e.g.,* Cal. Civ. Code § 1798.100 *et seq.* (2023); Colo. Rev. Stat. § 6-1-1301 *et seq.* (2023); Va. Code Ann. § 59.1-575 *et seq.* (2023). Many other states have passed laws in 2023 and many more may do so in 2024 and beyond.

[7] 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.

Further, companies adhering to the NAI Code of Conduct are prohibited from creating advertising segments intentionally targeting minors under the age of 16 without verifiable parental consent[8] and must contractually require unaffiliated parties to comply with the same requirement.[9] While self-regulation generally applies only to businesses that voluntarily adopt self-regulatory standards, these contractual obligations are designed to pass the limitations found in the NAI Code on to other businesses in the industry. Because the NAI represents some of the biggest and most critical players in digital advertising, this has helped set a standard for children's privacy in the ad-tech space, at a time when digital advertising was less regulated than it is today.

As a self-regulatory body, the NAI has been involved in developing higher standards and practices for digital advertisers that advance privacy-protective policies that actually work for businesses, and can be operationalized and adopted throughout the industry. While the NAI is proud of its efforts and their demonstrable results, there are limitations inherent in the self-regulatory model that increasingly require public policies to apply seamlessly across the entire digital media industry, particularly when it comes to protecting children. Therefore, the NAI has been a leading proponent for legislation to create a uniform national standard for protection of consumer data that is applied evenly across the entire industry, rather than merely those companies who embrace higher standards.

III. Key Policy Considerations

In considering new public policy solutions to better protect data of children and minors, there are two key areas that are central to tailored advertising that must be addressed effectively: (1) what criteria should be applied to assess when a business that collects or uses data is collecting data from a child or minor; and (2) how to assess when a website, app, or other online service is "directed to children." A related, but different, issue at the center of several new laws and legislative proposals at the state and federal levels address the mere likelihood of children or minors accessing websites or online services and the creation of broad obligations to prevent harmful outcomes to children or minors based on that likelihood. This approach to protecting the privacy of children and minors is problematic from both a legal and policy standpoint however, because it does not take the context of the website or app into account, and it could lead to efforts to apply restrictions across general purpose websites and apps that are not just impractical, but potentially are unconstitutional. For example, the Kids Online Safety Act ("KOSA") (S. 1409), introduced in July 2023, defines a "covered platform" as an online platform that "connects to the internet and that is used, *or reasonably likely to be used*, by a minor."[10] This definition would include not only websites and platforms that are actually directed to children (as defined by the FTC's COPPA rule), but would also substantially broaden the scope of covered business and impose new requirements on the vast majority of websites or apps that are intended for general audiences but may incidentally be used or accessed by a small

[8] NAI Code § II.D.1.
[9] NAI Code § II.E.1.
[10] Kids Online Safety Act, S. 1409, 118th Cong. § 2(3) (2023) (emphasis added).

percentage of minors or children without the knowledge or intent of the operators of those digital properties.

As minors approach adulthood, they tend to have interests that closely align with adults. For example, digital media dedicated to general topics like sports and news may be of interest to teens, and even some children, but they are not specifically designed for or directed to an under-18 audience. Further, those sites may prefer to allow their users to browse anonymously without collecting information (like email address, payment information, and date of birth) that would be necessary to verify age. Therefore such a broad approach presents substantial challenges for implementation, including operational and legal uncertainties for digital media providers of all sizes, but particularly the smaller ones. Smaller and newer companies have fewer resources to dedicate to operational challenges like age verification and may rely more heavily on ad revenue for their operations (compared to larger and more established companies that may be supported by a subscription base) and would be put at a competitive disadvantage compared to larger companies that can more easily bear large compliance costs. Ultimately, this approach could practically require most websites or apps to either treat all consumers as children or require privacy-invasive practices like age gating while raising potential constitutional concerns as well.[11]

COPPA established a clear approach to understanding the age of young users – followed by most current state laws – by relying on an "actual knowledge" standard for user age. Under this approach, operators of general audience digital properties and digital advertising partners are responsible for adhering to COPPA's heightened protections when the company actually knows that it is processing children's data. On the other hand, and departing from the COPPA standard, some recent legislative proposals have promoted a "constructive knowledge" standard by asserting that in some circumstances companies *should know* they are using children's data, even if they do not *actually* know they are using that data. But constructive knowledge standards do not provide sufficient guidance for determining *when* companies should know they are processing children's data, and appear to be grounded in an assumption that companies should know even when they lack sufficient reason to know they have children's data. This standard also runs the risk of being overly broad and forcing all online platforms to treat every user as if they were a child or teen, or else require companies to adopt age verification policies that are detrimental to consumer privacy. The most robust forms of age verification, for example, require businesses to collect personally-identifiable information, such as government identifiers, where the risks associated with the collection are significantly higher for both consumers and businesses.[12]

---

[11] For example, a Federal district court found that the California Age-Appropriate Design Code Act's requirements for age estimation did not materially alleviate the harms associated with collecting children's data online; instead, the court found the Act was "likely to exacerbate the problem by inducing covered businesses to require consumers, including children, to divulge additional personal information." Order Granting Mot. for Prelim. Inj., NetChoice, LLC v. Bonta, 22-cv-08861-BLF (N.D. Cal. Sept. 18, 2023) at 22.

[12] The nonpartisan Congressional Research Service has noted the challenges with identifying minors through age verification technologies, such as potential racial biases in facial recognition software to First Amendment concerns with blocking access to the web, as well as the privacy risks associated with such data collection. *See* CLARE Y. CHO,

With overly-broad definitions and standards, most (if not all) websites and apps would be in the difficult position of being required to treat all of their users as if they were minors, even if the vast majority of them are not. In this case, they would (under the strictures of the same proposals) be unable to offer tailored advertising that drives free and low-cost digital media. This would be harmful to consumers that prefer a free, ad-supported experience over paid subscriptions; and harmful to competition because incumbents with an existing, large subscription base would be put at a further competitive advantage. Broad limitations would curtail advertising and are likely to put many smaller websites and apps out of business. In turn, this would result in a degradation in the diversity of digital content, ultimately causing the largest platforms to grow at the expense of consumers and smaller digital content providers.

These are interrelated challenges, combining a set of requirements and standards established under COPPA, with a wide range of different concepts. Any new laws or regulations must provide practical guidelines for industry. In short, an overly broad approach risks curtailing the current rich digital media marketplace and harming competition across digital media and advertising without significantly improving data protection for kids and teens.

IV. NAI Policy Recommendations

The NAI strongly supports a national, comprehensive privacy framework that both respects and protects consumer privacy while allowing for online businesses to continue to grow and thrive, driven by digital advertising. Under the current patchwork of state privacy laws, however, consumers do not have equal data protections or rights, and digital advertisers bear a compliance process that is unnecessarily complex. The federal government must act to ensure strong uniform protections for all consumers and reduce the compliance burden on businesses from a disparate set of state laws.

As part of a national law, the NAI supports several policies that would enhance privacy and data protection for children (*i.e.*, those under the age of 13 already covered under COPPA) and minors (*i.e.*, those between the ages of 13 and 17) across the digital media industry. These policies should be based on approaches that digital advertisers and their customers operating websites and online services can implement and operationalize, without unduly burdening consumers or mandating age verification obligations. These enhanced protections must be applied to all businesses, not just those that subject themselves to voluntary practices promoted by the NAI and other self-regulatory organizations.

Cong. Research Serv., IN12055, Challenges with Identifying Minors Online (2023), https://crsreports.congress.gov/product/pdf/IN/IN12055#:~:text=Potential%20Challenges%20with%20Identifying%20Minors,as%20those%20younger%20than%2013.

1. **Prohibit targeted advertising to known children and minors.**

As discussed above, under the NAI's self-regulatory Code, NAI members are currently prohibited from engaging in tailored advertising to users who they know to be under the age of 16, without parental consent. It is a common practice for NAI members to avoid creating segments targeting minors altogether, even for minors to whom the NAI's restrictions do not specifically apply. For these companies, the value of tailoring an ad to a 16- or 17-year old specifically, as opposed to 18- to 24-year-olds, is outweighed by the risk associated with such data collection. Various states have recently adopted similar limitations on tailored advertising to children and minors.[13]

However, for purposes of establishing a consistent national standard that applies evenly to minors across the United States and that is applicable to all companies, the NAI supports a national privacy law that would exceed these existing standards by simply prohibiting all companies from: (1) processing a known minor's personal data for engaging in tailored advertising; and (2) selling the personal data of known minors to third parties. These prohibitions should be clearly crafted to preserve the ability of digital advertising businesses to perform ad delivery and reporting, and other practices associated with contextual advertising.

2. **Establish a consistent national standard for companies to avoid targeting advertising to children and minors based on actual knowledge or willful disregard of available facts.**

As discussed above, one of the most challenging issues for advertising technology companies and others across the digital advertising industry is determining which users are children or minors, the latter who particularly have interests that may coincide with those of adults. "Constructive knowledge" approaches create substantial legal uncertainty and would likely lead to substantial degradation of user experiences, inconsistent enforcement, and legal challenges. Therefore, the NAI supports establishment of a national standard based on actual knowledge or *willful disregard* of facts about the age of particular users. This exceeds the COPPA standard and aligns with existing state law standards.[14] This can more practically be applied to companies engaging in tailored advertising and enforced in cases where companies ignore information they actually have, instead of speculating about what a company should or should not know.

3. **Establish a clear national standard for data protection assessments for digital media companies to evaluate whether their websites and online services are directed to children.**

Data protection assessments ("DPAs") are currently required by most of the comprehensive state privacy laws passed since 2020.[15] Consistent with these state law requirements, the

---

[13] *See, e.g.*, Conn. Gen. Stat. § 42-520(a)(4) (2023) (requiring parental consent for the processing of personal data pertaining to a consumer under the age of 13 and, for consumers aged 13-16, requiring consumer consent for the sale of personal data or its processing for targeted advertising), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF.

[14] *See, e.g.*, Cal. Civ. Code § 1798.120(c) (2023).

[15] *See, e.g.,* Conn. Gen. Stat. § 42-522 (2023).

requirement for digital publishers, advertisers, and advertising businesses to perform a DPA is usually triggered when a controller (*i.e.*, a person or entity that determines the purposes for and means of processing personal data) engages in sale of personal data, processes personal data for targeted advertising, or processes sensitive personal data – usually defined to include children's personal data. The NAI supports requiring a consistent national standard for DPAs in order to help companies across the online value chain fairly reduce privacy risks regarding data from all users.

Under those existing DPA standards, all companies – including ad-tech companies – are responsible for conducting assessments when they know they are processing children's personal data. However, ad-tech companies generally do not know – and are not in a position to know – whether a website or online service is *directed* towards children unless it is identified by the website or app publisher and flagged clearly, such as through a COPPA flag. A COPPA flag is an attribute of a bid request that signals whether that request is for the opportunity to serve an ad to a child. This flag allows media buyers (digital advertising companies) to programmatically decide whether to make a bid and whether or not they can deploy technologies that collect users personal information for purposes of audience generation and ad selection. In the absence of stronger standards for identifying child-directed properties, ad-tech companies may lack the information they need to limit their processing of information that more likely pertains to young users, which is particularly important when ad-tech companies already lack actual knowledge about a user's age.

The NAI therefore believes the best approach for determining when a website or app is directed to children is by assessing the totality of the circumstances (*i.e.,* the existing COPPA standard). A website or app that has games that appeal to children, uses a cartoon mascot, and actively tries to grow an audience of children is different from a website that reports on a sports league for a general audience, even though minors–or children–may incidentally access those sites, and even if those sites utilize cartoon mascots. Businesses in the former category intend their sites and services to be used by children and bear the responsibility of identifying this intention to partners, but businesses putting an advertising pixel on the latter cannot reasonably be expected to account for the possibility that a small percentage of users accessing the site are children without going through additional, privacy-invasive practices, including the possibility that they would be required to link pseudonymous user identifiers like device IDs with personally-identified information like email address and birthday, before offering tailored advertising services.

As part of a DPA, the NAI supports a requirement for websites or online services to assess the content of their sites and services in order to make a determination of the age of users their content is directed to. The NAI believes that such an assessment is the best approach for determining when a website or app is directed to children and will enhance the ability of ad-tech companies to protect children's data.

V. Conclusion

More discussion and work is needed to evaluate the potential parameters of these recommendations to avoid possible overbreadth in a way that could limit the ability of consumers to utilize online services and to seek out information, and for publishers to invest in and support their online services through digital advertising. If applied incorrectly, policies seeking to protect the data of children and minors run the risk of unnecessarily harming consumers by limiting free, ad-supported media and harming competition by introducing requirements that are most difficult for smaller and newer companies to meet, all while providing only speculative privacy protections to children and minors, and potentially undermining free speech rights. The NAI would be pleased to work with NTIA, the Biden-Harris administration and other stakeholders on constructive options that balance the policy and practical questions to advance shared privacy goals while avoiding undue burdens on consumers and businesses.

Again, thank you for conducting this thoughtful initiative, and for the opportunity to submit comments. 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 and CEO
Network Advertising Initiative (NAI)