March 11, 2024

By Electronic Filing

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

RE: COPPA Rule Review, Project No. P195404

Dear Secretary Christie:

The Entertainment Software Association ("ESA")[1] and its members strongly support COPPA's goals of "enhancing parental involvement in a child's online activities in order to protect the privacy of children" while also "preserving the interactivity of children's experience on the Internet" and "children's access to information in this rich and valuable medium."[2] The video game industry has made and continues to make significant investments in developing innovative solutions to promote privacy, safety, and parental involvement in children's online video game experiences.

ESA and its members urge the FTC to approach the COPPA rulemaking with an eye towards the existing state of technology, the limitations of the statute, and the perspectives of operators seeking to provide valuable experiences to children online. The FTC should ensure that any changes to the Rule improve the online experience for children and their parents while providing clear, administrable standards for operators that are consistent with previous FTC guidance. While the landscape of children's online experiences continues to evolve, the FTC must respect the limits of its statutory rulemaking authority.

As explained in more detail below, ESA requests that the FTC continue to carefully balance the need to protect children online while ensuring access to the numerous benefits children may derive from online engagement. Specifically,

- Section I requests that the FTC clarify that the proposed rule does not expand the scope of child-directed services;

[1] ESA is the U.S. trade association representing nearly all of the major video game publishers and manufacturers of video game consoles and handhelds. ESA's members deliver high-quality, interactive experiences that promote storytelling, competition, and communication, while maintaining the safety of all video game players, including children, as a top priority.

[2] 144 Cong. Rec. S12787 (1998) (statement of Sen. Bryan).

601 Massachusetts Avenue, NW | Suite 300 West | Washington, D.C. 20001 | www.theESA.com

- Section II explains why the proposed revisions to the already broad definition of "personal information" are unnecessary;
- Section III encourages the FTC to ensure the Rule's consent requirements are helpful to parents and promote positive experiences for children online; and
- Section IV explains why the FTC should avoid burdensome written requirements that provide little value to consumers.

I. The FTC Should Clarify That It Is Not Intending To Expand The Scope of Child-Directed Services.

The FTC correctly decided not to expand the scope of services covered by COPPA, including by rejecting adoption of a constructive knowledge standard. ESA similarly urges the FTC to avoid other proposed interpretations that could have the effect of inappropriately expanding the scope of COPPA beyond its statutory limits. For example, many of the proposals in the NPRM could create ambiguity for operators in determining whether their services are child-directed. These proposals could also inadvertently expand the scope of COPPA, thereby restricting adults' access to online content in a manner that raises constitutional concerns. Accordingly, ESA requests that the FTC reconsider or clarify the proposed changes to the child-directness factors, the age estimation exception, and the mixed audience definition.

A. User reviews and age of users on similar services should not be considered as part of the child-directedness test.

The FTC correctly concluded that the multi-factor test for determining whether a service is child-directed remains the appropriate standard.[3] However, ESA cautions against reliance on user reviews and the age of users on similar sites and services as evidence of audience composition and intended audience. Neither of these data points serve as reliable evidence of child-directedness, and overemphasis on these two factors could therefore lead to arbitrary and capricious results.

First, user reviews do not constitute "competent and reliable empirical evidence regarding audience composition"[4] for a number of reasons. User reviews represent a specific individual's purported experience with the service, not the actual experience of a representative population of users. In addition, because general audience video game platforms might have a diverse range of third-party video game content, a user review based on such third-party content could be misleading about the nature of the overall platform. For example, a user might leave a review for a general audience video game

[3] 89 Fed. Reg. 8, 2046 (Jan. 11, 2024).

[4] 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children" stating that "[t]he Commission will also consider *competent and reliable empirical evidence regarding audience composition* . . . .) (emphasis added).

platform based on their child playing a single child-directed game published by a third party. Such user review should bear no weight on classification of the general audience video game platform. As another example, a parent might leave a user review for a game they purchased for their teen, and refer to their "child" in that review even though the game is not child-directed. Moreover, as the Commission has acknowledged, user reviews are not always made by someone who has actually used the service,[5] further demonstrating the unreliability of user reviews as a measure of child-directedness. Therefore, relying on user reviews is inconsistent with the Rule's mandate to use "competent and reliable empirical evidence regarding audience composition."[6]

The NPRM does not make clear how the FTC would consider user reviews in practice, creating ambiguity for operators in understanding their COPPA obligations. For example, the proposed rule does not state whether it will consider a certain raw number of reviews mentioning children or a percentage of reviews mentioning children as evidence of child-directedness. The proposed rule also does not address whether the FTC will continue to evaluate new user reviews or if child-directedness will be based on a single snapshot in time. User reviews of a video game, for example, may change throughout time as the game becomes popular with different audiences and becomes more nostalgic over time. Moreover, the proposed rule does not address how the FTC will reconcile conflicting user reviews. For example, users may have different views as to whether a game is appropriate for or directed to children — one reviewer may discuss how their child loved the game while another reviewer might discuss the mature content best suited for an older audience. These challenges with considering user reviews as an indicator of a service's child-directedness demonstrate how arbitrary any such finding based on user reviews would be.

Second, age of users on similar sites and services is a vague and arbitrary standard by which to determine child-directedness. The NPRM does not provide any guidance on what is considered a "similar" service. Would two video games be considered similar based on their subject matter, their interactive features, both, or neither? Furthermore, focusing on a comparison to other similar services has no bearing on child-directedness. Two services can be similar without both being directed to the same audience. For example, a car racing game could be targeted to older players based on its visual and audio design while another could be targeted to children. But if both games are fundamentally car racing games, they could be considered "similar" services under this guidance. This standard is too vague to give operators sufficient notice as to whether their service might be deemed child-directed.

Accordingly, the FTC should not consider either user reviews or age of users on similar services as evidence of audience composition in its child-directedness analysis.

---

[5] *See* 88 Fed. Reg. 145, 49370–73 (July 31, 2023).

[6] 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children" stating that "[t]he Commission will also consider *competent and reliable empirical evidence regarding audience composition* . . . .) (emphasis added).

Neither of these are "competent and reliable empirical evidence regarding audience composition."

B. The proposed age estimation exception is unworkable, privacy-invasive, in tension with the statute, and inconsistent with the Rule's multi-factor test for child-directedness.

The FTC correctly declined to modify the definition of "website or online service directed to children" to include an audience percentage based standard.[7] Nevertheless, and seemingly contrary to this decision, the FTC also seeks comment on "whether it should provide an exemption for operators from being deemed a child-directed website or online service if such operators undertake an analysis of their audience composition and determine no more than *a specific percentage of its users* are likely to be children under 13."[8] Even though the FTC frames this standard as voluntary, this proposed age estimation provision would in essence incorporate an audience threshold standard into the child-directed test. While seemingly well-intentioned, such a provision inadvertently could lead to operators collecting more personal information from consumers than they otherwise would need to provide the service and would be challenging to implement in practice. Such a provision would also directly contradict the statutory mandate to consider whether services are "directed" to children, not merely accessed by children.

The age estimation provision is potentially privacy-invasive. The provision could lead operators to collect more personal information than is necessary to provide the service, in tension with the statutory text prohibiting conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.[9] The age estimation provision would seemingly contradict the statutory requirement because operators would need to collect unnecessary age information to take advantage of the exception. For example, a game publisher that collects only username and password for account creation may now feel the need to collect age information and other age verification information solely for purposes of satisfying the age estimation provision. Consumers may be hesitant to use online services that employ age estimation techniques that request additional information, such as a face scan or photo ID, even if that information is used only temporarily and not stored by the service. The Rule should not incentivize collection of unnecessary information that may dissuade consumers from accessing online services or penalize operators who follow best practice data minimization techniques.

The NPRM is not clear on the level of certainty such age estimation would require for an operator to take advantage of the provision, leading to potentially inconsistent and arbitrary application of the provision. For example, a neutral age gate is one method to estimate users' age that is less burdensome to consumers than other

[7] 89 Fed. Reg. 8, 2036 (Jan. 11, 2024).

[8] 89 Fed. Reg. 8, 2070 (Jan. 11, 2024) (emphasis added).

[9] 15 U.S.C. § 6502(b)(1)(C); 16 C.F.R. § 312.7.

601 Massachusetts Avenue, NW | Suite 300 West | Washington, D.C. 20001 | www.theESA.com

age estimation techniques that require hard identifiers. However, self-declared age may be less reliable than a check of a government-issued ID, which is more burdensome for the consumer. Although some automated age estimation technologies, like facial age estimation, can be used to determine the ages (or age bands) of adults, they are not currently as accurate and effective in distinguishing between children and teens as would be necessary to determine audience demographics. There is no consensus on the appropriate method of age estimation that balances accuracy, reliability, and data privacy and security concerns. Congress itself has recognized this fact; the proposed Kids Online Safety Act ("KOSA") would require the National Institute of Standards and Technology to conduct a study evaluating the most technologically feasible methods and options for developing age verification systems.[10] The FTC should leave space for this additional thinking before enacting prescriptive regulations that might not accommodate changes in technology.

Without clear guidelines, a threshold-based provision would be arbitrary and difficult for operators to apply. For example, for game publishers with multiple games offered across different game platforms, it is unclear what the appropriate unit of analysis for the audience composition would be. Different game platforms (*e.g.*, mobile, PC, consoles, handhelds) may have different user age demographics, and it is unclear whether a publisher would need to do separate age estimation for each platform or across these various platforms. The ambiguity in the application of the exception could lead to arbitrary results where operators apply different units of analysis. Additionally, the required analysis would simply provide evidence of user demographics for a certain moment in time. A service's user base may be wildly different at different points of the year, for example, during the school year versus the summer, and this inconsistency may cause an operator to face significant uncertainty in its COPPA obligations.

Although the provision is framed as voluntary, the provision could become a de facto requirement if enough operators in a certain industry take advantage of the provision. The operator who chooses not to engage in age estimation could be placed at a competitive disadvantage because they do not have the benefit of the exception. Operators would be faced with the choice of deploying costly age estimation technologies or otherwise taking a risk that regulators might second-guess their general audience classification and face potential COPPA-liability.

The FTC has previously considered this audience-based threshold issue and decided against it. In 2013, the FTC declined to adopt a per se legal standard that services should be deemed directed to children if audience demographics show that 20% or more of visitors are children under 13.[11] In doing so, the FTC re-affirmed that it will apply the Rule's multi-factor test, recognizing that audience demographics are not available for all sites and services and are not sufficiently reliable.[12] That is still true

[10] Kids Online Safety Act, S. 14909 § 9 (as reported to the Senate on Dec. 13, 2023).

[11] *See* 76 Fed. Reg. 187, 59814 (Sept. 27, 2011).

[12] *Id.*

today. The proposed provision would consider only one factor in the multi-factor test, audience demographics, thereby privileging this factor over all others. Consistent with the statutory mandate, the multi-factor test ensures that only services that are "directed" to children are brought in scope for COPPA, not all services that have a certain percentage of child users.

Accordingly, ESA urges the FTC not to adopt the proposed age estimation provision, instead maintaining the long-standing multi-factor test that appropriately captures the Congressional intent of applying COPPA only to those services that are directed to children.

C. The FTC should revise the "mixed audience" definition to be consistent with the 2013 Amendments.

ESA appreciates that the NPRM indicates the addition of the mixed audience definition is intended only to codify the 2013 Rule Amendments.[13] However, as drafted the proposed definition appears to inadvertently exclude important explanation from the 2013 Statement of Basis and Purpose intended to avoid expanding the scope of services subject to COPPA beyond its statutory and constitutional limits.[14]

Specifically, the proposed definition does not make clear that the FTC applies a two-step process to determine whether a website or online service is mixed audience, to avoid expanding the scope of child-directed services. For example, ESA and other commenters expressed concern in 2012 that the proposed mixed audience designation was ambiguous and unclear as to when a site or service would fall in scope and could expand the scope of COPPA to cover teen-oriented and general audience services that incidentally appeal to children as well as older audiences.[15] In response to ESA's and others' comments expressing such concerns, the FTC explained that "[t]he Commission did not intend to expand the reach of the Rule to additional sites and services, but rather to create a new compliance option for **a subset** of Web sites and online services **already considered *directed to children* under the Rule's totality of the circumstances standard**."[16] To ensure that the mixed audience designation applies only to services that are already considered child-directed under the Rule, the FTC clarified that it will "first apply its 'totality of the circumstances' standard to determine whether any Web site or online service falling under paragraph (3) is directed to children" and *only then* will the FTC consider whether children are the primary or secondary audience.[17] This two-step process ensures that COPPA's reach is not expanded beyond its statutory and constitutional limits; only websites and services that

[13] 89 Fed. Reg. 8, 2037 (Jan. 11, 2024).

[14] 78 Fed. Reg. 12, 3984 (Jan. 17, 2013).

[15] *See id.*

[16] *Id.* (bold emphasis added).

[17] *Id.*

601 Massachusetts Avenue, NW | Suite 300 West | Washington, D.C. 20001 | www.theESA.com

meet the standard for child-directedness considering all the of the Rule's factors will pass the first step and move on to be evaluated for whether children are the primary or secondary audience as the second step.

The NPRM's proposed "mixed audience" definition does not properly codify this two-step analysis. Instead, the definition appears to collapse the analysis of whether children are the primary or secondary audience into the initial child-directedness analysis. This could unintentionally expand the scope of services subject to COPPA. The result would likely be that more services would require users to pass through an age gate or otherwise verify their age before accessing the service, thereby unduly burdening older users' access to constitutionally protected speech.

Furthermore, the definition would appear to eliminate a mixed audience service from utilizing the exceptions to prior parental consent contained in Section 312.5(c) of the Rule. To codify the two-step process, the FTC should revise the definition as follows:

> "Mixed audience website or online service means a website or online service that**, only after applying** the criteria set forth in paragraph (1) of the definition of website or online service directed to children **and determining such website or online service is directed to children**, **also targets children as a secondary audience for the site or service applying the same criteria. Mixed audience websites and online services shall** not collect personal information from any visitor prior to collecting age information or using another means that is reasonably calculated, in light of available technology, to determine whether the visitor is a child**, unless such collection is permitted under Section 312.5(c)**. Any ~~**collection of age information, or other**~~ means of determining whether a visitor is a child~~,~~ must be done in a neutral manner that does not default to a set age **at or above 13 years old** or encourage visitors to falsify age information."

II. The NPRM Proposes Unnecessary Additions To The Already Broad Definition of "Personal Information."

The FTC proposes several additions and clarifications to the Rule's definition of "personal information." The Rule must remain within the statutory bounds enacted by Congress while carrying out the important goals of promoting the privacy and safety of children online. Any expansion of these bounds is a matter for Congress; it is inappropriate to achieve such expansion through this rulemaking. Accordingly, ESA urges the FTC to refrain from adopting the proposed modifications to the definition of "personal information" discussed below.

Specifically, expanding the definition of "personal information" to include *all* screen names and user names — even if they cannot be used to contact an individual online — and the type of "biometric identifiers" proposed in the NPRM exceeds the FTC's statutory authority to add to the definition information that "permits the physical or online contacting of a specific individual."[18] Designating avatars derived from an offline photo of a child would likewise exceed the scope of the FTC's authority, which is limited to information collected online, and would flout the FTC's prior guidance suggesting that photos of children are not personal information if they cannot be used to identify an individual. Finally, though ESA agrees with the FTC's decision not to include "inferred data" in the definition of "personal information," it urges the FTC to clarify that inferred data does not fall within the catch-all provision in the definition of personal information when it is not collected *from* a child.

A. The FTC should maintain its position that screen names and user names that cannot be used to contact an individual online are not "personal information."

In 2013, the FTC correctly declined to add screen names and user names that cannot be used to contact an individual online from the Rule's definition of "online contact information."[19] At that time, ESA and other commentators expressed concern that such a modification would prohibit the use of anonymous screen names or the use of screen or user names to enable, for example, game leaderboards, moderated or filtered chat, and multiplayer game modes.[20] In response, the FTC clarified in the 2013 Rule Statement of Basis and Purpose that the Rule's current definition "permits operators to use anonymous screen and user names" for these purposes and more, including "content personalization, filtered chat, for public display on a Web site or online service, or for operator-to-user communication via the screen or user name."[21]

Restricting the use of anonymous screen names and user names would negatively impact the online experience for children and undermine the data minimization principles underlying COPPA. Many of these screen and user names are automatically generated and assigned by the service, and therefore are unlikely to allow a user to contact another user on another website or online service. Game publishers use screen names and user names that do not facilitate the contacting of an individual as an important means of protecting privacy and to avoid collecting personal information like names and email addresses. However, the proposed change would require operators to collect additional information from a child in order to obtain verifiable parental consent to process anonymous user names and screen names.

---

[18] 15 U.S.C. § 6501(8)(F).

[19] 78 Fed. Reg. 12, 3978–79 (Jan. 17, 2013).

[20] *Id.* at 3979.

[21] *Id.*

Alternatively, some operators may choose not to offer certain services to children at all if they are required to obtain additional personal information and verifiable parental consent to do so. Many operators offer services that allow users to maintain their preferences and progress in a game by using an anonymous user name and persistent identifiers associated with the account. If operators must obtain verifiable parental consent to offer these features, it could deter them from offering their services to children altogether. Losing the ability to save the user's preferences or gameplay history, would significantly impact the experience of video game users, particularly where these features are integral to the experience.

Although the FTC purports to limit the definition to user names and screen names enabling contact on *another* website or service, it is not possible to craft language that would provide operators sufficient clarity on when the Rule is triggered. This standard would seemingly require operators to monitor screen and user names on all other websites and online services. The practical result would likely be that operators would need to treat ***all*** user and screen names as online contact information due to the possibility that there could exist another service that enables online contacting where the user is using the same user or screen name.

Furthermore, the proposed modification would exceed the FTC's statutory authority to add "any other identifier that the FTC determines *permits the physical or online contacting of a specific individual*" to the definition of personal information.[22] The current Rule correctly recognizes that — when an operator uses screen and user names in a manner that does not constitute contacting — such information must be beyond the scope of the FTC's rulemaking authority. ESA urges the FTC to maintain the Rule's specification that screen names and user names are personal information only when the operator itself uses the screen name or user name as online contact information.

B. The NPRM's proposed addition of a "biometric identifier" exceeds the FTC's statutory authority.

The NPRM proposes expanding the Rule's 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."[23]

The COPPA statute explicitly limits the FTC's authority to add other identifiers to the statute's definition of "personal information" to any identifier that "permits the physical or online contacting of a specific individual."[24] The NPRM does not explain how

[22] 15 U.S.C. § 6501(8)(F) (emphasis added).

[23] 89 Fed. Reg. 8, 2041 (Jan. 11, 2024).

[24] 15 U.S.C. § 6501(8)(F).

any of the enumerated biometric identifiers in the proposed definition would allow for the physical or online contacting of a child — nor could it. Instead, the NPRM states in a conclusory manner that "the FTC believes that biometric recognition systems are sufficiently sophisticated to permit the use of identifiers . . . to identify and contact a specific individual either physically or online."[25] While it may be true that biometric recognition systems allow the identification of individuals online via biometric identifiers, that is not the standard required by the statute. Furthermore, it is unclear how the inclusion of "data derived from voice data, gait data, or facial data" would allow the identification of an individual, let alone the contacting of an individual.

Not only would the proposed definition exceed the FTC's statutory authority, it would also be inconsistent with the FTC's 2017 Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, which the NPRM proposes to codify.[26] In the policy statement the FTC clarified that it would not take action against companies that collected voice recordings as a replacement for written words without parental consent and deleted such recordings after a brief period. The proposed definition of biometric identifier is at odds with the policy statement because voice recordings could be considered a biometric identifier as "data derived from voice data." At minimum the FTC should clarify how it proposes to reconcile these two proposals within the NPRM.

Furthermore, the proposed definition of biometric identifier is inconsistent with existing state privacy law definitions of biometric information, which exclude information such as photographs and video or audio recordings. For example, Illinois's Biometric Information Privacy Act ("BIPA") defines a biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[27] The definition explicitly excludes photographs. Even the broader definition of "biometric information" captures information derived from a biometric identifier only where such information on its own could be used to identify an individual. Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Washington laws all exclude audio recordings, videos, and photos from their definitions.[28] Derived data is only considered biometric information where it is used or intended to be used to identify a specific individual. For example, Washington's biometric privacy law defines "biometric identifier" as data "generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific

[25] 89 Fed. Reg. 8, 2042 (Jan. 11, 2024).

[26] Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, 82 Fed. Reg. 235, 58076 (Dec. 8, 2017).

[27] 740 ILCS 14/10.

[28] 4 CCR 904-3 Rule 2.02; Conn. Gen. Stat. § 42-515(3); Del. Code 6 § 12D-102(3); Fla. Stat. § 501.702(4); Ind. Code Ann. § 24-15-2-4(b); Iowa Code Ann. § 715D.1(4); Mont. Code Ann. § 30-14-2801(2)(3)(b); OR SB 619 § 1(3)(b); Tenn. Code Ann. § 47-18-3201(3)(B); Tex. Bus. & Com. Code § 541.001.3; Utah Code Ann. § 13-61-101(6)(c); RCW § 19.375.010(1).

individual."[29] "Biometric identifier" does not include a physical or digital photograph, video or audio recording, or data generated therefrom.

Rather than stretching its statutory authority to fit biometric identifiers into the definition of "personal information," the FTC should defer to Congress on this matter. Congress is currently considering proposed legislation that would amend the COPPA statue. In that proposal, Congress is considering amending the definition of "personal information" to add the language excerpted below that differs from that proposed in the NPRM.

> *Information generated from the measurement or technological processing of an individual's biological, physical, or physiological characteristics that is used to identify an individual, including— (I) fingerprints; (II) voice prints; (III) iris or retina imagery scans; (IV) facial templates; (V) deoxyribonucleic acid (DNA) information; or (VI) gait.*[30]

Significantly, this language does not use the term "biometric" at all and would be limited to information used to identify an individual, an important concept missing from the definition proposed in the NPRM. Furthermore, this language notably excludes photographs and video and audio recordings, hewing more closely to the scope of biometric information prevalent in other privacy laws. Congressional amendments to the statute are the appropriate vehicle for expanding the definition of personal information, and the FTC should avoid taking action via this rulemaking that may conflict with legislative action on this topic.

C. An avatar derived from a child's offline photo should not be considered "personal information."

The NPRM requests comment on whether an avatar generated from a child's image constitutes ''personal information'' under the Rule even if the photograph of the child is not itself uploaded to the site or service and no other personal information is collected from the child.[31] This proposal reaches beyond COPPA's application to information that is collected *online* and is inconsistent with FTC guidance, which affirms that photographs are not personal information if they cannot be used to identify a child.

First, if the photograph of the child is not uploaded to the site or service, the photograph is processed locally on the device to generate the avatar. The FTC previously has recognized that local processing of a child's personal information does not trigger COPPA because the statute requires that personal information must be

[29] RCW § 19.375.010.

[30] Children and Teens' Online Privacy Protection Act, S. 1418, 118th Cong. (2023).

[31] 89 Fed. Reg. 8, 2070 (Jan. 11, 2024).

collected, used, or stored over the Internet.[32] The attempt to reach personal information processed locally exceeds COPPA's statutory limits.

Second, this proposal would be inconsistent with the FTC's own longstanding guidance that operators may blur a child's photo without triggering COPPA or use reasonable filtering tools to otherwise remove personal information before it is publicly posted.[33] Transforming the child's photo into an avatar is akin to removing the personal information from the image itself, since an avatar would no longer contain uniquely identifying markers of the child.

Third, the FTC's original justification for adding photographs to the definition of "personal information" in the 2013 rulemaking was that a photo could "be paired with facial recognition technology" to "'permit the physical or online contacting of a specific individual."[34] Once a photo has been transformed into an avatar, facial recognition technology no longer is able to identify the specific individual. Thus, there is no basis for including photo-generated avatars within the definition of "personal information."

D. The FTC should clarify its "inferred data" position does not conflict with the support for internal operations exception.

ESA supports the FTC's decision not to include "inferred data" in the definition of "personal information" and agrees this modification would have exceeded the statutory bounds of COPPA. Such data is not collected "from" a child even if it may arguably be about a child. However, ESA urges the FTC to clarify its statement that inferred data could fall within COPPA's catch-all "if it is combined with additional data that would meet the Rule's current definition of 'personal information.'"[35] Specifically, the FTC should make clear that such inferred data does <u>not</u> fall under the catch-all provision if it was not collected *from* a child online. The language of the catch-all provision itself makes this clear.[36]

ESA understands the FTC's intent was to restate the existing subsection 10[37] of the Rule's definition of "personal information." To clarify this intent, ESA requests that

---

[32] COPPA FAQ F.5, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[33] 78 Fed. Reg. 12, 3982 n.123 ("The FTC believes that operators who choose to blur photographic images of children prior to posting such images would not be in violation of the Rule"); *see also* COPPA FAQ F.3, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[34] 78 Fed. Reg. 12, 3981 (Jan. 17, 2013).

[35] 89 Fed. Reg. 8, 2042 (Jan. 11, 2024).

[36] 16 CFR § 312.2(10) ("Information concerning the child or the parents of that child that the operator collects online *from* the child and combines with an identifier described in this definition.") (emphasis added).

[37] *Id.*

601 Massachusetts Avenue, NW | Suite 300 West | Washington, D.C. 20001 | www.theESA.com

the FTC clarify that this statement does not undermine the support for internal operations exception, which allows an operator to collect persistent identifiers combined with inferred information in order to support the internal operations of the site or service without parental consent.[38] For example, a video game publisher might combine persistent identifiers with inferred game data (such as skill) in order to match similarly-skilled players for multiplayer game play. Such activity falls within the exception for maintaining and analyzing the functioning of the service. And the combination of such data should not result in the exception being unavailable.

In order to avoid any interpretation that would eliminate the availability of the support for internal operations exception, ESA requests that the FTC clarify the definition of "personal information" as follows:

> "Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition, **except to the extent such information is combined with a persistent identifier and used solely to support internal operations**."

III. The FTC Should Ensure The Rule's Consent Requirements Are Helpful To Parents And Promote Positive Experiences For Children Online.

ESA recognizes the importance of parental involvement in children's online engagement, as evidenced by the numerous parental controls features offered by members. ESA continues to support consent requirements that facilitate parents' involvement in their children's online experiences, including a potential platform-based verifiable parental consent mechanism. However, ESA cautions against changes to the Rule's consent requirements that would be burdensome for parents or limit operators' ability to provide safe experiences for children online. Specifically, ESA opposes the proposal to require separate consent for third party disclosures that are not integral to the service, which could lead to more burdensome and confusing consent flows for parents. ESA also suggests modifications to the proposed support for internal operations disclosure requirement, which would do little to increase transparency for parents while undermining operators' ability to keep their platforms safe.

A. ESA supports the FTC's continued consideration of additional consent mechanisms, including a platform-based approach.

ESA appreciates that the NPRM invites comments on the role platforms can play in enabling verifiable parental consent.[39] ESA continues to believe that gaming platforms can be well positioned to obtain verifiable parental consent that covers the gaming experience available on that platform. ESA encourages the FTC to allow

[38] 16 C.F.R. § 312.5(c)(7).

[39] 89 Fed. Reg. 8, 2070 (Jan. 11, 2024).

platform operators to voluntarily consider implementing platform-based consent mechanisms that are appropriate in light of the technical functionality of the platform and the available games.

Platform-based verifiable parental consent is workable in light of the overall gaming experience. The gaming platform is typically the first point of entry for a new player. Users might create an account for the game platform before accessing any game content, making the platform account creation a convenient moment for parents to receive COPPA notices and provide verifiable parental consent. Publishers can provide information about their practices for the collection, use, and disclosure of children's personal information in a uniform way, such as on game pages where parents and players can access the game for the first time on the platform. These are just some examples of the ways in which a platform-based approach to verifiable parental consent could be workable in the gaming context; operators should be left to determine the exact contours of a platform-based consent mechanism that is best suited to the technical specifications of the platform and the games available on the platform.

Platform-based verifiable parental consent is clearer for parents and consistent with their expectations. When a parent purchases a video game console or subscription to an online gaming service for their child, they necessarily expect that their child will play games on that platform. In ESA members' experience, parents are often confused when, after going through the consent flow for the platform and providing consent for their children to use interactive gaming features, they must again give the game publisher consent for that same purpose. Platform level consent would allow parents to provide the necessary consent for their children to use interactive gaming features in one streamlined set up process.

For example, the platform could provide the baseline notice that the child's personal information will be disclosed to third-party game publishers and application providers who may collect, use, and disclose such information through the platform in order to provide a joint or related service. The platform could then obtain verifiable parental consent for itself and those third-party video game publishers and application providers. The scope of the consent would be made clear to the parent. And if a third-party publisher wanted to collect, use, or disclose the child's personal information in a manner inconsistent with the platform's disclosures, the platform could require the publisher to provide additional notice and to secure a secondary verifiable consent from the parent for such purposes. Third-party publishers could rely on the verifiable parental consent obtained by the platform and would still be responsible for other substantive COPPA requirements, including parental access and deletion rights, data security, and data retention requirements.

Importantly, because the viability of a platform-based consent mechanism will be highly dependent on the specific technical requirements of the platform and associated games, the FTC should not require a platform-based consent. Instead, operators should be free to use the consent mechanism that works best for them, consistent with the requirements of the Rule. Furthermore, if the FTC endorses platform-based consent,

601 Massachusetts Avenue, NW | Suite 300 West | Washington, D.C. 20001 | www.theESA.com

the FTC should make clear that there will be no liability for the platform based on another operator's COPPA violation.

B. The FTC should clarify when and how operators must obtain consent for third-party disclosures.

The NPRM proposes to modify the Rule's consent requirements to require that operators obtain separate verifiable parental consent before they disclose personal information collected from a child to a third party unless such disclosures are integral to the nature of the website or online service.[40] While ESA appreciates the sensitive nature of disclosure of children's personal information, the proposed language is vague both as to when this separate parental consent is required and how operators must obtain such consent.

First, the NPRM does not make clear what types of disclosures to third parties are "integral to the nature of the website or online service." The online video game industry involves both platform operators (*i.e.*, operators of console, handheld, mobile device, and app store services) and game publishers working together to provide the gaming experience. The disclosure of children's personal information between these operators is integral to the functioning of online video game services. For example, for a child user to have a properly functioning experience in a third-party game, the platform operator may need to disclose certain player information along with information such as parental controls and permissions to access certain purchased entitlements along to the game publisher. In the context of game play, neither the platform operator or the game publisher is unknown to the player; the player intentionally interacts with both operators and parents reasonably expect that disclosures between platforms and publishers will occur. Disclosures between game platforms and publishers are thus "integral" to the site or service, and ESA encourages the FTC to recognize such disclosures fall within this exception.

Second, the NPRM does not make clear what it means for an operator to obtain separate consent for the disclosure of a child's personal information to a third party. The proposed modification should not impose requirements that are unreasonably burdensome for parents. For example, a parent should not be required to re-start the verifiable parental consent process from scratch to consent to third-party disclosures. Instead, this separate consent to disclosure could be as simple as an affirmative action the parent must take within the existing verifiable parental consent flow. Another alternative could be for parents to use previously-provided parental passwords or pins to provide this additional consent at a later time. Moreover, many platforms and games have parental controls that allow a parent to control whether their child can disclose personal information to third parties, among other privacy and safety settings. These parental controls are generally accessible only after the parent has gone through the verifiable parental consent flow to create a child's account. Because the parent is taking an affirmative action to allow a child to disclose their personal information *after* the

[40] 89 Fed. Reg. 8, 2051 (Jan. 11, 2024).

parent has already reviewed the operator's direct notice and provided verifiable parental consent, these settings should satisfy the additional verifiable parental consent requirement.

The FTC should avoid any modifications to the Rule that would unreasonably burden parents and inadvertently discourage the use of child accounts that provide safer experiences for children online. Accordingly, ESA proposes the following clarification to the language for Section 312.5(a)(2):

> An operator required to give the parent this option must obtain separate verifiable parental consent to such disclosure, **which includes any affirmative action taken by the parent to authorize such disclosure**, and the operator may not condition access to the website or online service on such consent.

Relatedly, the NPRM also proposes that operators that disclose personal information to third parties should be required to identify those parties (or categories of third parties) and the purposes for which information is disclosed in the direct notice to parents.[41] ESA supports providing parents with the information necessary to make informed decisions about their children's experiences online; however, such provisions are unworkable in contexts like video gaming, where disclosures depend entirely on what games the child selects to play, what features the child chooses to use, and what permissions parents grant via parental controls. For an operator in the video game context to comply with this requirement, the disclosures would need to be written at such a level of generality, similar to the notices described above provided when a parent is consenting to the disclosure of information to third parties. Accordingly, ESA requests that the FTC remove this proposed requirement from the final rule.

C. The FTC should clarify its proposal to prohibit operators from relying on the support for internal operations exception to provide functions that "encourage or prompt use of a website or service."

The NPRM proposes expanding the list of use restrictions in the support for internal operations exception, to prohibit operators from relying on the exception to provide functions that "encourage or prompt use of a website or service."[42] The FTC should not adopt this change because it does not provide adequate notice to operators of the types of functions that are prohibited and would worsen the consumer experience. Moreover, this prohibition would exceed COPPA's bounds and risk conflict with constitutional principles.

The language proposed in the NPRM does not clearly indicate the type of functions and features that are prohibited by the proposed restriction. Read broadly, the

[41] 89 Fed. Reg. 8, 2049 (Jan. 11, 2024).

[42] 89 Fed. Reg. 8, 2045 (Jan. 11, 2024).

proposed restriction could include nearly ***any*** design feature that improves the user experience. A streamlined user experience could be seen as "encouraging" or "prompting" the use of the service by making the service enjoyable. For example, the FTC presumably does not intend to capture use of a persistent identifier to allow a player to level up in a game, but on its face, the language does not appear to explicitly exclude such a broad interpretation. The vague language seemingly could require game publishers to modify core gameplay mechanics depending on the age of the user, potentially compromising the integrity of the game itself. This would be particularly unworkable in the support for internal operations context where publishers intentionally collect minimal personal information from users and thus may not be able to determine the age of the user.

Furthermore, the proposed restriction on using the exception to provide functions that "encourage or prompt use of a website or service" is in tension with aspects of the exception that the NPRM would not disturb.[43] For example, "personalization" is expressly permitted under the support for internal operations exception,[44] as the FTC reaffirmed in the NPRM.[45] Personalization is a key aspect of providing consumers positive experiences with video games and can come in a variety of different forms. For example, players may be able to customize the appearance, personality, and abilities of their game-play character. Other games may be personalized based on the player's gameplay experience; consumers value the ability to develop a history of activity on a service that adapts the content of their gameplay in response to the player's actions. The NPRM seeks comment on the difference between ''user-driven'' personalization and personalization driven by an operator. But this distinction does not appreciate how operator-driven personalization can benefit consumers. For example, another type of personalization might be the use of trust and safety measures such as automated chat monitoring to filter out undesired content. Video game companies use machine learning to identify cheat behaviors, and ensure players can engage in fair, competitive, and productive game play.[46] In addition, an educational game could use personalization to recognize that the player is struggling with math, while doing well in reading, and recommend more math-related content in response.

---

[43] *Id.*

[44] 16 C.F.R. § 312.2.

[45] 89 Fed. Reg. 8, 2045 (Jan. 11, 2024).

[46] Ubisoft, a video game publisher, learned that players were gaining a competitive advantage from using "external input spoofing devices" that allowed them to play with a keyboard and mouse instead of the controller. In response, Ubisoft developed *MouseTrap*, which uses hardware identifiers to add additional latency to penalize players using a keyboard and mouse and encourage them to stop using the cheating devices. Mouse and Keyboard Anti-Cheat Feature on Consoles (Mar. 6, 2023), https://www.ubisoft.com/en-us/game/rainbow-six/siege/news-updates/65UBprZeK2lHJw1qKI8ygM/mouse-and-keyboard-anticheat-feature-on-consoles?isSso=true&refreshStatus=noLoginData .

The NPRM also specifically calls out "machine learning processes" as falling within the scope of the restriction. While it is again unclear what "machine learning processes" the FTC intends to restrict, such a restriction on a certain class of emerging technologies could hamper operators' ability to innovate and provide quality video game experiences for children online. For example, an operator might use machine learning processes to dynamically adjust game dialogue or the skills of a game character in order to improve the game experience. The proposed rule creates too much uncertainty in how such activities would be treated under COPPA, thereby discouraging such innovation.

In addition, the proposed prohibition may extend beyond COPPA's intended scope and raise constitutional concerns. The intent of COPPA was not to regulate how operators design experiences for children online beyond the specific requirements related to the processing of children's personal information. The FTC should not use this rulemaking to implement age-appropriate-design-code-style features that would overstep its statutory authority and congressional intent in order to, for example, restrict the amount of time children spend online. Congress is already addressing this topic in its consideration of KOSA, the current draft of which imposes limitations on "features that result in compulsive usage of the covered platform by a minor."[47] The FTC should defer to Congress on this issue. Furthermore, an overly broad interpretation of this prohibition could also unconstitutionally limit adults' ability to access online content by making sites and services less easy to use (*e.g.*, by limiting personalization).

IV. The FTC Should Avoid Burdensome Written Requirements That Provide Little Value To Consumers.

ESA supports the FTC's goal of protecting children's personal information online and providing transparency for parents. However, certain proposals in the NPRM would create burdensome paperwork and notice requirements for operators while providing little additional value to consumers. In particular, establishing and maintaining a written comprehensive security program specific to the processing of children's personal information may be unduly burdensome for operators that already maintain general data security programs, and the proposed support for internal operations disclosures may create unnecessarily long notices that will not benefit consumers. Accordingly, ESA requests that the FTC reconsider these additions to the Rule.

A. The FTC should clarify that a generally applicable data security program can satisfy the proposed modifications to the Rule.

The NPRM proposes to modify Section 312.8 of the Rule to require that operators, at minimum, must "establish, implement, and maintain a written *children's* personal information security program . . . ."[48] However, the proposed modifications to the Rule are ambiguous about whether operators would be required to establish,

[47] Kids Online Safety Act, S. 1409, 118th Cong. (2023).

[48] 89 Fed. Reg. 8, 2075 (Jan. 11, 2024) (emphasis added).

implement, and maintain a separate written comprehensive security program specific to the processing of children's personal information. Instead, the revisions to the Rule should make clear that a general data security program can satisfy this requirement so long as it considers the sensitivity of children's personal information and implements appropriate safeguards as necessary to address any identified risks.

Requiring a separate written comprehensive security program for children's personal information would be duplicative of existing information security programs, creating unnecessary burdens for operators while providing little value to consumers. Many operators already have implemented the type of comprehensive data security program contemplated by the proposed revisions to the Rule; however, these data security programs might apply to the operator's processing of all types of personal information (including from children) broadly. An existing data security program can take into account the heightened sensitivity of children's personal information and implement appropriate safeguards, without requiring a second, overlapping written security program for children's personal information only. Creating a separate data security program for children's personal information would therefore be redundant, burdensome, and costly. Such costs are likely to be passed on to consumers without providing additional consumer benefit.

Accordingly, the FTC should clarify that a generally applicable comprehensive data security program would satisfy the proposed modified data security requirement, as long as it contains all of the elements described in the NPRM. Specifically, the language should read as follows:

> § 312.8 Confidentiality, security, and integrity of personal information collected from children.
>
> [. . .]
>
> (b) At a minimum, the operator must establish, implement, and maintain a written ~~**children's**~~ personal information security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children and the operator's size, complexity, and nature and scope of activities. **A generally applicable information security program that applies to children's personal information shall satisfy this requirement.** To establish, implement, and maintain a ~~**children's**~~ personal information security program, the operator must:
>
> (1) Designate one or more employees to coordinate the operator's ~~**children's**~~ personal information security program;
>
> [. . .]

> (5) At least annually, evaluate and modify**, if necessary,** the ~~**children's**~~ personal information security program to address identified risks, results of required testing and monitoring, ~~**new or more efficient**~~ **the reasonableness of additional** technological or operational methods **(in light of available technology)** to control for identified risks, or any other circumstances that an operator knows or has reason to know may have a material impact on its ~~**children's**~~ personal information security program or any safeguards in place.

The NPRM also proposes to modify Section 312.10 of the Rule to require an operator to publish its children's data retention policy on its website or online service.[49] ESA urges the FTC to reconsider this proposal. Instead, it should be sufficient for operators to maintain, as part of their written information security program, a retention schedule that covers children's personal information. Operators should not be required to publish such schedules, which could contain proprietary information about how the company operates its business. For example, publishing specific retention schedules regarding information retained for purposes of preventing and detecting fraud, cybersecurity threats, intellectual property infringement, and similar malicious conduct could allow bad actors to take advantage of these disclosures to carry out the actions the operator is attempting to prevent.

In addition, ESA encourages the FTC to clarify the Rule's data retention provision to specifically permit retention where the parent requests it. Specifically, ESA recommends that the FTC revise Section 312.10 of the COPPA Rule as follows:

> When such information is no longer reasonably necessary for the purpose for which it was collected, the operator must delete the information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion**; provided that an operator may retain personal information at the direction of a parent**.

B. The proposed requirement for operators to specify the particular internal operations for which the operator has collected the persistent identifier may be more harmful than helpful to players and parents.

In an effort to provide more transparency to parents, the NPRM proposes to require those operators that utilize the support for internal operations exception to the verifiable parental consent requirement to disclose "the specific internal operations for which the operator has collected a persistent identifier purpose to § 312.5(c)(7)" as well as the means the operator uses to ensure that such identifier is not used for any purposes beyond those that are permissible under the exception.[50] While well-

[49] *Id.*

[50] 89 Fed. Reg. 8, 2074 (Jan. 11, 2024).

intentioned, this additional detail is unlikely to meaningfully benefit parents while potentially harming players. The FTC should modify this proposed requirement to ensure that the Rule appropriately balances the goal of providing transparency with allowing operators to safely operate their services. Specifically, the Rule should only require operators to state for which of the specific activities enumerated in the support of internal operations exception they collect the persistent identifier and should not require the operator to explain the safeguards it uses to prevent the use of the persistent identifier for impermissible purposes.

In the 2011 COPPA Rule NPRM the FTC stated that in separately defining the term "support for internal operations" it "[did] not intend to limit operators' ability to collect" persistent identifiers "to aid the functionality and technical stability" of websites and services.[51] However, the requirement to provide a detailed description of the practices for which the operator has collected a persistent identifier may limit the utility of the support for internal operations exception by impairing operators' ability to enable functionality of their services.

For example, the 2013 COPPA Rule Statement of Basis and Purpose stated that the support for internal operations exception was intended to clarify that operators can use persistent identifiers to "protect[] against fraud or theft."[52] The proposed disclosure requirement could require operators to reveal previously nonpublic information regarding measures taken to protect against fraud. In the video game context, anti-cheat practices are particularly important to ensure fair play and an enjoyable experience, and such practices are only effective if they cannot be easily evaded. If video game operators are required to disclose their anti-cheat practices in significant detail, bad actors could then use these disclosures to thwart the operator's anti-cheat efforts.

Not only would this disclosure requirement thwart the very purposes of the support for internal operations exception, for video game operators this requirement is particularly impractical. The specific purposes for which an operator might rely on the support for internal operations exception will vary from player-to-player and game-to-game depending on the specific functionality the player chooses to use or the parental controls set by the parent. For example, while one player might prefer to play solo, others might choose to play in multi-player mode. Similarly, some games may offer filtered chat, but permit parents to disable this functionality through parental controls.

While ESA members support the principle of transparency, it should be sufficient to describe generally the purposes for which persistent identifiers are used to support internal operations. This disclosure would give parents the information they need to make informed decisions about their children's online information without overwhelming parents with overly technical information. Furthermore, the requirement for the operator

[51] 76 Fed. Reg. 187, 59809–10 (Sept. 27, 2011).

[52] 78 Fed. Reg. 12, 3979 (Jan. 17, 2013).

to explain the safeguards it uses to prevent the use of the persistent identifier for impermissible purposes is unlikely to provide parents with meaningful additional information. The technical and organizational controls that an operator uses to ensure the persistent identifier is only used to support internal operations of the service are not likely to be meaningful to the average parent. Operators are already required to put these measures in place to comply with the Rule and presenting the parent with even more technical information increases notice fatigue. Accordingly, the FTC should clarify that operators need only specify which of the activities enumerated under the support for internal operations exemption justifies the collection of persistent identifiers.

V. Conclusion

ESA and its members remain steadfastly committed to providing children with meaningful online experiences in a safe and privacy-protective manner. We believe that the COPPA statute and Rule are important tools for advancing this goal, and we look forward to working with the Commission in its revisions of the Rule.

Respectfully submitted,

Gina Vetere
General Counsel

Maya A. McKenzie
Senior Counsel, Tech Policy