March 11, 2024

By Electronic Filing
Ms. April Tabor, Secretary
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 Tabor:

The Entertainment Software Rating Board ("ESRB") appreciates the opportunity to provide comments in response to the Federal Trade Commission's Notice of Proposed Rulemaking ("NPRM").[1] Providing parents with the information and tools to protect their children online is at the core of what the ESRB – the non-profit, self-regulatory body for the U.S. video game industry – does every day.

The ESRB's comprehensive age and content rating system and its self-regulatory code have been described consistently by regulators and opinion leaders as the most effective in the entertainment industry in the U.S., if not the world.[2] Its Advertising Review Council actively enforces industry-adopted advertising guidelines to ensure, among other things, that companies do not target advertising for video game products rated "Teen," "Mature," or "Adults Only" to consumers for whom the product is not rated as appropriate.[3] Most relevant to this Rulemaking, our privacy certification and compliance program, ESRB Privacy Certified ("Privacy Certified" or the "Program"), facilitates its members' compliance

[1] Federal Trade Commission ("FTC"), Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking [hereinafter, "NPRM"], 89 Fed. Reg. 2034 (Jan. 11, 2024), https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule.

[2] Max Jay, *FTC: ESRB Has Most Effective Ratings Enforcement*, ENTERTAINMENT SOFTWARE RATING BOARD (July 1, 2018), https://www.esrb.org/blog/federal-trade-commission-finds-that-esrb-has-most-effective-ratings-enforcement/). Indeed, 73% of parents with children that play video games use the ESRB rating system regularly ("every time" or "most of the time") when deciding which video games are appropriate for their kids.

[3] Patricia E. Vance, *Parents: Content is Key When Picking Appropriate Video Games*, ENTERTAINMENT SOFTWARE RATING BOARD (Nov. 10, 2023), https://www.esrb.org/blog/parents-content-is-key-when-picking-appropriate-video-games/.

with privacy laws, rules, and best practices including the Children's Online Privacy Protection Act ("COPPA").[4]

Since 2001, Privacy Certified has served as one of a small number of programs approved by the Federal Trade Commission ("FTC" or "Commission") as a Safe Harbor pursuant to COPPA and its implementing rule ("COPPA Rule"), which sets out the criteria and oversight requirements for the Safe Harbor programs.[5] Nearly every day, Privacy Certified applies COPPA's core principles and granular requirements to the websites, mobile apps, IOT products, downloadable games, and other services (collectively, "products") that our members submit to us for review and certification. Many of the technologies and features these products incorporate and offer did not exist when the Commission last updated the Rule in 2013. We therefore commend the Commission on its nuanced and thoughtful approach to proposing much-needed "modifications . . . intended to respond to changes in technology and online practices, . . . clarify the scope of the Rule and/or strengthen its protection of personal information collected from children."[6]

Privacy Certified's two decades plus of experience with COPPA compliance provides us with a unique vantage point into the issues raised by the NPRM. Our comment, which focuses on the Safe Harbor proposals, is in three parts:

(1) **First**, we respond to the Commission's rule proposals and supplemental questions that relate directly to the Safe Harbor programs. To set our responses in context, we include background information on the Program and our engagement with children's online privacy and safety. We then address the Commission's enhanced recordkeeping and reporting obligations, many of which reflect suggestions we have made in the past. We also respond to the Commission's proposals on data security as they relate to Safe Harbor oversight. Finally, we provide a response to the NPRM's supplemental questions on "conflicts."

(2) **Second**, we draw on our deep familiarity with our members' privacy practices and challenges to provide input on two proposals that fall squarely within our operational COPPA expertise: (1) target audience determination (including the additional evidence for the multi-factor test) and (2) verifiable parental consent ("VPC") methods.

(3) **Third,** we respond to selected supplemental questions not already addressed in our comments on proposed rule text, which relate to screen/usernames and the inclusion of avatars as personal information.

---

[4] COPPA Act, 15 U.S.C. §§ 6501 - 6506 (1998), http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

[5] COPPA Rule, 16 C.F.R. § 312 (2013), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. The COPPA Safe Harbor provisions are at § 312.11.

[6] NPRM, 89 Fed. Reg. 2034.

I. SAFE HARBOR PROPOSALS

The NPRM contains new and enhanced requirements for Safe Harbor programs consistent with the Commission's conclusion that, "[w]hile the Commission continues to believe that FTC-approved COPPA Safe Harbor programs serve an important function in helping companies comply with COPPA, it finds merit in the recommendations for enhanced oversight and transparency."[7] The Commission rightfully acknowledges that self-regulatory programs like Privacy Certified can be an important and effective complement to agency oversight.

In this section, we discuss both the text proposals and the supplemental questions that relate directly to the oversight and transparency of the Safe Harbor programs. First, however, we provide background on our Program in subsection A to provide context for our discussion of the proposed changes. We then address the new proposals on recordkeeping and reporting in subsection B, and respond to the Commission's proposal elevating data security as a core part of the Safe Harbor program in subsection C. Finally, we provide an answer to the Commission's question on ostensible "conflicts" in subsection D.

A. About the ESRB and the Privacy Certified COPPA Safe Harbor Program

Established in 1994 by the Entertainment Software Association,[8] the ESRB is a non-profit, self-regulatory body that independently assigns age and content rating information for video games and mobile apps; educates parents about age ratings, parental controls, and related topics; enforces industry-adopted advertising guidelines; and works with major retailers to help ensure children are not sold video games rated for an older audience without a parent or guardian present.

In 1999, the ESRB saw an opportunity to further its self-regulatory mission by establishing an online privacy certification program to help companies in the video game industry adopt lawful, transparent, and responsible online privacy practices.[9] In April 2001, the Commission approved the ESRB's online privacy program as a Safe Harbor under COPPA.[10]

Since then, the ESRB has continued to develop the Program, which now serves approximately 40 companies in the United States and around the world, mainly in the video

---

[7] NPRM, 89 Fed. Reg. 2034, 2063.

[8] The Entertainment Software Association ("ESA"), a Washington, D.C.-based trade association, serves as the voice and advocate for the U.S. video game industry. *See* ESA, *About Us*, https://www.theesa.com/about-esa/ (last visited Mar. 7, 2024). The ESA is submitting a separate comment in response to this NPRM. Although ESA and ESRB Privacy Certified share some (but far from all) members in common, they have different missions. Each organization's comment reflects its respective purposes and functions.

[9] FTC, *Self-Regulation and Privacy Online: A Report to Congress* (July 1, 1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf.

[10] FTC, Press Release, *Entertainment Software Rating Board Awarded "Safe Harbor" Status* (Apr. 19, 2001), https://www.ftc.gov/news-events/news/press-releases/2001/04/entertainment-software-rating-board-awarded-safe-harbor-status.

game and toy industries. These companies include multinational corporations, startups, and non-profit organizations. Privacy Certified members ("members") operate online services intended for a range of audiences, including some that are for users of all ages, some that are intended for parents or adults only, and some that are created specifically for children under the age of 13.

The ESRB has two separate sets of program requirements: (1) the ESRB Privacy Certified Seal Requirements, which apply to all online services (*i.e.*, websites, mobile apps, internet-connected products, and downloadable games) submitted to the Program for certification that are not primarily directed to and do not target children, and (2) the ESRB Privacy Certified Kids Seal Requirements (the "Kids Seal Requirements"), which apply to online services directed or targeted to children. The Kids Seal Requirements, which are rooted in COPPA, are at the core of the ESRB Safe Harbor Program. Currently, only slightly over one-third of our members use the Kids Privacy Seal on their products. Of these members, only a few use the Kids Privacy Seal exclusively.

Over the years, the ESRB has updated the COPPA Safe Harbor component of the Program to reflect changes in technology, law, and best practices for protecting children's privacy online. The Commission approved modifications to the ESRB's original COPPA Safe Harbor program in 2005, and again in 2013, in conformity with the FTC's amendments to the COPPA Rule.[11] In 2018, the ESRB submitted revised program requirements to the FTC to better align the Program with the Commission's direction.[12]

The ESRB has participated actively in discussions about strengthening children's online privacy and updating COPPA and the COPPA Rule. In 2019, the ESRB submitted extensive comments to the FTC's regulatory review of the COPPA Rule.[13] Reflecting our commitment

---

[11] The Commission approved changes to the COPPA Rule in December 2012, which went into effect in July 2013. The Commission then approved the ESRB's revised COPPA Safe Harbor program when the revised COPPA Rule went into effect. *See* FTC Press Release, *Revised Children's Online Privacy Protection Rule Goes into Effect Today: FTC Continues Safe Harbor Programs, Expands Business and Parental Education Efforts* (July 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect.

[12] Letter from Donald S. Clark, Secretary, FTC, to John M. Falzone, Vice President, ESRB, *re Application of the Entertainment Software Rating Board for Approval of Modifications to its Children's Online Privacy Protection Rule Safe Harbor Program* (Aug. 13, 2018), https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-modifications-video-game-industry-self-regulatory-coppa-safe-harbor-program/p024526_commission_letter_approving_modified_esrb_program_and_exhibit_a.pdf. Exhibit A contains the ESRB's current Privacy Certified Kids Seal Requirements; *see also* Letter from Dona J. Fraser, Vice President, ESRB Privacy Certified to the Honorable Donald S. Clark, Secretary, FTC *Re: Children's Online Privacy Protection Rule: Submission of Amended Safe Harbor (ESRB Privacy Certified Kids' Seal) Program Requirements - RESUBMISSION(Redacted Version)*, https://www.ftc.gov/system/files/attachments/press-releases/entertainment-software-rating-board-awarded-safe-harbor-status/sh_130701esrb_application.pdf.

[13] ESRB, *Comment Submitted by Entertainment Software Rating Board to the COPPA Rule Review, 16 CFR Part 312, Project No. P195404* [hereinafter "*ESRB 2019 COPPA Rule Comment*"] (Dec. 10, 2019), https://www.regulations.gov/comment/FTC-2019-0054-116012. In July 2019, the FTC sought public comment on the effectiveness of the 2013 COPPA Rule amendments and asked for public input on whether additional

to COPPA and the seriousness with which we take our responsibilities as a Safe Harbor provider, we made several suggestions for improving not only the COPPA Rule but also the FTC's oversight over the COPPA Safe Harbor program. These included additional reporting requirements for the Safe Harbors to "help the Commission monitor [Safe Harbor programs] for potential rubber-stamping."[14] We also proposed a "thorough, biennial audit of each Safe Harbor, which could include review of our internal processes and procedures and in-person interviews of all staff involved in the compliance review and certification process."[15] If a Safe Harbor falls short of expectations, we made clear that we "strongly support the Commission's suspending or revoking that company's Safe Harbor status."[16] We subsequently shared those suggestions with members of Congress and other stakeholders.

We also have commented on several COPPA issues raised by the current NPRM. For example, we supported adding biometric information and a broader set of government identifiers to COPPA's definition of personal information.[17] We called for more clarity on the Section 312.2 criteria for determining when an online service is "directed to children."[18] And we included three recommendations for improving VPC, including by permitting "fingerprint and facial recognition, which are already built into parents' mobile devices," expanding "email plus," and exploring "steps to engage platforms in the VPC process."[19]

In the years since the Commission first announced the COPPA Rule Review, ESRB has continued to call for additional privacy protections for children as well as teens. In response to the Commission's 2022 call for public comment on its *Advanced Notice of Proposed Rulemaking for Commercial Surveillance and Lax Data Security Practices*,[20] we submitted copious comments focusing on the questions the Commission raised about privacy for children and teens, including whether the Commission ought to go "beyond COPPA" to protect their privacy.[21] There, we discussed the value of rigorous self-regulation

---

changes were needed in light of "continued rapid changes in technology." FTC Press Release, *FTC Seeks Comments on Children's Online Privacy Protection Act Rule* [hereinafter "*2019 COPPA Rule Review*"] (July 25, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule.

[14] *ESRB 2019 COPPA Rule Comment*, supra note 13, at 5.

[15] *Id*.

[16] *Id*.

[17] *Id*.

[18] *Id.* at 6. In particular, we explained that ESRB's age and content ratings "have been used improperly and out-of-context to support the argument than an online service is directed to Children." *Id.* at 7. We therefore asked the Commission to make clear that, "An age rating that shows a video game or mobile app does not contain content that would be inappropriate for Children (e.g., E and E10+) should not be considered when assessing whether a video game or mobile app is directed to Children for purposes of COPPA."

[19] *Id.* at 8.

[20] FTC, *Trade Regulation Rule on Commercial Surveillance and Data Security: Advanced Notice of Proposed Rulemaking* [hereinafter, "ANPR"], 87 Fed. Reg. 51273 (Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[21] ESRB, *Comment Submitted by the Entertainment Software Rating Board on the FTC's Advance Notice of Proposed Rulemaking on "Commercial Surveillance and Data Security"* [hereinafter, "*ESRB 2022 Commercial Privacy Comment*"] (Nov. 21, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1117.

in the privacy and data protection context, including technical compliance and certification mechanisms (such as Safe Harbor programs) and enforceable codes of conduct.[22] We also drew on our experience as a Safe Harbor to suggest a "multilayered, inclusive, and nuanced" model for protecting the data of children and teens.[23] Finally, we urged the Commission to consider promulgating more specific data security standards for children's data.[24]

More recently, in June 2023, Privacy Certified, along with Yoti Ltd. (and Yoti (USA) Inc.) and Kids Web Services Ltd., requested that the FTC approve a new VPC mechanism known as "Privacy-Protective Facial Age Estimation" to respond to "advances in digital technologies."[25] Our application explained how the proposed method complies with COPPA Rule requirements and provides an "accurate, reliable, accessible, fast, simple, and privacy-preserving mechanism for ensuring that the person providing consent is the child's parent."[26] That application is currently pending before the Commission, with a decision expected on or before March 29, 2024.[27]

B. The Safe Harbor Recordkeeping and Reporting Proposals

The NPRM proposes several amendments to the recordkeeping and reporting requirements in Section 312.11 (d). We first discuss the enhanced requirements relating to the annual

---

[22] *ESRB 2022 Commercial Privacy Comment*, *id*. at 4-12.
[23] *Id*. at 14-20.
[24] *Id*. at 20-24.
[25] ESRB, *Application for Approval of a Verifiable Parental Consent Method Pursuant to the Children's Online Privacy Protection Rule 16 C.F.R. §312.12(a)* [hereinafter, "*ESRB VPC Application*"] (June 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf. ESRB filed the application together with Yoti Ltd. (and Yoti (USA) Inc.) and SuperAwesome Ltd. Yoti is a digital identity company that offers identity verification, age assurance, reusable digital identity, and e-signature solutions around the world. At the time of filing, SuperAwesome operated the Kids Web Services platform to facilitate developers' compliance with the parental consent requirements of COPPA as well as the EU's General Data Protection Regulation. In January 2024, KWS became an independent company Kids Web Services Limited, separate from SuperAwesome Ltd. It is now a wholly owned subsidiary of Epic Games.
[26] *Id*. at 1.
[27] The FTC published the application in the Federal Register and solicited public comment via supplemental questions in July 2023. *See* FTC Press Release, *Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method: Request for Public Comment*, 88 Fed. Reg. 46405-46706 (July 21, 2023), https://www.federalregister.gov/documents/2023/07/20/2023-15415/childrens-online-privacy-protection-rule-proposed-parental-consent-method-application-of-the-esrb. The comment period closed on August 21, 2023. The rule requires the Commission to respond to such applications within 120 days. On September 25, 2023, the FTC extended the deadline by 120 days. FTC Press Release, *FTC Extends Deadline for Commission Decision on ESRB Application for New Consent Mechanism Under COPPA* (Sept. 25, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-extends-deadline-commission-decision-esrb-application-new-consent-mechanism-under-coppa. On January 29, 2024, the Commission further extended the deadline for decision by another 60 days. FTC Press Release, *FTC Extends Deadline by 60 days for Commission Decision on ESRB Application for New Consent Mechanism Under COPPA* (Jan. 29, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-extends-deadline-60-days-commission-decision-esrb-application-new-consent-mechanism-under-coppa.

report the agency requires the Safe Harbor programs to file each year. Many of these requirements reflect suggestions ESRB made in 2019 to prevent "potential rubber-stamping" by Safe Harbor programs. Some of these new requirements are already part of the FTC-provided template that Safe Harbors must use in preparing their annual reports. Not surprisingly, therefore, we strongly support most of the proposed changes, although we do raise some concerns about requirements that do not appear to advance the Commission's oversight. We then discuss the Commission's proposal to require the Safe Harbor programs to publish their member lists and update them every six months. This proposal would not advance transparency and would likely mislead consumers. Finally, we comment on the Commission's proposal for the Safe Harbor programs to submit a triennial report, a requirement we support.

1. Annual Report Proposals (Proposed § 312.11(d)(1)(i) – (iv))

The NPRM retains some of the recordkeeping and reporting requirements from the 2013 Rule and adds several new or enhanced requirements. The first new reporting requirement, in Section 312.11(d)(1), would require Safe Harbor programs to annually "identify each subject operator and all approved websites or online services in the program, as well as all subject operators that have left the safe harbor program."[28] The second would require a "narrative description of the safe harbor program's business model, including whether it provides additional services such as training to subject operators."[29] As we indicated in the *ESRB 2019 COPPA Rule Comment*, we strongly favor enhanced reporting requirements that can help the Commission oversee the Safe Harbor programs. These two requirements certainly fall into that category, and, as the Commission is aware, the ESRB and the other Safe Harbors already provide such information to the Commission as required in the FTC-provided template for the Safe Harbors' annual confidential reports.

The NPRM also modifies the current Rule's requirement for Safe Harbor operators to maintain for three years consumer complaints alleging violations of the guidelines by subject operators and to make those complaints available to the Commission upon request.[30] In place of this provision, it adds new Section 312.11(d)(1)(ii), which would require Safe Harbors to submit "each consumer complaint related to each subject operator's violation of a safe harbor program's guideline" as part of the annual report.[31] Although we do not object to this requirement, we question whether it would provide any additional information for the Commission that it could not readily obtain under the current version of the Rule.

First, the FTC can already access any complaints under the current version of the Rule. Privacy Certified already provides aggregate information about the complaints it receives to the Commission as part of the annual reporting requirement. The Commission could

[28] NPRM, 89 Fed. Reg. 2034, 2076 (proposed § 312.11(d)(1)).
[29] *Id.* (proposed § 312.11(d)(1)(i)).
[30] COPPA Rule, 16 C.F.R. § 312.11(d)(3)(i)).
[31] NPRM, 89 Fed. Reg. 2034, 2076.

simply require the Safe Harbors to turn over any complaints it had questions about after reviewing the annual reports.

Second, for the past three years (and even beyond), the ESRB has not received any consumer complaints alleging violations of COPPA or our Safe Harbor program guidelines. Although our current Kids Privacy Certified Seal requirements are available online (including on the FTC's Safe Harbor website), we do not expect consumers to be familiar with our program requirements or to cite them in their complaints.[32] We construe any consumer complaints we receive broadly to determine if the consumer has alleged a violation of COPPA or our program requirements.

Indeed, our analysis of the 3,670 emails and other communications from consumers that we received over the past three years shows that nearly two-thirds of the emails we received were unrelated to privacy or to compliance with our Kids' Seal (or general privacy) program requirements.[33] Instead, they mainly related to customer service issues, including requests to reset passwords, complaints about banned accounts, requests for refunds, general game-play matters, and product suggestions.

Of the roughly one-third of emails that did relate to companies' privacy practices, most of them were from users who wanted to delete their accounts or update their personal information. We also received emails from users claiming their accounts were hacked and a small number from people receiving unsolicited commercial messages. Even in this group, a significant number of complaints related to the privacy practices of companies that are not members of our program or products that we do not certify. Others alleged lack of compliance with technical requirements of laws like the European Union's General Data Protection Regulation or the California Consumer Privacy Act, not COPPA.[34] Also, many of the communications we received were not specific enough for us to identify the online service about which the consumer complained. Although we respond to such complaints by requesting additional information, we often do not receive it.

Third, the paucity of actionable privacy complaints exists despite our best efforts to provide consumers with information on how they can contact us and file complaints. The ESRB requires its members to include our public email address (privacy@esrb.org) and the URL for our complaint form (https://www.esrb.org/privacy/contact/) in their privacy policies.[35] We also require members to provide a description of the Program along with text informing users that they can email us with privacy complaints. Our complaint form is easy to locate

---

[32] *See COPPA Safe Harbor Program*, FTC, available at https://www.ftc.gov/enforcement/coppa-safe-harbor-program (last visited Mar. 7, 2024).

[33] This analysis is based on summaries of the complaints that we received between in the past three years. We have provided this information to the FTC in our annual Safe Harbor reports.

[34] We do not expect consumers to be familiar with COPPA, ESRB's Kids Seal program requirements, or any particular privacy law. Therefore, when a consumer alleges a violation of another privacy statute or raises any type of privacy issue, we consider whether it also raises a COPPA concern.

[35] *ESRB Privacy Certified Kids Seal Requirements*, supra note 12.

on our website.[36] It is also available from our Kids' Seal FAQs.[37] It is not confusing or cumbersome to complete – after choosing the complaint filing option from a drop down menu it prompts the consumer to enter the URL or app name of the product the consumer is complaining about and provides a box for them to enter a free-text complaint. Despite all this, we receive very few complaints that are actually about companies' privacy practices. Therefore, the collection of actual complaints is not "necessary for the proper performance of the functions of the FTC" nor will it have "practical utility" as required by the Paperwork Reduction Act.[38] However, if the Commission does include this requirement in its Final Rule, it should require the Safe Harbor programs to redact any personal information from the complaints that it submits under this new subsection.

Similarly, the NPRM adds a requirement in Section 312.11(d)(1)(iv) for Safe Harbors to provide a "description of the process for determining whether a subject operator is subject to discipline."[39] This is in addition to the requirement in the current Rule to provide "a description of any disciplinary action taken against any subject operator under paragraph (b)(3) of this section."[40] Here, too, we fail to understand how this additional requirement is necessary to help the Commission determine whether the Safe Harbor programs are appropriately disciplining their members. In the template the Commission provides to the Safe Harbors for the annual reports, the Commission requires the Safe Harbors to explain the process they use to determine whether and when an operator found to be out of compliance with Safe Harbor guidelines is subject to discipline. As with copies of complaints, this collection of information does not appear to be necessary for the Commission to perform its oversight functions.

If the purpose is simply to make this explicit in the Final Rule, the Commission should make clear that both the requirement to report disciplinary action and the further requirement to describe the process only applies to the formal disciplinary measures set out in Section 312.11(b)(3) of the COPPA Rule and does not require Safe Harbor programs to report on every instance of non-compliance with COPPA's requirements. Safe Harbors and their members should not be held to a "perfection" standard. Requiring Safe Harbor programs to disclose every remedial action they take would be self-defeating and dissuade companies from joining Safe Harbor programs.

---

[36] *See Get in Touch*, ESRB, https://www.esrb.org/privacy/contact/ (last visited Mar. 7, 2024).
[37] *See Kids Seal Requirements FAQs*, ESRB, https://www.esrb.org/privacy-certified-seals/#what-if-i-have-a-complaint-about-the-service-2 (last visited Mar. 7, 2024).
[38] 89 Fed. Reg. 2034, 2065 (requesting Paperwork Reduction Act responses).
[39] NPRM, 89 Fed. Reg. 2034, 2076 (proposed § 312.11(d)(1(iv)).
[40] *See* 16 C.F.R. § 312.11(d)(1) (stating that approved Safe Harbor programs shall, on an annual basis, "submit a report to the Commission containing, at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section, a description of any disciplinary action taken against any subject operator under paragraph (b)(3) of this section, and a description of any approvals of member operators' use of a parental consent mechanism, pursuant to § 312.5(b)(3).") The Commission's proposal would reorganize the existing requirement to report disciplinary actions and the new requirement to describe the process into a new, standalone section.

Through our biannual reviews and random checks of our members' certified products and services, Privacy Certified issues (at least) two reports per year per member describing what changes the member must make for their certified products and services to remain compliant with the Kids Seal Requirements. We often identify issues that are technically non-compliant but are often inadvertent and easily remedied. We then work with our members to implement tailored, privacy-protective solutions to the issues we identify in our review.[41] Requiring our members to take prompt remedial action when we identify issues usually averts the need for more formal disciplinary measures. We see no reason for the COPPA Rule to require us to describe the iterative process we engage in with our members to remediate these issues.

If a clear violation were to exist and the member company were to fail to remedy it or to communicate its plans to remedy it, we would withdraw certification of the impacted online service and require our seal to be removed. Likewise, if the member appeared to attempt to mislead us purposefully or had repeated and/or enduring instances of non-compliance of a similar and serious nature, termination of the member's participation in the Program and other potential discipline likely would be warranted. In such cases, under the existing Rule, we would provide the Commission with information on the disciplinary measure and the process that led to our imposition of such a measure.

2. Publication of member names (Proposed § 312.11(d)(4))

Apart from the enhanced recordkeeping and reporting requirements, the NPRM would add a new paragraph, Section 312.11(d)(4), requiring Safe Harbor programs to "publicly post a list of all current subject operators on each of the approved safe harbor program's websites and online services" and update that on a six-month basis.[42] In our view, such a requirement would not benefit consumers and could even mislead them into believing that all products and services provided by the company have been certified as compliant by the Safe Harbor. Like many of the Safe Harbor programs, Privacy Certified certifies products, not companies. The choice whether to submit a product to the Program for certification belongs to the member. A public list of operators would not provide consumers with relevant information about certification or the privacy features of the products they might wish to purchase.

The risk of misleading consumers is even greater in the context of mobile apps. Certifications may differ for products that are part of the same overall title but appear on different platforms or have different privacy features. When we certify apps, we do so on a platform-by-platform basis because there may be issues that are iOS-specific that do not impact Android-based users (or vice versa).

[41] This includes, for example, reconfiguring or removing a third-party cookie or SDK (software development kit), adding or fixing an age gate (based on reassessment of the target audience for a member's product), adding or revising privacy disclosures based on new features introduced into a product, or upgrading security measures such as encryption protocols.

[42] NPRM, 89 Fed. Reg. 2034, 2076 (proposed § 312.11(d)(4)).

Moreover, we do not see any evidence in the record that would support such a requirement other than a few assertions that such a requirement would lead to more "transparency."[43] As we explained in the *ESRB 2019 COPPA Rule Comment*, we have yet to find any empirical evidence suggesting that consumers would find such a list helpful. That remains the case. In our experience, it is more likely that a consumer will look for the seal at the point they encounter or download one of our members' products, than they will go to each of the six authorized Safe Harbor websites to see if the publisher of the product is the member of a Safe Harbor and whether the specific product they wish to purchase has received a COPPA Safe Harbor certification.

Indeed, we question whether the coalition of consumer groups that purportedly found it "difficult" to locate Safe Harbor seals actually shopped for video games and toys that bear the ESRB Kids Privacy Certified seal.[44] As noted above, our seal requirements state that a member that has been awarded the Kids Seal must provide, on the relevant website's home page and on any other pages where personal information and data is collected from children, a prominent and clearly labeled link to its privacy statement. The Kids Seal must be posted near the link to the privacy statement. For mobile apps, we have long required that our members post a link to the privacy policy, with our seal, that a consumer can review before downloading the app. Consistent with these requirements, our Kids Seal features prominently on certified websites' home pages, mobile apps' storefront pages and in-app settings screens, packaging for IOT products, and on other products that we certify.

The Kids Seal in turn links to a confirmation page hosted on the ESRB website, which confirms the company is a member of the Program, shows the seal(s) the member is approved to use, and provides a link to the member's online privacy statement(s). In 2020, the ESRB added to all member confirmation pages a link for consumers seeking more information about the EPC seals.[45] The link takes consumers to a page with information about the seals and additional, in-depth FAQs that explain the types of online services to which each seal applies, the requirements that must be met to display each seal, and what to do if a consumer has a question or complaint.

If the Commission desires to address complaints about "whether and where subject operators display membership seals,"[46] it could instead set out more specific criteria in the Rule for seal display (and related information about the seal). This could range from a

---

[43] NPRM, 89 Fed. Reg. 2034, 2064 n. 347.

[44] NPRM, 89 Fed. Reg. 2034, 2064 n. 350. A coalition of consumer groups supported greater transparency and argued that FTC-approved COPPA Safe Harbor programs' current practices with respect to whether and where subject operators display membership seals makes it difficult for parents and others to determine whether websites or online services are participants of an FTC-approved COPPA Safe Harbor program. The only example they provided was for an entertainment company that uses a different Safe Harbor than ESRB. There, the company did not post the approving Safe Harbor's seal on the home page of the websites that the consumer groups reviewed. The remedy for this omission, however, as discussed herein, is not to require the Safe Harbor operator to publish a list of members but rather to mandate more specific requirements for the use and placement of seals and related information.

[45] *Privacy Certified Seals*, ESRB, https://www.esrb.org/privacy-certified-seals (last visited Mar. 7, 2024).

[46] *NPRM,* 89 Fed. Reg. 2034, 2064 n. 350.

requirement that operators display Safe Harbor program seals in a "clear and conspicuous" manner to specific placement instructions. If the Commission wishes to encourage transparency even further – and determines that this would benefit consumers – the Commission could consider establishing a database containing all products certified by the Safe Harbor programs (similar to the RN Database maintained by the FTC) that consumers could easily search.[47]

There are other mechanisms as well, unrelated to operators' lists or to seal display that could promote transparency. For example, the FTC could issue a report based on anonymized, aggregated information from the approved Safe Harbors.[48] This could provide more transparency into how the COPPA Safe Harbors supplement FTC monitoring and enforcement as well as emerging compliance issues and challenges. The agency has used this method in many of its Section 6(b) reports on industry practices.[49]

3. Triennial Reports (Proposed § 312.11(f))

Along with the additional annual report requirements, the NPRM proposes a new Section 312.11(f), requiring each Safe Harbor program to submit a triennial report that details the program's "technological capabilities and mechanisms for assessing subject operators' fitness for membership in the safe harbor program."[50]

The ESRB welcomes this requirement. In fact, we proposed a biennial report in our *2019 ESRB COPPA Rule Review Comment*.[51] It would be helpful, however, for the FTC to set minimum expectations for Safe Harbor programs' technological capabilities and assessment mechanisms. For example, the Commission could require that all Safe Harbor programs use technology capable of detecting advertising trackers on child-directed products. It could also require all assessments to be preserved in writing for a specified time period. These types of standards would assist the Safe Harbors in preparing the triennial report and promote consistency among the approved programs.

---

[47] The FTC has done this in other contexts. For example, the RN database, located on the FTC's website, contains a list of all U.S. businesses that manufacture, import, distribute, or sell products covered by the Textile, Wool, and Fur Acts. *See* RN Database, FTC, available at https://rnftc.gov/Account/BasicSearch (last visited Mar. 7, 2024).

[48] As we explain in Section I.D below, the agency could also review the Safe Harbor programs' fee schedules and lists of other charges (if any) by the Safe Harbor program or their affiliates, as part of the triennial review. This could help ensure that inappropriate financial incentives do not undermine the integrity of the Safe Harbor program.

[49] *See, e.g.*, FTC Staff Report, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf. We do not suggest that the Commission would need to use its information gathering powers under Section 6(b) of the FTC Act. Here, the FTC would already have such anonymized, aggregated information from the Safe Harbor programs' annual reports and could use its oversight authority to request additional information, if needed.

[50] NPRM, 89 Fed. Reg. 2034, 2076 (proposed § 312.11(f)).

[51] *ESRB 2019 COPPA Rule Comment*, supra note 13, at 5.

C. Data Security (Proposed § 312.8(b)-(c), § 312.11(b)(2))

The NPRM proposes changes to the Rule's data security provision in Section 312.8(b), adding new, detailed elements to the existing requirement that operators use "reasonable procedures" to protect the confidentiality, security, and integrity of personal information from children.[52] Among the elements, the proposal would require operators to have a written children's data security program, appoint a data security coordinator, perform at least annual data security assessments on internal/external threats and sufficiency of safeguards to control risks, implement and test these safeguards, and evaluate and modify their information security programs on an annual basis.[53] The proposed Rule further requires that operators that release personal information to other operators or third parties obtain written assurances that the recipient will employ reasonable measures to maintain the confidentiality, security, and integrity of the information.[54]

The FTC's proposal is in line with our call for the Commission to create stronger, "enforceable standards for children's data" through the current COPPA rulemaking.[55] In the *ESRB 2022 Commercial Privacy Comment*, we advocated that any expanded data security requirements, whether promulgated as part of the COPPA Rule, a new trade regulation rule, or as additional guidance, should be "clear and consistent[,] aligned with existing laws, guidance, and industry practices[,] and not overly prescriptive." [56] In general, the Commission's proposals meet these standards, although we are concerned that some of the proposed requirements might create unnecessary burdens for operators without providing corresponding benefits for consumers.

In particular, we are concerned about the effect on our members, especially our smaller program members, of what we interpret as a requirement for a separate written children's data security policy and a separate data security coordinator in Section 312.8(b).[57] We have similar concerns about the proposed requirement for an operator to establish and maintain a written children's data retention policy in proposed Section 312.10.[58] When an operator already has comprehensive written data security and data retention policies in place, we see no reason for requiring a separate policy or program as long the overarching policies account for the heightened sensitivity of children's data and the operator implements corresponding measures. As we previously explained, "What may be essential for a multinational corporation may not be a feasible approach for a startup." [59] Accordingly, in promulgating a Final Rule, the Commission should adhere to its own statement that COPPA's data security safeguards should be "appropriate to the sensitivity of children's information and to the operator's size, complexity, and nature and scope of activities" and

---

[52] 16 C.F.R. § 312.8.
[53] NPRM, 89 Fed. Reg. 2034, 2075 (proposed § 312.8(b)).
[54] NPRM, 89 Fed. Reg. 2034, 2075 (proposed § 312.8(c))).
[55] *2022 ESRB Commercial Privacy Comment*, supra note 21, at 23-24.
[56] *Id.* at 23.
[57] NPRM, 89 Fed. Reg. 2034, 2076 (proposed § 312.11(b)(2)).
[58] NPRM, 89 Fed. Reg. 2034, 2075 (proposed § 312.10).
[59] 2022 ESRB Commercial Privacy Comment, supra note 21, at 22.

permit operators to maintain one comprehensive data security policy and program so long as it meets the requirements set out in the NPRM.[60]

In parallel with the proposed changes to Section 312.8(b), the NPRM seeks to amend Section 312.11(b)(2) to elevate data security as a Safe Harbor program responsibility to co-equal with privacy. In particular, the proposed Rule states that the effective, mandatory mechanisms for independent assessment of subject operators' compliance with a Safe Harbor programs' guidelines must include, at a minimum, a "comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information privacy and security policies, practices, and representations" (emphasis added).[61] The NPRM explains that the Safe Harbor programs can use the guidance that accompanies the proposed changes to Section 312.8 to determine whether subject operators meet the new requirements.[62]

As we stated in the *2022 ESRB Commercial Privacy Comment*,

> "[W]e cannot overstate the importance of ensuring strong safeguards for children's and teens' data. As children and teens spend more and more time online, for studying, entertainment, and communication, their personal data is increasingly at risk of being hacked, stolen, and sold, potentially leading to severe consequences both online and offline. Although it is virtually impossible to guarantee the complete security of online information, additional action by the FTC in this area . . . would incentivize companies to provide better data security and would help them comply with their obligations."[63]

Nonetheless, we believe that the guidance in the proposed Rule does not provide the Safe Harbor programs with sufficient clarity regarding their enhanced responsibilities. In particular, the language of the proposed Rule could force the Safe Harbor programs to bear responsibility for data security policies and practices that go far beyond those implicated by the products they certify. This could essentially compel the Safe Harbor programs to become specialists in overseeing each operator's company-wide IT systems, policies, and practices (as well as those of the vendors who access the company's systems), and their cybersecurity teams.

We therefore request that the Commission remove the phrase "and security" from Section 312.11(b)(2) to avoid enlarging the Safe Harbor programs' responsibilities beyond recognition. If the Commission does not choose to do so, then we request that it include

---

[60] NPRM, 89 Fed. Reg. 2034, 2061.

[61] NPRM, 89 Fed. Reg. 2034, 2076 (proposed § 312.11(b)(2)).

[62] NPRM, 89 Fed. Reg. 2034, 2061.

[63] *ESRB 2022 Commercial Privacy Comment*, supra note 21, at 24. There, citing the FTC's recognition in the ANPR that, "[H]arms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology," we proposed that "any data security standard should allow for flexibility and industry-specific permutations. *Id.* at 23 (internal citations omitted).

more concrete guidance in the Final Rule on how Safe Harbor programs can meet the proposed Rule's requirement that the programs' comprehensive independent assessments include both privacy and security without forcing the programs into a role that extends so far beyond their mandate that they essentially will need to become data security systems auditors.

Simply put, conducting macro-system-wide independent assessments of an operator's data security program requires a different type of specialized knowledge and different types of technological tools than privacy reviews require.[64] In conducting its independent privacy assessments, the ESRB uses tools that can detect the collection of personal data not otherwise apparent to a user (e.g., precise location coordinates, device identifiers), reveal the use of tracking technologies (e.g., cookies, pixels), and identify basic security-related issues (e.g., expired certificates, collection of personal data over nonsecure protocols). We manually review and analyze all such scans. But analyzing whether an operator has put in place reasonable safeguards to prevent, detect, mitigate, and recover from system-wide cyberattacks and data hacks – and evaluating whether they have sufficiently tested, monitored, and modified these safeguards – would require a very different type of expertise and technology. And this does not account for the type of access Safe Harbor would require to operators' systems, which many of the operators might limit for precisely the security reasons the Rule is intended to address. For the proposed revision to be operationally feasible, the Safe Harbors should be permitted to rely on subject operators' evidence and documentation about their cybersecurity programs, including independent cybersecurity certifications (if they have them), as well as the results of penetration testing by external validators.

To be clear, we do not seek to shirk our Safe Harbor responsibility to ensure that our members have in place reasonable procedures to protect the confidentiality, security, and integrity of children's personal information. Our Kids Seal Program Requirements already contain a specific section dedicated to data collection and security, which require members to:

- Use appropriate, commercially reasonable methods such as encryption to protect personal information and data;
- Release personal information and data only to service providers and third parties capable of maintaining the confidentiality, security, and integrity of such information;
- Assure that personal information and data is up-to-date, complete, and accurate;

[64] The Commission does not include an estimate of the time or costs required for Safe Harbor programs to implement this responsibility fully in its estimates of the additional recordkeeping, reporting, and labor needed to comply with the Final Rule. In our experience, the time and costs of conducting the same type of in-depth assessments that we currently conduct for our members to review their privacy policies and practices would be double, if not more, if we were required to conduct "comprehensive" system-wide assessments of operators' data security programs.

- Implement reasonable, user-friendly, clear, and effective processes and/or mechanisms that allow users to correct material inaccuracies in personal information and (such as account or contact information);
- Provide details regarding how personal information is gathered and tracked;
- Avoid and, if applicable, cease the collection of any unused personal information and data; and
- Disclose to consumers how their personal information and data is being used, as well as the relevant security measures in place.[65]

Outside of these core security requirements, we look for and raise known data security vulnerabilities in our compliance reviews and member communications. We enforce these requirements by testing for the following elements when we review products for initial certifications and in our ongoing monitoring:

- Whether personal data is collected and transferred over a secure connection;
- Whether the browser flags any security-related issues (e.g., expired security certificates, unsafe scripts);
- Whether an email provider (e.g., Gmail) flags any security-related issues for emails received by our test accounts;
- Whether account set-up, and particularly password, practices are secure; and
- Whether additional consumer-side security features are available (e.g., two-factor authentication).

Accordingly, as set out above, we ask that the Commission remove the phrase "and security" from Section 312.11(b)(2) or include clarifying language to help the Safe Harbor programs assess whether its members are complying with the Rule's new data security requirements. The Commission's statement in the NPRM that its approach "provides additional guidance to operators and FTC-approved Safe Harbor programs, while also maintaining the Rule's flexibility by allowing for technological advancements and taking into account an operator's size, complexity, and the nature and scope of its activities" is simply not enough.[66] The Commission should provide the Safe Harbor programs with multiple pathways for oversight that do not require the Safe Harbor programs to become the guarantors of a company's data security system.

D. Conflicts of Interest

The last Safe Harbor issue we address relates to the NPRM's Supplemental Question 19 (Safe Harbor), which asks,

[65] *ESRB Privacy Certified Kids Seal Requirements*, supra note 12.
[66] NPRM, 89 Fed. Reg. 2034, 2061.

> What types of conflicts would affect an FTC-approved COPPA Safe Harbor program from effectively assessing a subject operator's fitness for membership in the FTC-approved COPPA Safe Harbor program? What policies do FTC-approved COPPA Safe Harbor programs have in place to prevent such conflicts?[67]

Implicit in this question is the assumption that conflicts of interest are inherent in the COPPA Safe Harbor program. That is not true.

Indeed, the FTC advocated for, and Congress designed, the Safe Harbor program to mitigate such risks.[68] As we explained in the *ESRB 2022 Commercial Privacy Comment*, self-regulation exists on a continuum, with the COPPA Safe Harbors falling more into a co-regulatory model than a pure self-regulatory model.[69] Unlike industry led self-regulatory schemes that do not incorporate strong governmental oversight, Congress empowered the FTC to set minimum standards, approve the Safe Harbor programs' substantive requirements, and oversee the Safe Harbor programs through the annual report and other information gathering powers.[70] Congress also provided the agency with the authority (which the FTC has exercised) to withdraw a Safe Harbor program's authorization.[71]

Despite the agency's robust oversight of the Safe Harbor programs (which the Commission is seeking to enhance through this NPRM), critics of self-regulation generally and the

---

[67] NPRM, 89 Fed. Reg. 2034, 2071 (Supplemental Question 19).

[68] In its testimony on the draft COPPA legislation, the FTC testified that, "The Commission believes that a key objective of any legislation should be to encourage development and implementation of meaningful, effective self-regulatory activities and to provide a basis for their widespread adoption." S. 2326, *Children's Online Privacy Protection Act of 1998: Hearing Before the S. Subcomm. on Communications of the S. Comm. On Com., Sci., and Transp.*, 105th Cong. 11 (1998) (statement of Robert Pitofsky, Chairman, FTC), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protection-childrens-privacy-world-wide-web/priva998.pdf.

[69] *ESRB 2022 Commercial Privacy Comment*, supra note 21, at 7.

[70] *Id.*

[71] 16 C.F.R. § 312.11(f) ("The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part."). In 2021, the FTC revoked the authorization of former COPPA Safe Harbor provider, Aristotle International, for failing to fulfill its statutory obligations and public responsibilities as a COPPA Safe Harbor. FTC Press Release, *Aristotle Removed from List of FTC-Approved Children's Privacy Self-Regulatory Programs* (Aug. 4, 2021), https://www.ftc.gov/news-events/press-releases/2021/08/aristotle-removed-from-ftc-approved-childrens-privacy-programs. Outside the COPPA context, the FTC has also sued TRUSTe (now TrustArc), a privacy seal program, for failing to conduct annual recertifications of companies using its privacy seals despite representing to the public that companies awarded such seals receive recertification every year. FTC Press Release, *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program* (Nov. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its. Several years later, New York's Attorney General entered into a settlement with TRUSTe for failing to conduct adequate scans on its customer's web pages for third-party tracking technologies prohibited by COPPA. *See* N.Y. State Office of the Att'y Gen, A.*G. Schneiderman Announces $100,000 Settlement With TRUSTe Over Flawed Privacy Certification Program for Popular Children's Websites* (Apr. 6, 2017), https://ag.ny.gov/press-release/2017/ag-schneiderman-announces-100000-settlement-truste-over-flawed-privacy. The FTC aided the New York Attorney General's Bureau of Internet and Technology in that matter.

COPPA Safe Harbor program specifically have raised the issue of financial conflicts. Indeed, one former FTC Commissioner raised the issue of financial conflicts in the context of an enforcement action, arguing that the Commission should "limit[] conflicts of interest by COPPA Safe Harbors by restricting additional fee-based consulting offered by affiliates of the Safe Harbor to participating websites and apps."[72]

A key role of a Safe Harbor program is to provide guidance and input to members on their privacy policies and practices to enable them to comply with COPPA. Therefore, the ESRB would not recommend that the FTC categorically prohibit Safe Harbor programs (or their affiliates) from providing any type of consulting services to its members. That said, if the Commission were to permit this type of consulting, it should institute transparency reporting requirements to ensure that Safe Harbor programs that engage in this conduct are accountable to the FTC. This could include, for example, a requirement for the Safe Harbor programs (and their affiliates) to submit their fee schedules and lists of other charges (such as consulting fees) for review as part of the triennial review mandated by proposed Section 312.11(f). This requirement could help prevent inappropriate financial incentives that could undermine the integrity of the Safe Harbor program.

For our own part, however, the ESRB does not provide, either directly or indirectly, fee-based COPPA consulting services to its Safe Harbor members. Instead, we charge a variable annual membership fee dependent on a member company's revenue, to cover the costs of our activities. We do not charge our members higher annual fees for the Kids Seal or any COPPA-related service we provide, such as scanning network traffic, compiling third-party service provider lists, and vetting third-party service providers in child-directed products.[73]

II. OPERATIONAL PERSPECTIVE ON RULE CHANGES

Apart from the proposals relating to the COPPA Safe Harbor Program, the NPRM proposes numerous changes to the 2013 Rule to "clarify the scope of the Rule and/or strengthen its protection of personal information collected from children."[74] As with the Safe Harbor proposals, several of the proposed changes reflect recommendations we made in

---

[72] *See Statement of Commissioner Rohit Chopra Regarding Miniclip and the COPPA Safe Harbors Commission File No. 1923129* (May 18, 2020), https://www.ftc.gov/system/files/documents/public_statements/1575579/192_3129_miniclip_-_statement_of_cmr_chopra.pdf. In *Miniclip*, the Commission brought an enforcement action against a company that misrepresented that it was certified by the Children's Advertising Review Unit (CARU), another FTC-authorized Safe Harbor program, when, in fact, CARU had terminated Miniclip's participation in its program.

[73] Recognizing that some of our members use our services more than others, ESRB recently introduced a two-tier fee structure, which allows members to choose between standard and premium membership categories. The standard membership covers everything necessary for a member to obtain and maintain a COPPA certification for the products it submits for certification. Members who elect the premium category do have a higher product allowance than members in the standard category.

[74] NPRM, 89 Fed. Reg. 2034.

response to the 2019 COPPA Rule Review.[75] Others involve pure policy issues, which industry, consumer groups, academics, and others are already debating. We do not comment on many of the Commission's proposed changes here. Instead, we focus on the two on which we believe our operational perspective would be particularly useful: (A) target audience determination and (B) methods for VPC mechanisms.

A. Target Audience Determination (§ 312.2 - Definition of website or online service directed to children)

The COPPA Rule sets forth a multi-factor test for determining whether a service is "directed to children" so that COPPA protections apply. As the ESRB's decades-long experience reviewing thousands of online services shows, however, that determination is far from straightforward. In the ESRB's 2019 COPPA Rule Comment, we asked the Commission to provide more clarity on this threshold issue.[76]

In the NPRM, the Commission recognizes ESRB's request for more direction, echoed by many other commenters. The FTC proposes adding a "non-exhaustive list of examples of evidence the Commission will consider in analyzing audience composition and intended audience."[77] To accomplish this, the Commission proposes adding the following sentence to the definition of "website or online service directed to children" in Section 312.2: "The Commission will also consider competent and reliable empirical evidence regarding audience composition and evidence regarding the intended audience, 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."[78] We agree that marketing and promotional materials, as well as representations to consumers and third parties, could constitute "competent and reliable" evidence that augments the "child-directed" determination. The last two factors, "reviews by users or third parties" and the "age of users on similar websites or services" do not, however, rise to that level and should be excluded from the Final Rule.

As the Commission is aware, consumer reviews can be unreliable, biased, and even fake.[79] It is often impossible to verify that the authors of user reviews are users of the product they endorse, let alone to determine whether such reviews were written by children or adults.

---

[75] For example, the ESRB supported adding biometric identifiers, such as fingerprint and facial geometry scans, which are used to identify children as a category of personal information. It also supported expanding the definition of government identifiers to include "passport numbers, alien registration numbers, and other potential government identifiers that could be used to identify Children," noting that we had already made this change in our program requirements. *See ESRB 2019 COPPA Rule Comment*, supra note 13, at 5-6.

[76] *Id.* at 6.

[77] NPRM, 89 Fed. Reg. 2034, 2047.

[78] NPRM, 89 Fed. Reg. 2034, 2072 (proposed § 312.2).

[79] *See* FTC Business Blog, *FTC and endorsements: Final revised guides, a proposed new rule, and an updated staff publication* (June 30, 2023), https://www.ftc.gov/business-guidance/blog/2023/06/ftc-endorsements-final-revised-guides-proposed-new-rule-updated-staff-publication. The FTC has brought numerous enforcement cases involving misleading or fake reviews, and is currently conducting a rulemaking proceeding on fake reviews.

Reviews by third parties can also be inaccurate, biased, or simply factually incorrect. Including this factor as one of the indicia for determining whether a product is "child directed" is especially problematic for the ESRB given the long history of third parties conflating the ESRB's age and content ratings with COPPA's child-directed multi-factor test.

Indeed, many third parties have mistakenly charged that the ESRB's "E for Everyone" and "E10+" age ratings, which indicate that the content of a video game or mobile app is generally appropriate for all ages, means that the product is child-directed for COPPA purposes. In fact, the ESRB assigns these designations to many mobile apps directed to adults (such as travel apps, maps and navigation apps, ride-sharing apps, general and financial news apps, stock tracker apps, live event ticketing apps, retailer apps, and card games) because those apps do not contain content that would be inappropriate for children under ESRB's rating criteria; not because they meet COPPA's multi-factor test.

Even ESRB's own rating search app, which is rated "E for Everyone," has been wrongly characterized as "child-directed." ESRB's rating search app is intended to provide parents and guardians with information to make informed choices about age-appropriate games for their children to play. [80] Nothing about the app meets the other factors of the multi-factor COPPA test. Nonetheless, several years ago, a third party that conducts child-directed assessments of apps available in the Apple App and Google Play stores included ESRB's rating search app on a list of child-directed apps.

Similarly, using the "age of users on similar sites and services" would not qualify as competent and reliable evidence. From a factual perspective, it can be difficult to determine what constitutes a "similar" site or service or to discern the true ages of the users on a second service. In the video game context, what factors would the Commission consider to determine "similarity"? Game category or theme would be overbroad; the categories of "action," "battle royale," or even "role-playing" games all include a wide variety of games, some that are more popular among children than others. The same is true of other features that the Commission might use to make such a determination. From a legal perspective, evidence of "similar" services is relevant to a "constructive knowledge" standard; not an "actual knowledge standard."[81] As the Commission acknowledges elsewhere in the NPRM, "Congress did not intend for the 'actual knowledge' standard to be read to include the concept of constructive knowledge."[82] Accordingly, absent Congressional action, the Commission should not include evidence about the age of users on similar sites and services as part of the non-exhaustive list of evidence set forth in the definition of "website or online service directed to children" in Section 312.2.

---

[80] ESRB App, ENTERTAINMENT SOFTWARE RATING BOARD, https://www.esrb.org/tools-for-parents/mobile-app/ (last visited Mar. 7, 2024).

[81] Indeed, in the NPRM, the Commission cited to a comment urging the Commission to "consider current and historic audience composition evidence of both the specific service and similar services in determining whether an operator has met the actual knowledge standard." NPRM, 89 Fed. Reg. 2034, 2037 (citing comment by 5Rights Foundation) (emphasis supplied).

[82] *Id.*

B. Methods for Verifiable Parental Consent Mechanisms (Proposed § 312.5(b))

The NPRM proposes several changes to VPC mechanisms, namely codifying specific consent mechanisms it had previously approved and eliminating the monetary transaction requirement (and requiring only notice) when an operator obtains consent through a parent's use of a credit card, debit card, or an online payment system.[83] The ESRB supports these changes.

In discussing the many comments about the existing VPC mechanisms, the Commission wrote:

> [T]he Commission continues to believe that the Rule's current approach to verifiable parental consent is appropriate and sound. With respect to the more general concerns that COPPA's consent methods create "friction," the Commission stresses that COPPA requires a balance between facilitating consent mechanisms that are not prohibitively difficult for operators or parents, while also ensuring that it is a parent granting informed consent, rather than a child circumventing the process. In response to commenters indicating that this friction has discouraged operators from creating services or caused operators to change their practices, the Commission welcomes the development of methods that prove less cumbersome for operators while still meeting COPPA's statutory requirements.[84]

The Commission also noted that it would "welcome[] further explanation detailing the necessity and practicality of any recommended new consent method, including how it would satisfy the Rule's requirements."[85]

In June 2023, ESRB filed a Section 312.12(a) application, together with Yoti and KWS, requesting that the Commission approve a new method of VPC, known as privacy-protective facial age estimation.[86] The proposed method analyzes the geometry of the face of a parent or legal guardian to confirm that they are an adult capable of providing VPC. It does not entail any scanning of a child's face or entail any estimation or verification of a child's age. As the application explains, "Privacy-Protective Facial Age Estimation offers parents an easy way to provide VPC through a quick process, without needing to provide extensive personal information, in line with data minimization principles."[87] Indeed, the

---

[83] NPRM, 89 Fed. Reg. 2034, 2074 (proposed § 312.5(b)(ii) (eliminating monetary transaction); proposed § 312.5(b)(vi) (adding knowledge-based authentication questions); and proposed § 312.5(b)(vii) (adding facial matching to verified photo identity method).

[84] NPRM, 89 Fed. Reg. 2034, 2052.

[85] *Id*.

[86] See Section I.A, herein, for a description of the pending application.

[87] *ESRB VPC Application*, supra note 25, at 13.

proposed method meets the Commission's call in the NPRM for methods that are "less cumbersome for operators while still meeting COPPA's statutory requirements."[88] We also mark the Commission's statement that "operators are free to develop and use any [VPC] method that meets the standard contained in § 312.5(b)(1) and to tailor their approach to their own individual situation."[89] We respectfully request that the Commission consider adding language in the Final Rule to address the possibility of an operator using – or a Safe Harbor program approving – such a method, believing in good faith that it meets the Rules' requirements only to have the Commission (or another COPPA enforcer) later disagree.

In particular, we request that the Commission amend current Section 312.5(b)(3), which allows a Safe Harbor program to approve its member operators' use of a VPC method if it determines that the method meets the requirements of the Rule, to provide for an expedited authorization process for VPC applications filed by the Safe Harbor programs and/or to provide an exemption from liability and an opportunity to cure any violation for a company that uses a new VPC mechanism based on a good faith approval by their Safe Harbor program. This could encourage more innovation although it is unlikely that we would approve a precedent-setting method of VPC without specific authorization from the Commission.

Finally, we request clarification of the Commission's position on text messages as a potential VPC mechanism. In the NPRM, the Commission discussed the large number of comments that proposed new methods for VPC, including recommendations to allow operators to use text messages to obtain consent from parents. The NPRM cites to comments noting that "text messages are a common alternative to email for verification purposes" and arguing that "text message-based consent is no weaker than consent initiated through the collection of an email address."[90] In response, the Commission stated that it "agrees with the recommendation to modify the Rule to allow the use of text messages to obtain consent."[91] It wrote, however, that this would be best achieved through its proposed modification to include mobile telephone numbers to the definition of "online

[88] The Commission's proposed addition of "biometric identifiers" to the Rule's definition of personal information in Section 312 should not affect the pending VPC application. Simply put, the addition of biometric information to the Rule's definition of personal information only affects operators' collection of information from the child online, not an operators' collection of information from a parent or guardian for VPC purposes. As the FTC has made clear in the COPPA FAQs, "COPPA only applies to personal information collected online from children, including personal information about themselves, their parents, friends, or other persons." FTC, *Complying with COPPA: Frequently Asked Questions* A.8, FTC, available at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Mar. 7, 2023). Nothing in the proposed definition would preclude the Commission from approving a VPC method involving the collection of non-identifying age estimation information from a parent.

[89] NPRM, 89 Fed. Reg. 2034, 2052.

[90] NPRM, 89 Fed. Reg. 2034 2051-52 & 2052 n. 206.

[91] NPRM, 89 Fed. Reg. 2034, 2052-53.

contact information" definition in Section 312.2. It therefore declined to modify the text of Section 312.5(b)(2)(ii).[92]

This disconnect between the Commission's statements in the NPRM, which might lead some to believe that the Commission has endorsed text messages as a VPC method, and the Commission's decision not to modify the text of the Rule, has caused considerable confusion. Although we interpret the Commission's statement that it is not adding any new methods of VPC proposed in 2019 comments in the Rule as a decision that it is not permitting operators to use text messages for VPC, the language is murky. Accordingly, we ask the Commission to clarify in the Final Rule that the addition of a parent's mobile number to the definition of online contact information is for the sole purpose of allowing companies to contact a parent, via text for the purpose of initiating a VPC flow.

III. RESPONSES TO SELECTED SUPPLEMENTAL QUESTIONS

In this last section, we provide brief answers to selected supplemental questions included in the NPRM for which the Commission has not proposed modifications to the Rule. We also focus on issues we have encountered in our Safe Harbor compliance assessments because the questions themselves explicitly relate to video game companies.

Question 4 ("Definitions"): *In conjunction with the 2013 Amendments, the Commission acknowledged that screen and user names have increasingly become portable across multiple websites or online services, and that such identifiers permit the direct contact of a specific individual online. Through the 2013 Amendments, the Commission defined personal information to include screen or user names only to the extent these identifiers function in the same way as "online contact information" as the Rule defines that term. Since 2013, the use of screen and user names has proliferated across websites and online services, including on online gaming platforms that allow users to directly engage with each other. The Commission is concerned that children may use the same screen or user name on different sites and services, potentially allowing other users to contact and engage in direct communications with children on another online service.*
(a) Should screen or user names be treated as online contact information, even if the screen or user name does not allow one user to contact another user through the operator's website or online service, when the screen or user name could enable one user to contact another by assuming that the user to be contacted is using the same screen or user name on another website or online service that does allow such contact?
(b) Are there measures an operator can take to ensure that a screen or user name cannot be used to permit the direct contact of a person online?

ESRB Answer: We oppose treating screen or user names as online contact information when they do not rise to the level of "online contact information" by enabling users to

[92] *Id.* In the section of the NPRM addressing the "online contact information" definition, the Commission stated that "permitting parents to provide consent via text message would offer them significant convenience and utility." NPRM, 89 Fed. Reg. 2034, 2040. It stated that "operators should be able to collect parents' mobile telephone numbers as a method to obtain consent from the parent." *Id.*

contact one another as currently set out in the Rule. The Commission made the correct decision in 2013 when it limited the requirement for operators to obtain VPC for user or screen names only to such names that rose to the level of "online contact information" and not to situations when an operator used "anonymous screen and user names in place of individually identifiable information" for purposes such as "content personalization, filtered chat, for public display on a website or online service, or for operator-to-user communication via the screen or username."[93]

Indeed, the Commission explicitly rejected its original 2011 proposal to include screen or user names as personal information when "such screen or user name is used for functions other than or in addition to support for the internal operations of the Web site or online service."[94] Significantly, the Commission was persuaded by comments that its original proposal would run counter to data minimization principles that protect children's data and unnecessarily inhibit functions that are important to the operation of child-directed Web sites and online services.[95] The Commission explained:

> The Commission has long supported the data minimization purposes behind operators' use of screen and user names in place of individually identifiable information . . . Moreover, after reading the comments, the Commission is persuaded of the benefits of utilizing single sign-in identifiers across sites and services, for example, to permit children seamlessly to transition between devices or platforms via a single screen or user name. The Commission therefore proposes that a screen or user name should be included within the definition of personal information only in those instances in which a screen or user name rises to the level of online contact information.[96]

The same rationale that supported the Commission's previous decision applies with equal force today. Our members use screen names, in lieu of identifiers with personal information, to post results on online game leaderboards, moderate or filter chat sessions, and enable multiplayer games. (Many do this for adults as well as children to preserve their users' privacy.)

We are not aware of any empirical evidence supporting the Commission's supposition that the "proliferation" of new services necessarily means that "children may use the same screen or user name on different sites and services . . . ."[97] Indeed, some of our members – especially those that operate services directed to children – limit children to selecting

---

[93] FTC, Children's Online Privacy Protection Rule, 2013 Statement of Basis and Purpose, 78 Fed. Reg. 3972, 3978 -79, 3998 (Jan. 17, 2013), https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule.

[94] 78 Fed. Reg. 3972, 3998.

[95] *Id*.

[96] FTC, Children's Online Privacy Protection Rule: Supplemental Notice of Proposed Rulemaking; Request for Comment, 71 Fed. Reg. 46643, 46646 (Aug. 6, 2012), https://www.govinfo.gov/content/pkg/FR-2012-08-06/pdf/2012-19115.pdf.

[97] NPRM, 89 Fed. Reg. 2034, 2070.

display names from drop-down menus of choices, e.g., using colors and animals to set up "Purple Puppy," rather than allowing alphanumeric entry while others assign children randomly generated screen or user names. Many have measures in place to ensure that children cannot pick screen or user names that contain personal information (such as a street address or telephone number). Some members also allow children to change their screen names on a regular basis.

Besides the lack of empirical evidence supporting the Commission's concerns, it would be extremely unfair to create a rule that would impose liability on operators who do not allow child users to contact other users or who enact measures similar to those we describe above to ensure that screen names are random and do not contain personal information. Accordingly, we see no basis for the Commission to make any modifications to the definition in the current Rule.

Question 6 ("Definitions"): *The use of avatars generated from a child's image has become popular in online services, such as video games. Should an avatar generated from a child's image constitute "personal information" under the COPPA 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? If so, are these avatars sufficiently covered under the current COPPA Rule, or are further modifications to the definition required to cover avatars generated from a child's image?*

ESRB Answer: ESRB does not believe that further modifications to the definition of personal information are required to address avatars created from a child's image. Photorealistic avatars created from a photo or video of a child and stored or used online (even if the avatar is created locally from a photo on a user's device rather than via an upload to an online site or service) would be covered by the Rule to the extent that they are an immutable extension of the child and would be characterized or perceived as a photo of an identifiable child.

In general, however, most avatars are not photorealistic and are not immutable or static. Children adorn avatars with all sorts of features (e.g., eye color changes, hair colors) as well as clothes, jewelry, and other accessories and constantly change them. Therefore, it would be difficult to imagine how such avatars could qualify as individually identifiable information under the COPPA Rule's definition of personal information, especially if the operator collected no other personal information from the child and did not combine the avatar with other personal information collected from the child.

Question 20 ("Effective Date"): *As part of the issuance of the initial Rule and the 2013 Amendments, the Commission stated that the Rule and amended Rule, respectively, would become effective approximately six months after issuance of the Commission's final rule in the* ***Federal Register****. (Emphasis in original.) The Commission requests comment on whether such timeframe is appropriate for the modifications set forth during this Rule review that do not specify an effective date.*

ESRB Answer: Based on the wide variety of changes proposed in the NPRM, we believe that a one-year time frame would be more reasonable than the proposed six months. Some of the provisions, such as the proposed second VPC requirement for targeted advertising and the enhanced data security obligations, could require operators to engage in substantial design, engineering, development, and testing activities.

We note further that the NPRM does not set a date for the Safe Harbor programs to modify and resubmit their guidelines to the FTC, instead stating that the Commission will provide an "appropriate deadline."[98] Therefore, we respectfully request that the Commission set at least a six-month deadline following its issuance of the Final Rule, for such submissions to give the Safe Harbor programs adequate time to modify their program requirements and their accompanying policies and procedures, as well as to educate their members on the Final Rule's requirements.

CONCLUSION

As an FTC-approved Safe Harbor, the ESRB works every day to develop and implement effective privacy protections for children and their data. We are committed to working with the Commission to modernize and strengthen COPPA's existing protections for children through the Rule review process. We appreciate the opportunity to submit this comment and welcome further engagement, including by answering additional questions and providing more information to the FTC.

Respectfully submitted,

Stacy Feuer
Senior Vice President, ESRB Privacy Certified
Entertainment Software Rating Board

[98] NPRM, 89 Fed. Reg. 2034, 2064.