Before the
Federal Trade Commission
Washington, D.C.

In re	Docket No. 2023-28569
Children's Online Privacy Protection Rule	

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Federal Trade Commission's Notice of Proposed Rulemaking published in the Federal Register at 89 Fed. Reg. 2034 (January 11, 2024), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments. CCIA is pleased to participate in the Commission's proposed rulemaking to amend the Children's Online Privacy Protection Rule ("COPPA Rule" or "the Rule").[2]

I. Introduction

COPPA has the twin aims of protecting children's privacy online and promoting the availability of innovative online services and content for children.[3] CCIA strongly believes that children are entitled to a higher level of security and privacy in their online experiences. The Association's members have led the effort to implement settings and tools to specifically tailor younger users' online use to the content and services that are suited to their lived experiences and developmental needs. For example, various services allow users to set time limits, provide

[1] CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at http://www.ccianet.org/members. Legal research and summaries provided by Sheryl Wang, CCIA Law Clerk, were instrumental to these comments.
[2] *Children's Online Privacy Protection Rule Notice of Proposed Rulemaking*, 89 Fed. Reg. 2034 (Jan. 11, 2024) (hereinafter "NPRM"), available at https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule#open-comment.
[3] *See* 144 Cong. Rec. S12787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan) ("The legislation accomplishes these [privacy] goals in a manner that preserves the interactivity of children's experience on the Internet and preserves children's access to information in this rich and valuable medium").

enhanced privacy protections by default for known child users, and other tools to allow users to block specific sites entirely.[4]

CCIA and its members appreciate the FTC's sustained efforts to ensure that the Rule keeps pace with an ever-changing online landscape by seeking public input and stakeholder feedback. More recently, the COVID-19 pandemic demonstrated the importance of internet connectivity for all individuals but even more so for children who had to rely on the internet for schooling and developing important social communication skills.[5] Users, including children, interact with these digital tools and services in a variety of manners which continues to change with improvements to augmented and virtual reality products. To ensure that the Rule continues to adhere to the statute's twin aims, the Commission should seek to provide greater clarity about the application of the Rule to the dynamic internet ecosystem and consider ways to enable operators to provide appropriate content and comply with COPPA requirements like obtaining parental consent. In particular, the Association appreciates the Commission's decision to decline a proposal to change the Rule's actual knowledge standard to a constructive standard.

We provide comment herein on several of the specific questions raised in the NPRM, including the proposed amendments to the Rule and the additional considerations, to ensure any proposed changes are consistent with the requirements of the Children's Online Privacy Protection Act.

II. Discussion

A. Question 3

The Commission proposes an amendment to include mobile telephone numbers within the definition of "Online Contact Information" so long as such information is used only to send text messages. The modification would help ensure that the Rule is keeping pace with today's technological landscape as a recent Pew study found that the "vast majority of Americans—97%

[4] *See e.g.*, Competitive Enterprise Institute, Children Online Safety Tools, https://cei.org/children-online-safety-tools/; Software & Information Industry Association (SIIA), Keep Kids Safe and Connected, https://www.keepkidssafeandconnected.com/.

[5] UNICEF, *How many children and young people have internet access at home?; Estimating digital connectivity during the COVID-19 pandemic* (Dec. 2020), https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/

—now own a cellphone of some kind."[6] Text messages also represent one of the most direct and frictionless verifiable methods for contacting a parent to provide notice or obtain consent. CCIA supports this proposal to improve the Rule's functionality.

B. Question 5

The Commission proposes expanding the scope of the Rule's definition to include biometric identifiers. As written, the proposed Rule would exceed the FTC's statutory authority. The COPPA statute requires that the Commission determine that a proposed identifier "permits the physical or online contacting of a specific individual" to be included in the definition.[7] Under the statute, it is not sufficient that the identifier can be used to recognize an individual. Rather, the identifier must permit physical or online contacting of a s*pecific individual.* The FTC has not demonstrated that this high standard is met regarding the various elements included in the proposed biometric identifier definition—especially considering that biometric identifiers like physical data can be used to provide *non-identifying* services. The Commission should also consider providing an exception for biometric identifiers that are promptly deleted.

The proposed definition is also at odds with other aspects of the NPRM. For example, the Commission rightly concluded that inferred data and data that is a proxy for personal information cannot itself be "personal information" under COPPA, yet nevertheless proposes to treat such data as "biometric identifier" personal information to the extent it is derived from voice data, gait data, or facial data. The proposal is also inconsistent with the FTC's 2017 Enforcement Policy Statement regarding the Rule's application to the collection and use of voice recording, which the FTC proposes to incorporate into the updated COPPA Rule. The Enforcement Policy Statement provides that although the FTC added audio files containing a child's voice to the definition of "personal information" in the 2013 revisions to the COPPA Rule, the FTC will not require parental notice and consent to collect voice recordings from a child as a replacement for text inputs, as long as the voice recordings are deleted promptly after responding to the child's request.[8] The NPRM proposes to codify this Policy Statement and extend it to cover voice

---

[6] *See* Mobile Fact Sheet, PEW Research Center, (Jan. 31, 2024) ("Nine-in-ten own a smartphone, up from just 35% in Pew Research Center's first survey of smartphone ownership conducted in 2011.") https://www.pewresearch.org/internet/fact-sheet/mobile/

[7] 15 U.S.C. § 6501(8)(F).

[8] Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, FED. TRADE COMM'N (Oct. 20, 2017).

recordings even when they are not used as a substitute for written words. Treating all information derived from voice data as "biometric" personal information, regardless of whether it is used to identify or contact *a specific person*, is at odds with the FTC's intent to permit the collection and processing of voice recordings and to encourage the use of innovative, more accessible alternatives to text-based inputs.

The NPRM discusses another proposed change to the definition that would include screen or user names. Despite the proliferation of such names for gaming and other online services, it is not clear how this proposal would adhere to the statutory requirement that an identifier can be used to contact a *specific individual.* From picking a creative homage to their favorite fiction character to simply choosing the only available name, users may choose a specific user name for a plethora of reasons. A username for gaming is fundamentally different from the other existing categories of personal information like name and telephone number. Broadening the scope of the definition to include nonspecific user names would create uncertainty around the development of new services and contradict COPPA's data minimization goals. CCIA recommends the Commission oppose this proposal, especially given that it raises several of the same concerns raised by the Commission when inferred data was being considered but ultimately declined.[9]

C. Question 9.

The dynamic digital ecosystem relies upon the transmission and processing of certain information for the basic operations, functions, and utilization of modern websites and online services. The COPPA Rule recognizes the importance of allowing for the transmission of this routine information with the carve-out for the support of internal operations to prevent unnecessary disruption to the functioning and availability of all types of children's content. CCIA appreciates the Commission's clarification that the definition of "support for the internal operations of the website or online service" already covers user-driven and user-engagement personalization, and enhanced personalization techniques based on certain operator-driven metrics and inferences. However, CCIA is concerned about the unintended consequences the proposal to prohibit operators from using this exception to "optimize user attention or maximize children's engagement" without verifiable parental consent would create if broadly defined.

[9] NPRM, at 2042.

The NPRM specifically discusses including the use of notifications or prompts that drive such engagement under this prohibition. Operators would be unable to provide timely and helpful notifications about location tracking or changes to a family group unless they had verifiable parental consent. Some educational applications, for instance, utilize push notifications to help children remain focused on their studies, including in conjunction with usage "streaks" and other methods intended to gamify learning for children's benefit. Other applications prompt children to complete educational content before accessing entertainment content, which again is intended to promote learning for the benefit of children. Under this proposal, such apps may be found to "encourage use of a service" which would mean they would not be able to rely on the support for internal operations exception—a possible unintended consequence of the proposed Rule.

Preventing businesses from improving transparency or parental controls through vague restrictions would result in a worse online environment for children and families. As such, the Rule must differentiate between techniques that are used solely to promote a child's commercial or otherwise detrimental engagement, like to promote an in-app purchase, and those that provide other functions, such as for personalization which the Rule currently permits. CCIA recommends the Commission consider a narrow interpretation for prompts and notifications that could be limited to those with a commercial aspect—encompassing push notifications that promote microtransactions or targeted advertising.

D. Question 10

Currently, operators can collect persistent identifiers for contextual advertising purposes without parental consent so long as they do not also collect other personal information. The Commission included contextual advertising in the non-exhaustive list of activities that fall under the internal operations exemption, reflecting an understanding of how this practice differs from other forms of advertising. Unlike targeted advertising, contextual advertising displays ads based on the content of the site and does not rely on the collection and tracking of specific user's information.[10] This business model has created an improved online experience by enabling

[10] Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 Santa Clara High Tech. L.J. 3, 44 (2010) (The FTC declined to include contextual advertising within its Self Regulatory Principles for Online Behavioral Advertising "because contextual advertising does not involve the compilation and storage of a profile of consumers' behavior, FTC concluded it did not pose the same risk of privacy-related harms as behavioral advertising").

websites of all sizes to provide users with free content, which is often only made possible by advertising revenue. Beyond access to an abundance of diverse and free content, users have also benefited from seeing more relevant advertising when viewing a site with a related product or service—seeing an ad for a coffee machine while reading a blog that focuses on coffee recipes.[11] Contextual advertising has been especially helpful in the growth of young content creators who have been able to monetize their content with ads that are appropriate for their audience and help advertisers ensure brand safety amongst other benefits.

The Commission should not disrupt this economic model, which has allowed businesses to support a rich array of free content for users. The current Rule's approach to both types of advertising, contextual and targeted, represents a careful balance that continues to protect children's privacy and allows for content to be both relevant and monetizable. The Commission should decline the proposal to eliminate this distinction under the Rule.

E. Question 11

The Rule's multifactor test for determining whether a website or online service is directed toward children sets forth a comprehensive and balanced set of criteria. The determination relies upon several content-specific and context-based factors including subject matter, visual content, use of animated characters, and language.[12] CCIA opposes the proposal to add new, unclear examples of evidence to consider during this determination. While the amendments attempt to provide clarity for when a service is directed to children, the specific examples would actually invite confusion by creating factors that are not directly tied to the direct activities or intention of the business.

The "age of users on similar websites or services" would introduce factors outside a business' control and operators would face confusing and difficult compliance requirements. To comply, an operator would need to determine what service or website is considered "similar"—despite the agency offering no such guidance—and then somehow determine the "age of users" on those "similar" websites or services. It is unclear how an operator would have the ability to

[11] Personalized ads are prohibited on YouTube Kids, as well as for users in a supervised experience on YouTube. This means the ads that appear are matched to videos being watched based on the content, not the specific user watching. *See* YouTube, *How does YouTube help keep kids and teens protected on the platform?* (last accessed, Feb. 22, 2024) https://www.youtube.com/howyoutubeworks/our-commitments/fostering-child-safety/#childrens-data.

[12] 16 C.F.R. § 312.2

accurately assess the actual or intended audience of another operator's service that is deemed "similar". Operators also would be unable to accurately obtain information about the audience composition of other services.

The proposed inclusion of "review by users or third parties" into this determination also raises serious concerns by introducing factors that are outside a business' control. Operators would face heavy compliance burdens by having to monitor and assess external sources, again without any guidance on what constitutes an acceptable "review". The Agency should decline the proposed expansion of this assessment to include "reviews by users or third parties" and "age of users on similar websites or services".

The NPRM also discusses the ability of websites or online services to rebut that they are directed to children through an audience composition analysis. CCIA appreciates the proposed flexibility created by this exception but encourages the Agency to consider a higher threshold than 20% as discussed in the notice.

F. Question 12

To ensure that the Rule's existing notice requirements remain clear and consistent, CCIA recommends that operators should be able to identify the categories of those third parties and rely upon their existing privacy and security programs for purpose limitation.

The Commission is also considering modifying the online notice requirements in § 312.4(d) to require any operator using the support for the internal operations exception to specifically identify the practices for which the operator has collected a persistent identifier and the means the operator uses to comply with the definition's use restriction.[13] This proposed amendment to online notice requirements is unlikely to result in additional compliance clarity or provide more relevant information to parents and guardians. However, requiring such detailed disclosures about internal operations could risk exposing sensitive business information and other unintended consequences. For instance, the definition provides a list of activities that include those necessary to maintain or analyze the function of a site and to protect the "security or integrity of the user, website, or online service."[14] As written, the proposed Rule could require

[13] NPRM, at 2045, 2050. A persistent identifier could not be used to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website or online service, or for any other purpose, except as permitted by the support for.
[14] 16 C.F.R. 312.2, definition of ''support for the internal operations of the website or online service.'' The definition includes activities such as those necessary to maintain or analyze the functioning of a site or service;

operators to reveal potentially sensitive security practices that include mitigations measures that help protect the site and users. Malicious actors may be able to leverage the new information found in these notices to discover vulnerabilities that they can then use to compromise an operator's website, service, or users.

CCIA recommends that the Commission confirm that online notice requirements do not require operators to disclose potentially sensitive business information that could compromise the safety, security, or competitiveness of the operator and their service or website.

G. Question 13

The NPRM asks whether platforms can play a role in establishing consent mechanisms to enable obtaining verifiable parental consent (VPC). The Commission is also interested in any potential benefits a platform-based common consent mechanism would create for operators and parents. It is not clear whether the Commission seeks to impose a greater role upon app stores or device makers, regardless, this proposal to exempt developers from one of the Rule's most important requirements should be declined.

The Rule's VPC requirements provide parents with control over the content their child may view and the personal data they share with the website or services. The Commission developed context-specific flexibility for obtaining VPC by allowing operators to either use an approved VPC method or one that is "reasonably designed in light of available technology."[15] Operators can choose the VPC method that is most suitable to their service or website and avoids burdening or frustrating parents.

The Commission's vague proposal would undermine the objectives of the COPPA Rule's VPC requirements by shifting this obligation, and related substantial liability and legal risks, from developers to platforms. Platforms should not have an obligation to develop a VPC method for third-party developers and their offered services. Shifting this burden to platforms, whether app stores or device makers, would result in a more static, and less innovative ecosystem for online services and websites for children. Developers, not platforms, are best suited for ensuring that their offered services adhere to the consent provided by a parent. The proposed approach would impose costly, and possibly infeasible, obligations upon platforms with little to no benefit

---

personalize content; serve contextual advertising or cap the frequency of advertising; and protect the security or integrity of the user, site, or service.

[15] 16 C.F.R. 312.5(b)(1)

to parents. Children could still circumvent platforms by using other internet-connected devices or resort to other operators with less stringer requirements, which may include age-inappropriate experiences.[16] CCIA urges the Commission to confirm that developers, not platforms, must comply with the Rule's implementation requirements.

H. Question 14

Currently, the COPPA Rule permits operators to obtain a single consent for the collection, use, and disclosure of a child's personal information, including any relevant disclosures to third parties for targeted advertising. The Commission proposes amending this provision by removing operators' ability to bundle all consent for such disclosures with other consents they obtained to collect, use, and disclose the child's personal information. Specifically, the proposed Rule would require operators to obtain an additional and separate parental consent for disclosures to third parties, unless such disclosure is "integral to the nature of the website or online service."

The proposed substantial changes to the parental consent requirements would create unnecessary confusion for parents and businesses. Parents would encounter longer and repetitive consent requests that may introduce consent fatigue and importantly, reduce their understanding of the data practices presented. Businesses would face mounting compliance costs for each additional disclosure, which again would provide no substantial benefits to parents. Rather than overwhelming consumers through bifurcated consent, the Commission could allow operators to provide the third-party disclosure as part of the larger first-party VPC process. The Commission could clarify that an operator would be able to comply with this requirement by providing a clear disclosure that contains a checkbox or another reasonable mechanism to obtain separate VPC for third party disclosures. This alternative would still provide parents with additional clarity and information but avoids the confusion and costs associated with an overly prescriptive VPC requirement. Additionally, the Commission should clarify that any disclosures made under a legal or compliance purpose are included under the "integral to the nature of the website or online service" exemption.

[16] Federal Trade Commission, *Transcript of The Future of the COPPA Rule: An FTC Workshop Part 2* (October 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_2_1.pdf.

The proposed bifurcated consent requirement, in addition to the proposed modifications to contextual advertising, could make advertising, including contextual advertising to children, more difficult if not impossible. CCIA recommends the Commission to decline this proposed change unless further changes and clarifications are made.

The Commission is also proposing eliminating the monetary transaction requirement when an operator obtains consent through a parent's user of a credit card, debit card, or online payment system. Under this proposal, a parent would only need to enter their payment information and no charge would be imposed. As noted in the NPRM, many operators offer their online services at no charge and charging a parent a nominal fee associated with obtaining consent would "undercut[] their ability to offer the service at no cost."[17] This would be a beneficial change and CCIA supports the elimination of monetary transactions.

I. Question 15

Currently, an operator is not required to obtain verifiable parental consent if one of several exceptions are met. The Commission proposes to modify exception § 312.5(c)(4) to exclude the use of push notifications to encourage or prompt use of a website or online service.[18] As explained above, the Rule should differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that provide other functions such as making the content more relevant. Any further changes to the Rule should seek to clarify that engagement techniques refer to those that seek to primarily drive engagement such as through the use of a variable reward system or excessive push notifications to sign in.

J. Question 16

The Commission's past actions and guidance have indicated that schools, state educational agencies, and local educational agencies may authorize the collection of personal information from students younger than 13 under specific situations.[19] The Commission has determined that such authorization is permissible so long as the data is used for a school-authorized education purpose and no other commercial purpose. CCIA welcomes this proposal to codify this exemption to parental consent.

[17] NPRM, at 2052.
[18] NPRM, at 2053.
[19] Policy Statement on Education Technology and the Children's Online Privacy Protection Act, FED. TRADE COMM'N (May 18, 2022).

K. Question 20

The proposed amendments would greatly expand the scope and extent of the obligations for covered operators. CCIA urges that the Commission give businesses more time than the six-month on-ramp to implement the final requirements from the NPRM. The Commission should consider giving businesses 18-24 months for compliance.

L. Additional Provisions in Proposed Rule

Data Retention and Deletion. As proposed, an operator would be required to at least establish and maintain a written data retention policy specifying its business need for retaining children's personal information and its timeframe for deleting it prohibiting operators from retaining children's personal information indefinitely.[20] The Commission further proposes clarifying that operators may retain personal information for only as long as is reasonably necessary for the specific purpose for which it was collected, and not for any secondary purpose.

The proposed changes attempt to strengthen the Rule's data retention limits, in addition to reinforcing the data minimization requirements but further clarity and modifications are needed to provide enough flexibility for operators.[21] First, the Commission should clarify that an operator can comply with the data deletion requirements for children's data if the operator is already covering it in another broader assessment, such as required under a state privacy law. Operators should not be required to spend considerable resources if a comparable assessment has already been conducted. Second, it is unclear whether an operator can comply with this requirement by providing a general data retention policy that covers both adults and children under 13, or if a separate retention policy specifically for children's data is required. Moreover, regarding the data retention timeline in the education context, the Commission should confirm that this limit is determined by the school, who are better situated for this requirement, and not the ed-tech provider. Lastly, the Commission should amend the Rule to provide exceptions for certain instances of indefinite data retention. These necessary exceptions could be limited to security, fraud & abuse prevention, financial record-keeping, complying with relevant legal or regulatory requirements, ensuring service continuity, or when the user has provided verifiable parental consent to the extended retention of data.

[20] NPRM, at 2062.
[21] *Id.,*"The notice describes that the proposed modifications to §312.10 are intended to reinforce § 312.7's data minimization requirements."

III. Conclusion

The FTC has the opportunity to provide greater clarity for businesses regarding their COPPA obligations and parents concerning what privacy options and controls they have for their child. As the Commission continues to review the proposed rules, it should remain aware of the statute's twin aims and the potential costs, and unintended consequences, any broad modification could create. CCIA is pleased to provide this information and welcomes any questions from the Commission.

Respectfully submitted,

Alvaro Marañon
Policy Counsel, Privacy and Security
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
amaranon@ccianet.org

March 11, 2024