U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

March 11, 2024

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue
Suite CC-5610 (Annex E)
Washington, DC 20580

Re: COPPA Rule Review, Project No. P195404

The U.S. Chamber of Commerce ("Chamber") respectfully submits comments to the Federal Trade Commission ("FTC" or "Commission") in response to its Notice of Proposed Rulemaking to update the Children's Online Privacy Protection Rule ("Proposed Rule").[1] Technology platforms are enabling small businesses to grow and thrive[2] and expanding educational opportunities. At the same time, the Chamber supports robust data protections for all Americans regardless of age or geography through national privacy legislation. Until Congress enacts comprehensive privacy legislation, the Commission possesses limited authority to enforce against unfair and deceptive privacy practices[3] as well as make privacy rules for children under thirteen.[4] We support the Commission's appropriate utilization of these authorities and appreciate the FTC re-affirming that "actual knowledge" is the appropriate scoping standard under the statutory text.

I. Definitions

A. Personal Information

i. *Avatars and Screennames*

The Commission asks for public comment on whether to include user screennames and avatars in the definition of "personal information" to be covered by the COPPA Rule.[5] The Chamber recommends against the inclusion of these terms.

---

[1] 89 Fed. Reg. 2034 (January 11, 2024) *available at* https://www.govinfo.gov/content/pkg/FR-2024-01-11/pdf/2023-28569.pdf.

[2] U.S. Chamber of Commerce, *Empowering Small Business: The Impact of Technology on U.S. Small Business* (September 14, 2023) *available at* https://www.uschamber.com/assets/documents/The-Impact-of-Technology-on-Small-Business-Report-2023-Edition.pdf.

[3] 15 U.S.C. § 45.

[4] 15 U.S.C. § 6501, et seq.

[5] 89 Fed. Reg. 2069-70 (Questions 5 and 6).

Avatars do not constitute "individually identifiable information about an individual,"[6] as the statutory definition of "personal information" requires. Additionally, if an avatar image does not leave the device, no personal information is "collected" under COPPA. Furthermore, allowing users to create avatars generated from an image is a privacy-protective alternative that should be encouraged, consistent with data minimization principles and FTC guidance encouraging blurring or other modifications to a child's image before it is publicly displayed.

Additionally, the FTC lacks a statutory basis for including avatars in the Rule's definition of personal information. While the statute permits the FTC to expand the definition of "personal information," that authority is limited to where the information, on its own, is "individually identifiable" and "permits the physical or online contacting of a specific individual."[7] There is no demonstration that an avatar generated from an image satisfies either requirement. To the contrary, operators utilize such avatars, similar to anonymous user and screen names, to allow a user to personalize their settings and experiences (such as game leaderboards and filtered or moderated chat) without collecting identifiable information.

An avatar is notably distinct from other types of information that the FTC has previously added to the Rule's "personal information" definition. Whereas photographs were added to the definition of personal information in 2013 on the basis that a photo could "be paired with facial recognition technology" to "'permit the physical or online contacting of a specific individual,"[8] an avatar, even when paired with facial recognition technology, cannot permit physical or online contacting of a specific individual. The features of a digital avatar are significantly abstracted from, and therefore cannot be associated with, those of individuals represented by the avatar. In fact, avatar creation is offered as an alternative to displaying actual images and should be encouraged.

Also, defining "personal information" to include screennames could have a counter-privacy effect as many users choose particular screennames to engage with online services in a way that will provide them with anonymity. The extremely broad proposed interpretation would fundamentally change how services operate on the Internet in ways that would reduce the privacy of children, a dramatically increase the number of services that would need verifiable parental consent, and nullify the support for internal operations exception.

Many operators collect an anonymous username or screen name precisely to avoid collecting personal information—such as a full name or email address —when such information is not otherwise needed. Yet, under this proposed change, operators

[6] 16 C.F.R. § 312.2.
[7] 15 U.S.C. § 6501(8).
[8] 78 Fed. Reg. 3972, 3981 (Jan. 17, 2013).

would need to collect more personal information from children and their parent than otherwise would be collected to seek verifiable parental consent, since an anonymous username or screen name is not sufficient to enable the operator to contact a parent to request verifiable parental consent.

ii. *Biometric Identifiers*

The Commission proposes amending the definition of "personal information" to include a "biometric identifier that can be used for the automated or semi-automated recognition of an individual, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data."[9]

Generally, the Commission should avoid promulgating rules that contribute to a confusing and conflicting patchwork of privacy laws. For seamless operationalization and enforcement, the Commission should harmonize its definition with other laws, particularly the Consensus State Privacy Approach which has been adopted by multiple state legislatures and protects over 95 million Americans already. For example, the Virginia Consumer Data Protection Act defines biometric data as "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."

Regarding "biometric identifiers," the Children's Online Privacy Protection Act ("COPPA") grants the Commission authority to designate as personal information an "identifier that the Commission determines permits the physical or online *contact* of a specific individual."[10] Not all the data proposed by the Commission as a "biometric identifier" can be used to contact individuals. To avoid vagueness, the Commission should revise the definition of "biometric identifier" to include biometric identifiers when they *are used* for the automated recognition of an individual rather than where they *could* be used for such purposes.

In addition, we recommend removing the reference to "data derived from voice data, gait data, or facial data" as much of this information is already covered by the inclusion of audio files and photographs including a child's image in the definition of "personal information." At a minimum, "data derived from voice data" should expressly exclude the data covered by the proposed exemption for audio data to assure that the audio file exemption is meaningful.

[9] 89 Fed. Reg. 2041.
[10] 15 U.S.C. § 6501(8)(F) (emphasis added).

iii. *Inferred Data*

The Commission's Proposed Rule correctly refrains from including "inferred data" in the definition of "personal information." As the Chamber noted in its comments ("2019 Comments") responding to the Commission's 2019 inquiry about its intended COPPA update, "a specific inclusion of inferred personal information would create more uncertainty and ambiguity around the scope of the [COPPA] Rule that could impede the development of new services."[11]

Nevertheless, the Commission also stated in the NPRM that "[i]nferred data or data that may serve as a proxy for 'personal information' could fall within COPPA's scope . . . if it is combined with additional data that would meet the Rule's current definition of 'personal information.' In such a case, the existing 'catch-all' provision of that definition would apply."[12] This approach both mischaracterizes the statute's catch-all provision and inadvertently nullifies COPPA's support for the internal operations exception.

Treating inferred and proxy data as "personal information" under COPPA's catch-all would inadvertently eviscerate COPPA's support for the internal operations exception. If such data were to be considered "personal information," important fraud prevention and other safety-promoting activity currently protected by the support for internal operations exemption would be at risk. Accordingly, we request that the Commission clarify that the processing of inferred data and information that serves as a proxy for personal information does not fall within COPPA's catch-all definition.

iv. Online Contact Information

The Chamber supports the expansion of "'an identifier such as a mobile telephone number provided the operator uses it only to send a text message" to the definition of "online contact information,"[13] which is appropriate since mobile phone numbers are used in messaging, and such information could be used to contact an individual under the age of thirteen. Additionally, this new definition would help enable parental notification and consent through text messaging.

However, we urge the FTC to verify that collection and use of mobile phone numbers provided by children to contact parents to start the notice and consent process will not violate relevant federal or state law restrictions on text messaging.

---

[11] Chamber Comments to Commission (Dec. 9, 2019) at 3 *available at* https://americaninnovators.com/wp-content/uploads/2019/12/191125_Comments_COPPA_FTC.pdf.
[12] 89 Fed. Reg. 2034, 2042 (Jan. 11, 2024).
[13] 89 Fed. Reg. 2040.

B. Support for Internal Operations

i. *Practices that Support Internal Operations*

The COPPA Rule exempts from its requirements the use of personal information that support the internal operations of the website or online service. The Chamber agrees with the Commission's interpretation that the 2013 amended definition[14] of "internal operations" applies to ad attribution, particularly as it relates to measuring or reporting advertising or content performance, including independent measurement.

Although the Commission expands the uses of data that support internal operations, the Commission proposes "the exception should not be used to allow operators to maximize children's engagement without verifiable parental consent."[15] The Commission asks for comment on how it should differentiate techniques that drive engagement as opposed to other functions like personalization.[16]

First, it is not clear that COPPA confers authority on the FTC to propose this restriction or that doing so would be consistent with the First Amendment. Nor is it apparent whether these proposed restrictions unduly restrict truthful communications about features and activities available to and suitable for children. Personal information used to make content more relevant to a user should not be considered an engagement technique.

Second, if such authority exists, engagement techniques falling outside the Support for Internal Operations exception should be restricted to practices that have negative consequences for children, rather than restricting things that simply make a service more relevant for them, notify them of rewards, or even promote an age-appropriate experience. For example, a push notification may be used for something positive, like a bed-time reminder. Such applications can be utilized without compromising a user's privacy.

ii. *Notice Requirement*

The Commission proposes that entities availing themselves of the Support for Internal Operations exception are required to have an online notice that describes the "specific internal operations for which the operator has collected a persistent identifier."[17] It is not clear how a more granular explanation will be helpful to parents. In fact, a broad interpretation of the contemplated requirements — particularly one that would require operators to provide a detailed description of "the practices for

[14] 78 Fed. Reg. 3972, 3981 *available at* https://www.govinfo.gov/content/pkg/FR-2013-01-17/pdf/2012-31341.pdf.
[15] 89 Fed. Reg. 2045.
[16] *Id.* at 2046.
[17] *Id.* at 2074.

which the operator has collected a persistent identifier" — would undermine the purpose and usefulness of the exception. Some of the most important activities covered by the support for internal operations exception are operators' efforts to protect "the security and integrity of the user, website, or online service."[18] The new disclosure requirements could make it easier for fraudsters to circumvent protections implemented by operators, including spam detection and transaction verification systems that enable operators to flag suspicious or exploitative activity before it causes harm.

Business should be permitted to use categories to explain the purposes for which they utilize the Support for Internal Operations exception, and to rely on their data privacy and security programs for purpose limitation. This approach would accomplish the NPRM's objectives of "increas[ing] transparency" and "ensur[ing] that operators follow the use restriction"[19] without undermining the usefulness of the support for internal operations exception or adding ambiguity and arbitrariness to COPPA enforcement.

C. Website or Online Service Directed to Children

i. Directed to Children Factors

The Commission proposes adding new factors to consider when determining whether a website or online service, or a portion of such service, is directed to children. Under the current COPPA Rule, the FTC is to "consider competent and reliable empirical evidence regarding the intended audience."[20] The Proposed Rule would define specific evidence to be included as part of that evaluation including "marketing or promotional materials or plans, representations to consumers or to third parties, reviews by users or third parties, and the age of users on similar websites or services."[21]

The Chamber agrees with the Commission that marketing and promotional materials are a reasonable factor to determine whether a service is directed to children. However, some of the proposed factors like reviews by third parties or age of users on similar websites or services would create substantial uncertainty for business because they are highly subjective and would introduce factors totally outside the control of an operator.

[18] 16 C.F.R. § 312.12.
[19] 89 Fed. Reg. 2034, 2045 (Jan. 11, 2024).
[20] 16 C.F.R. § 312.2
[21] 89 Fed. Reg. 2047.

ii. Collection of Information from Other Websites or Online Services

The current COPPA Rule deems websites and online services to be child-directed if its operator "has actual knowledge that it is collecting information *directly* from users of another Web site or online service directed to children."[22] The Commission proposes amending the COPPA Rule to eliminate the requirement that information be collected *directly* from third-party websites or services directed to children. Such an approach would effectively impute knowledge of whether a third party's operations are directed to children to a first-party operator, triggering liability for a first-party operator of a website or online service. Removing the direct collection requirement would also create further uncertainty, particularly if no determination has been made by the Commission or the third-party that a third-party website's content is directed to children.

iii. *Mixed Audiences*

Confusion exists as to whether analysis of the proposed "mixed audience" definition is a two-step process. The FTC should clarify that an operator must show first that a website or service is deemed directed to children and *then* whether is primary audience is for children. If, and only if, the service is directed to children at that first step, will the FTC continue to the second step of applying the same totality of the circumstances criteria to assess whether children are the primary audience or whether the service is part of the subset of services directed to children as a secondary audience.

It is critically important that the FTC also clearly state its existing view that general audience sites are not subject to COPPA. The mixed audience designation requires some intentional action on the part of an operator to develop content intended for children. An example of an excluded general audience site would be an e-commerce platform. Although such a site may feature children's products, and might be visited by children, these sites are not directed to children primarily or even secondarily.

II. Knowledge Standard

The current COPPA Rule applies only when an operator has *actual knowledge* that it is collecting or maintaining personal information from a child.[23] The plain language of the COPPA statute also limits applicability to actual knowledge.[24] The Chamber strongly agrees with the Commission's rejection of expanding the knowledge standard beyond actual knowledge. The Chamber's 2019 Comments cautioned that a

[22] 16 C.F.R. §312.
[23] 16 C.F.R. § 312.3
[24] 15 U.S.C. § 6502(a)(1).

constructive knowledge standard "would hold platforms to an unreasonable level of accountability, increasing cost/burden to comply and could chill investments in child/family-directed content, service and platforms."[25]

Not only would a constructive or implied knowledge standard impact child-directed content, such a standard would also have a chilling effect on general audience services as well. Standards beyond actual knowledge are inherently subjective and operators may choose instead to apply regulatory requirements to all—not just child-related—data. Courts are growing increasingly suspicious of content and privacy regulations aimed at protecting children but impact broader audience practices. In *NetChoice v. Bonta*, a federal district court held that it was likely that California's Age-Appropriate Design Code fails speech scrutiny in part because:

> data privacy protections intended to shield children from harmful content, if applied to adults, will also shield adults from that same content. That is, if a business chooses not to estimate age but instead to apply broad privacy and data protections to all consumers, it appears that the inevitable effect will be to impermissibly 'reduce the adult population…"[26]

Given both constitutional and statutory concerns, the Commission correctly preserves the Actual Knowledge standard.

III. Consent

A. General Consent Issues

In addition to notice, COPPA requires that operators obtain verifiable parental consent ("VPC") before collecting, using, or disclosing children's personal information.[27] The Commission proposes requiring a separate consent for the disclosure of personal information.[28] It is unclear that the COPPA statute expressly authorizes a separate disclosure requirement. But even if the COPPA statute does expressly authorize a separate disclosure requirement, the Chamber recommends that to avoid notice overloading consumers, operators should be allowed to obtain the verified parental consent for disclosure in the same notice and consent flows that they utilize in their current VPC processes. Regarding data collection, the Commission should clarify that consent is required for materially new collection and not new offerings.

---

[25] *Supra* n. 11 at 7.
[26] Order Granting Motion for Preliminary Injunction, *Netchoice v. Bonta*, Case No. 22-cv-08861-BLF (N.D. Ca 2023) at 24.
[27] 15 U.S.C. § 6502(b)(1)(A)(ii).
[28] 89 Fed. Reg. 2051.

B. Methods of Consent

The Chamber agrees with the Commission's decisions to enable text message-based consent (subject to clarifying that such communications comport with federal and state text messaging laws) as well as the elimination of the money transaction requirement when operators obtain consent through use of a payment system.[29] Both changes to the COPPA Rule will ease parental burden and help streamline the consent process.

C. Consent Exceptions

i. *School Exception*

The Commission proposes a consent exception that authorizes schools to provide consent.[30] The Chamber supports the proposal to codify FTC's existing guidance[31] allowing schools to provide COPPA consent in lieu of a parent if the collection and use is for a school-authorized educational purpose.

ii. Audio File Exception

The Chamber strongly agrees with the Commission's decision to codify its Enforcement Policy Statement[32] on audio files into the COPPA Rule exceptions. Parental consent under the Proposed Rule would not be required "[w]here an operator collects an audio file containing a child's voice, and no other personal information, for use in responding to a child's specific request and where the operator does not use such information for any other purpose, does not disclose it, and deletes it immediately after responding to the child's request."[33] The Chamber's 2019 Comments endorsed this approach because the changing technology landscape regarding the ubiquitous use of voice-enabled technology is providing new commercial and educational benefits that should not be stunted by rigid application of COPPA to voice data.[34] The Commission should recognize a similar exception for biometric data and assure that any final definition of biometric data be consistent with this common-sense exemption.

---

[29] *Id.* at 2052.
[30] *Id.* at 2055.
[31] Complying with COPPA: Frequently Asked Questions *available at* https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS.
[32] Federal Trade Commission, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, 82 FR 58076 (Dec. 8, 2017) *available at* https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.
[33] 89 Fed. Reg. 2075.
[34] *Supra* n. 11 at 5-7.

iii. *Material Change*

The NPRM suggests a clarification to Section 312.5(a)(1) of the Rule, which requires that an operator obtain VPC "before any collection, use, or disclosure of personal information from children," including when the operator modifies practices to which a parent had previously consented. The NPRM seeks to clarify that the VPC requirement "applies to any feature on a website or online service through which an operator collects personal information from a child."[35]

Unfortunately, the NPRM's statement creates ambiguity and must be clarified. Specifically, we understand the FTC did not intend to require operators to seek VPC every time a new feature is introduced, even when prior notices and consent covers such processing of the child's personal information. Such an interpretation would be inconsistent with the text of the COPPA Rule, which states explicitly that additional verifiable parental consent is required only for "any material change in the collection, use, or disclosure"[36] of the child's personal information. It also would be detrimental to parents, who would face a deluge of consent requests from websites and services seeking to implement new features with no meaningful changes in how their child's information is processed.

The FTC should clarify that it was merely re-iterating what the COPPA Rule already requires – that verifiable parental consent must be updated when there are material changes in how an operator collects, uses, or discloses personal information from children. Relatedly, the FTC also should reiterate its longstanding guidance that VPC can be updated through, for example, a password or PIN number that the operator uses to confirm the parent's identity in any future contact with them.

IV. Data Retention

The current COPPA Rule limits operators' retention of personal information collected from children "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected" and to delete such data.[37] The Commission proposes that "operators must establish, implement, and maintain a written children's data retention policy that sets forth the purposes for which children's personal information is collected…"[38]

We encourage the Commission to align its data retention rules with those in legislatively enacted laws like the Colorado Privacy Act and Virginia Consumer Data

[35] 89 Fed. Reg. 2051.
[36] 16 C.F.R. § 312.5(a)(1).
[37] 16 C.F.R. § 312.10.
[38] 89 Fed. Reg. 2075.

Protection Act.[39] In order to harmonize with comprehensive state privacy laws, a written data retention policy should not be required to be posted in an online notice or policy. Moreover, if an operator has a data retention program or policy that generally applies, there should be no need for the operator to have a separate child-specific policy.

The Commission also proposes that "personal information from a child may not be retained indefinitely."[40] Revisions to the rule should include exceptions for certain instances of indefinite retention. For example, the Commission should allow for security, fraud and abuse prevention, financial record keeping, complying with legal or regulatory requirements, ensuring service continuity, and instances where with VPC the user has consented to extended retention.

V. Security Assessments

The Commission proposes that operators have a security program that "includes designating an employee to coordinate the information security program; identifying and, at least annually, performing additional assessments to identified risks, as well as testing and monitoring the effectiveness of such safeguards; and at least annually, evaluating and modifying the information security program."[41] Like the concerns expressed about data retention practices, the Commission should not require operators to institute a child-only data security program if an equivalent program already exists broadly.

VI. Contextual Advertising

The Commission asks whether it should make changes to its rules regarding contextual advertising as the current rules permit collection of persistent identifiers for contextual advertising without VPC.[42] Contextual advertising is a long-standing business model that has existed for generations and one of the few remaining ways many content creators under eighteen can support their business. Contextual ads incentivize operators to continue to offer high quality programming content for children. The current rules differentiating contextual advertising and targeted advertising strikes the right balance between protecting children and allowing content to be relevant.

[39] 6-1-1308(3),(4) C.R.S; Va. Code Ann § 59.1-578(1), (2).
[40] 89 Fed. Reg. 2075.
[41] *Id*. at 2061.
[42] *Id*. at 2070 (Question 10).

VII. Effective Date

The Proposed Rule would become effective six months after publication in the *Federal Register.*[43] To give businesses adequate time to comply, we recommend an effective date of two years after publication, which is in line with Europe's General Data Protection Regulation.

VIII. Conclusions

The Chamber agrees with many of the Commission's decisions to make consent more seamless, retain the Actual Knowledge Standard, and provide an exception for audio files in certain circumstances. We stand ready to work with you to ensure an updated COPPA Rule is workable and provides necessary statutory protections for children.

If you have any questions, please contact Jordan Crenshaw at jcrenshaw@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

[43] *Id*. at 2071.