epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

"Children's Online Privacy Protection Rule: Entertainment Software Rating Board's Safe Harbor Program Application to Modify Program Requirements"

Project No. P024526

May 9, 2018

By notice published on April 5, 2018, the Federal Trade Commission ("FTC") requests public comments on proposed modifications to the self-regulatory guidelines of the Entertainment Software Rating Board ("ESRB"), under the safe harbor provision of the Children's Online Privacy Protection Act ("COPPA") Rule.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that children's online privacy is adequately protected in response to changing technology and business practices. We commend ESRB's revised definition of "Personal Information and Data" to reflect the Amended COPPA Rule of 2013,[2] and clarifications to Section VII.A. of the self-regulatory guidelines to require data minimization.

However, several other proposed modifications diminish privacy safeguards and fall below the requirements of the COPPA Rule.[3] We urge the Commission to reject ESRB's proposals which (1) narrow the definition of "Children" to only residents of the United States, (2) terminate "Privacy Risk Assessments" and "Initial Self-Assessment Questionnaires," (3) diminish notice requirements, and (4) change "must" to "should" to demote obligations to mere recommendations. Given the sensitivity of children's personal information, it is imperative for

---

[1] Federal Register, A Proposed Rule by the FTC (83 FR 14611), *Children's Online Privacy Protection Rule Safe Harbor Proposed Self-Regulatory Guidelines; the Entertainment Software Rating Board's COPPA Safe Harbor Program Application to Modify Program Requirements* (April 5, 2018), https://www.federalregister.gov/documents/2018/04/05/2018-06976/childrens-online-privacy-protection-rule-safe-harbor-proposed-self-regulatory-guidelines-the

[2] FTC, *Children's Online Privacy Protection Rule: Final Rule Amendments to Clarify the Scope of the Rule and Strengthen Its Protections for Children's Personal Information*; 16 C.F.R. Part 312 (January 17, 2013), https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf

[3] 16 C.F.R. § 312.11 Safe Harbor Programs: Program requirements must ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

the FTC to implement and enforce the strongest standards for self-regulatory program guidelines under § 312.11 of the COPPA Rule.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC.[4] Since 1995, EPIC has pursued many of the critical online privacy issues concerning children.[5] We have testified before lawmakers in support of strong privacy safeguards for children.[6] EPIC has also filed complaints with the FTC detailing unfair and deceptive trade practices that put children's privacy at risk.[7] We have long advocated for the COPPA Rule to place meaningful limits on emerging technologies and business practices that extend data collection on children, and urged the FTC to vigorously enforce its provisions. This is a sensible approach that recognizes both the unique vulnerabilities of young children and the limitations of a self-regulatory approach which would place an unreasonable burden on young minors to interpret privacy policies and make informed decisions about the disclosure and use of personal information.[8]

I. Definition of "Personal Information and Data"

1. Modifications in Support of 2013 Amendments to the COPPA Rule

In Section I of the Proposed Requirements,[9] ESRB has revised the definition of the term "Personal Information and Data" ("PID") to mean "any information relating to an identified or

[4] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[5] EPIC, *EPIC Letter to Christine Varney on Direct Marketing Use of Children's Data* (December 14, 1995), *available at* http://epic.org/privacy/internet/ftc/ftc_letter.html.
[6] EPIC, *Children's Privacy Protection and Parental Empowerment Act: Hearing on H.R. 3508 Before the Subcomm. On Crime of the H. Comm. On the Judiciary*, 104th Cong (1996), (statement of Marc Rotenberg, Executive Director, EPIC), *available at* https://epic.org/privacy/kids/EPIC_Testimony.html.
[7] EPIC, *Children's Online Privacy Protection Act (COPPA)*, https://epic.org/privacy/kids/; *See also*, EPIC, *In re Echometrix (Complaint, Request for Investigation, Injunction, and Other Relief)*, https://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf; EPIC, *In re Facebook and the Facial Identification of Users (June 10, 2011)*, Request for Investigation of COPPA Violations in Facebook's Facial Scanning of Children, https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf; EPIC, *Complaint In re Universal Tennis to the FTC* (May 17, 2017), Complaint on COPPA Violations in the Secretive Scoring of Young Athletes Without Parental Consent, https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf; EPIC, *In re Genesis Toys and Nuance Communications (December 6, 2016)*, Complaint on COPPA Violations in "Toys that Spy", https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf
[8] *An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA): Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the Sen. Comm. Commerce, Science, and Transportation*, 111th Cong. (Apr. 29, 2009) (statement of Marc Rotenberg, Director, EPIC), at 2-5 (hereinafter Rotenberg Testimony), available at http://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.
[9] Entertainment Software Rating Board, *Application Filed Pursuant To Section 312.11 of the Children's Online Privacy Protection Rule, Requesting Approval of Modifications to the Entertainment Software Review Board Privacy Certified Kids Seal Requirements Under Section 312.11(e) of the Rule* (March 13, 2018) (Submitted to Donald Clark, Office of the Secretary, FTC) (hereinafter *Proposed Requirements*), *available at* https://www.ftc.gov/system/files/attachments/press-releases/ftc-seeks-comment-proposed-modifications-video-

identifiable individual collected online." This definition modifies the previous guideline which narrowly defined "Personally Identifiable Information" ("PII") as "any information that can be used to identify an individual or which enables direct contact with an individual."[10]

The revised definition of PID encompasses data points that may not be independently capable of identifying a person, but nonetheless relate to an identifiable person. This proposal internalizes important amendments to the updated COPPA Rule of 2013, which EPIC supported for adding new categories of information to the definition of "personal information" to address technological changes and pervasive data practices:

> The proposed regulation adds several new categories of information to the definition of "personal information" contained in 16 C.F.R. § 312.2: a "screen or user name," "persistent identifier" or "identifier that links the activities of a child across different Web sites or online services," "photograph, video, or audio file," and "Geolocation information." These new categories represent important improvements to the COPPA Rule.[11]
>
> […] The proposed regulations also consider persistent identifiers, such as cookies and IP addresses, to be personal information, regardless of whether they are paired with other identifying information. Again, this change reflects changes in technology and consumer behavior that have resulted in particular devices being increasingly associated with particular individuals. Furthermore, the rise of online behavioral advertising, the majority of which is accomplished through persistent identifiers, makes this addition to the COPPA Rule particularly important.[12]

ESRB's proposed modification also adds "including, but not limited to" before listing examples of information that qualify as PID.[13] This clarification is critical to preventing web operators and social network sites from alleging an exemption to COPPA requirements by disputing the scope of application, particularly on the definition of covered personal information.

Self-regulatory guidelines should be frequently updated to anticipate new methods of extensive data collection, and standard-setting bodies like the ESRB should adopt privacy-protective interpretations of COPPA for emerging technologies. Using flexible definitions for personal information would promote data minimization by directing web operators to consider whether the collection and use of certain information is necessary and COPPA compliant.

---

game-industry-self-regulatory-program-approved-under/esrb_amended_application_for_modifications_to_coppa_program_requirements_3-13-18.pdf

[10] FTC, COPPA Safe Harbor Program, *Entertainment Software Rating Board (ESRB) Revised Safe Harbor / Kids Seal Program Guidelines* (June 23, 2013) (hereinafter *Previous Program Requirements*), *available at* https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701esrbcoppa.pdf

[11] EPIC, *Comments of EPIC to the FTC "COPPA Rule Review, 16 CFR Part 312, Project No. P104503"* (December 23, 2011), https://epic.org/privacy/kids/EPIC-COPPA-Rule-Comments-FINAL-12-23-11.pdf, at 7.

[12] *Id.* at 8.

[13] *Proposed Requirements* at Section I, page 1.

2. Further Recommendations

a. Remove Exemption for "Information Rendered Anonymous"

ESRB omits from the definition of PID "information that is rendered anonymous."[14] However, ESRB does not elaborate on adequate standards and techniques for de-identification. EPIC is concerned by this critical omission, as information that contains no direct personal identifiers can often be combined to identify a specific individual from basic parameters of activity times, location, and demographic segments such as date of birth, gender, and zip code.[15] There are practical limits in completely "anonymizing" information due to the granular nature and extent of online data collection and publicly available information.[16]

The FTC has concurred in 'FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising' that the risk of consumer data falling into the wrong hands and misused for re-identification is why commercial data collection requires risk assessments and additional precautions for obtaining consent.[17] The Amended COPPA Rule of 2013 reaffirms this by regulating the collection of non-personal, persistent identifiers such as IP addresses. Therefore, the Commission should reject this general exemption to the definition of PID, as the intent of the Amended COPPA Rule may be undercut by misguided industry interpretations of "anonymous information."

b. Include Personal Information and Data Collected Offline for Online Uses

ESRB's definition of PID only refers to information "collected online,"[18] and fails to address business practices that onboard offline data to an online environment, such as an operator acquiring children's personal information offline then uploading, storing, or disclosing to third parties on the web.[19] One example of this is use of RFID technology for identity documents that makes it possible to track and record the location of children.[20] It is important for COPPA to consider how new technologies are gathering data on children in public spaces with new communications technologies.

---

[14] *Proposed Requirements* at Section I, page 2.
[15] EPIC, *Comments of EPIC to the FTC "COPPA Rule Review, 16 CFR Part 312, Project No. P104503"* (December 23, 2011), https://epic.org/privacy/kids/EPIC-COPPA-Rule-Comments-FINAL-12-23-11.pdf, at 16-17.
[16] Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, STANFORD CENTER FOR INTERNET & SOC'Y (Oct. 11, 2011), http://cyberlaw.stanford.edu/node/6740.
[17] FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf
[18] *Proposed Requirements* at Section I, page 1.
[19] FTC, *Data brokers: a call for transparency and accountability* (May 2014), http://1.usa.gov/1kXR5g0, at 27-30.
[20] Wired, *School Drops RFID Tag Program (February16, 2005),* http://www.wired.com/techbiz/media/news/2005/02/66626.

II. Data Minimization

1. Modifications Improving Privacy Safeguards

ESRB's submission of the proposed modifications to the FTC stated, "In Section VII.A. of the Proposed Requirements, consistent with the best practice of data minimalization, we have added text to make clear participants should not collect personal information and data if it is not being utilized."[21]

> VII. DATA COLLECTION AND SECURITY
>
> A. Participant shall, upon ESRB's reasonable request, provide details regarding how PID is gathered from and/or tracked through Participant's Monitored Products, as well as disclosure regarding how such PID is utilized. *If PID is not being utilized, Participant should not collect it.*
>
> B. Participant shall establish, implement and maintain reasonable procedures to protect the confidentiality, security and integrity of PID within its control, whether collected from adults or Children, from unauthorized access, use, alteration, distribution, or disclosure. Participant shall utilize appropriate, commercially reasonable methods (e.g., encryption) to protect any sensitive PID it collects, such as social security numbers or transactional information, including but not limited to financial information.[22]

EPIC strongly supports the prohibition of data collection without a specified purpose, and the general principle of data minimization. Data minimization requirements are an effective way to increase data security and thus work in tandem with the confidentiality, security, and integrity requirements contained in § 312.8. One of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks occur is to reduce the amount of sensitive personal information contained in the database.

Data minimization is one of the core tenets of the Fair Information Practices ("FIPs")[23] that supply the basis for the Privacy Act of 1974. The Privacy Act directs agencies to maintain in their records only the minimum amount of information "relevant and necessary" to accomplish their purposes.[24] Similar data minimization approaches have appeared in other federal privacy statutes[25] and should inform the enforcement of the COPPA Rule. COPPA should establish a

---

[21] Entertainment Software Rating Board, *Application Filed Pursuant to Section 312.11 of the Children's Online Privacy Protection Rule, Requesting Approval of Modifications to the Entertainment Software Review Board Privacy Certified Kids Seal Requirements Under Section 312.11(e) of the Rule* (March 13, 2018) (Submitted to Donald Clark, Office of the Secretary, FTC) at 3.

[22] *Proposed Requirements* at Section VII (emphasis added).

[23] EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.

[24] 5 U.S.C. § 552a(e)(1) (2010).

[25] For example, the Video Privacy Protection Act requires businesses to "[d]estroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected . . . ."37

general understanding that the collection and use of information on young children should be treated with care and avoided if possible.

III. ESRB Modifications that the FTC Should Reject

1. Section I: Geographical Limitations in the Definition of Children

ESRB's submission of post-approval modifications to the FTC includes a description of how the proposed changes affect the program's existing requirements, as required by 16 C.F.R. § 312.11(c)(2) and (e). ESRB claims that the statement "does not include non-substantive changes, for example changes in terminology."[26] Using this disclaimer, ESRB did not address the substantive narrowing of the definition of "Child/Children" in its self-regulatory guidelines, even though the modification would impose significant geographical limitations on who can benefit from the privacy protections of the safe harbor program. The blackline draft[27] of ESRB's proposed modifications reveals that the definition of "Child/Children" in Section I only applies to residents of the United States, striking the provisions for residents in "Canada or anywhere else in the world, who are under thirteen (13) years of age" from the program.[28]

EPIC strongly urges the Commission to reject this change. Privacy safeguards of the COPPA Rule should apply to children whose personal information is collected by web operators without regard to residency or nationality requirements. To be entitled for a safe harbor treatment pursuant to § 312.11, the proposed guidelines must contain requirements that are substantially similar to COPPA. Limiting the material and territorial scope of the COPPA Rule is an express derogation of the basic framework for children's privacy provided by law, and must be prohibited.

It is timely for the Commission to address this now, as data privacy laws are gaining extraterritorial implementation through the General Data Protection Regulation ("GDPR")[29], which identifies children as "vulnerable individuals" deserving of "specific protection."[30] Article 6(1)(f) of the GDPR notes that the rights and freedoms of a data subject may "in particular" override the interests of the controller or third party where the relevant data subject is a child.

The GDPR applies to "natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."[31] It is well established in international privacy law that data processing activities related to web services merit wide territorial scope. It would be unacceptable for ESRB, a major industry group for self-regulation, to impose residency

---

[26] Entertainment Software Rating Board, *Application Filed Pursuant to Section 312.11 of the Children's Online Privacy Protection Rule, Requesting Approval of Modifications to the Entertainment Software Review Board Privacy Certified Kids Seal Requirements Under Section 312.11(e) of the Rule* (March 13, 2018) (Submitted to Donald Clark, Office of the Secretary, FTC) at 1.
[27] *Proposed Requirements*, Exhibit B, at Section I, page 1.
[28] *Previous Program Requirements*, at Section I, page 1.
[29] EPIC, *EU General Data Protection Regulation,* https://epic.org/international/gdpr/; Marc Rotenberg, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS, The General Data Protection Regulation at 692-93.
[30] EU General Data Protection Regulation, Recital 75, Articles 6(1)(f), 8, 12(1), 40(2)(g), 57(1)(b).
[31] EU General Data Protection Regulation, Recitals 2, 14.

qualifications for children to benefit from COPPA, when they are unable to understand the adverse implications to their privacy and safety and act accordingly.

2. Sections I – II.A: Termination of Privacy Risk Assessments and Initial Self-Assessment Questionnaires

ESRB submitted the following proposed modifications to the FTC to terminate its program requirements for Privacy Risk Assessments and Initial Self-Assessment Questionnaires (SAQs):

> In Section I of the Proposed Requirements, we have removed the definition of the term "Privacy Risk Assessment" because that term was not otherwise utilized in the Program Requirements.
>
> In Section II of the Proposed Requirements, for new participants in the Program, we have removed the requirement for an initial Self-Assessment Questionnaire ("SAQ") to be completed prior to or upon joining the Program. This requirement, which is currently found in Section II.A., is no longer necessary. Instead, especially in the early stages of membership, we have found that Program participants benefit from a more personal approach, usually involving at least one (but more likely several) telephone calls or video conferences to introduce them to the Program and to allow us to gather necessary information. However, we have reserved the right to require an SAQ at other times, if necessary.[32]

Section III.B (Notifying ESRB of Material Changes) has been revised:

> Where changes to Participant's Monitored Products, Privacy Statement or Online Information Practices have been implemented, Participant *may* be required to submit a Self-Assessment Questionnaire ("SAQ") or provide updated information in a form determined by ESRB. Participant *may* also be required to submit a SAQ if Participant has undergone a change in control, or if there has been an investigation of Participant's practices by a federal or state authority, agency or regulatory body or any unit of federal or state government.[33]

EPIC strongly urges the Commission to reject these changes. Privacy Risk Assessments and SAQs are effective *ex ante* safeguards to identify and eliminate risks in processing children's data. Setting clear rules for Privacy Risk Assessments and SAQs can encourage data

[32] Entertainment Software Rating Board, *Application Filed Pursuant to Section 312.11 of the Children's Online Privacy Protection Rule, Requesting Approval of Modifications to the Entertainment Software Review Board Privacy Certified Kids Seal Requirements Under Section 312.11(e) of the Rule* (March 13, 2018) (Submitted to Donald Clark, Office of the Secretary, FTC) at 2.

[33] *Proposed Requirements*, Section III.B; cf. *Previous Program Requirements*, Section I Definitions ("Privacy Risk Assessment") and Section IIA. Program Documents and Procedures, Initial SAQ/Certification Report (emphasis added).

minimization by requiring web operators to evaluate the necessity and proportionate extent of their online privacy practices.

Mandatory privacy assessments increase accountability for data collection by web operators.[34] The requirement imposes negligible costs for the operators yet greatly benefits children's privacy. Therefore, EPIC recommends that web services that collect children's information should be auditable through their privacy assessments on why and how they processed personal data, and the effect on users.

3. Section VII.E: Change of Taxonomy from "Must" to "Should"

ESRB wrote to the FTC, "In Section VII.E of the Proposed Requirements, we have changed "must" to "should" to clarify that this requirement is a recommended best practice, as opposed to an obligation under COPPA or the Amended COPPA Rule."[35] The modified section reads:

> If Participant's Monitored Products provide links to third-party web sites or apps, Participant *should* implement "exit messages" or "bumper pages" wherever users travel via such links to a third-party site or app to inform a user that: (i) he/she is leaving Participant's web site or app; and (ii) Participant's Terms of Use and Privacy Statement will no longer be applicable upon user's departure from Participant's website or app. Prior to implementation, Participant *should* submit the specific language it intends to utilize for this purpose to ESRB for approval.[36]

EPIC strongly urges the Commission to reject this change. It contravenes the requirements of COPPA and falls below the minimum criteria for approval of self-regulatory program guidelines pursuant to § 312.11. Notice and consent provisions of COPPA establish clear minimum requirements for safe harbor programs, which the ESRB diminishes in Section VII.E as "recommended best practices." Operators must establish equivalent or greater privacy safeguards to COPPA and cannot be certified to self-regulate unless these mandatory provisions are enforced.

> § 312.4 Notice:
>
> (a) *General principles of notice.* It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

---

[34] EPIC, *EPIC Comments on Data Protection Impact Assessments Guidance to UK Information Commissioner's Office*, https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf.
[35] Entertainment Software Rating Board, *Application Filed Pursuant To Section 312.11 of the Children's Online Privacy Protection Rule, Requesting Approval of Modifications to the Entertainment Software Review Board Privacy Certified Kids Seal Requirements Under Section 312.11(e) of the Rule* (March 13, 2018) (Submitted to Donald Clark, Office of the Secretary, FTC) at 3.
[36] *Proposed Requirements* at Section VII.E, at 10 (emphasis added).

(b) *Direct notice to the parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.[37]

§ 312.4 of the COPPA Rule requires the operator to provide notice and obtain verifiable parental consent prior to the disclosure of children's personal information to third parties. This denotes a mandatory obligation for operators to inform users when they are leaving the Participant's web site or app and become subject to persistent tracking or disclosures to third parties. The transfer of user data to application developers and now to websites is much harder for users to observe and control, and mandate notice requirements under COPPA that reflect these technological advances.

Further Recommendation:

- The definition of "disclosure" needs to be strengthened in order to address the opaque manner in which social networking sites like Facebook share information with third parties.

IV. Conclusion

The central purpose of the COPPA Rule is to establish privacy safeguards for the collection and use of personal information on children. Through critical amendments in 2013, COPPA has evolved to address changes in technology and business practices. These provisions must be competently carried forward in safe harbor programs, as the sensitive nature of children's data requires caution against self-regulation. Therefore, ESRB's Proposed Requirements which fall below the COPPA Rule must be rejected by the Commission to ensure that children's online privacy is adequately protected and prioritized.

Respectfully Submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Sunny Seon Kang*
Sunny Seon Kang
EPIC International Consumer Counsel

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law
and Policy Fellow

[37] COPPA Rule (2013), 16 C.F.R. § 312.4