epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, 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

on

Request for Comment Amending the Children's Online Privacy Protection Rule

89 Fed. Reg. 2,034

March 11, 2024

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Federal Trade Commission (FTC)'s Request for Comment on proposed modifications to the Children's Online Privacy Protection Rule (COPPA).[1] These modifications are a result of a years-long process to strengthen and modernize COPPA's protections for children online, a goal which EPIC enthusiastically supports.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC regularly advocates for privacy safeguards for children online and routinely files comments in

[1] Request for Comment Amending the Children's Online Privacy Protection Rule, 89 Fed. Reg. 2,034 (Jan. 11, 2024), https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule [hereinafter *RFC*].
[2] EPIC, *About Us* (2023), https://epic.org/about/.

response to proposed FTC rules and consent orders regarding business practices that violate privacy rights, including the privacy of children online.[3]

From a young age, children participate in a broad range of activities online. From web search and educational activities to gaming, messaging, and more, children can access and benefit from incredible amounts of information online. Unfortunately, existing protections for the privacy of children as they engage in the online world are deeply inadequate.[4] Apps and websites routinely share and sell children's personal information to data brokers, advertisers, and other entities. Such data collection is pervasive, fueling commercial surveillance and profiling that leads to myriad privacy harms.[5] In particular, these practices can deprive children of their autonomy and subject them to heightened physical safety and data security risks.[6] The use of personal data for targeted and behavioral advertising presents unique harms to children. "[C]hildren particularly vulnerable to commercial manipulation,"[7] as many children cannot

[3] *See*, *e.g.*, Comments of EPIC, NTIA Initiative to Protect Youth Mental Health, Safety & Privacy Online (Nov. 16, 2024), https://epic.org/documents/epic-comments-to-the-ntia-on-rfc-regarding-youth-mental-health-safety-privacy-online/; Comments of EPIC, CDD and Fairplay, Proposed VPC Method Submitted by Yoti, Inc. Under COPPA Rule (Aug. 21, 2023), https://epic.org/documents/epic-cdd-fairplay-comments-to-the-ftc-on-proposed-parental-consent-method-submitted-by-yoti-inc-under-coppa-rule/; Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 167-80 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillanceANPRM-comments-Nov2022.pdf; Comments of EPIC, FTC COPPA Rule Review (Dec. 11, 2019), https://epic.org/documents/coppa-rule-review/.
[4] *See* Comments of EPIC, FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 167-80 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillanceANPRM-comments-Nov2022.pdf [hereinafter *EPIC Commercial Surveillance Comments*].
[5] Girard Kelly et al., *Privacy Risks and Harms*, Common Sense Media 9 (2019), https://privacy.commonsense.org/content/resource/privacy-risks-harms-report/privacy-risks-harms-report.pdf.
[6] EPIC Commercial Surveillance Comments, *supra* note 4 at 169-71.
[7] Joseph Jerome & Ariel Fox Johnson, *AdTech and Kids: Behavioral Ads Need a Time-Out*, Common Sense Media 3 (2021) https://www.commonsensemedia.org/sites/default/files/uploads/pdfs/blog/adtech-and-kids-explainer.pdf.

identify ads or realize that the ads are personalized to them. Further, companies employ design choices to increase engagement by children, which enables more expansive data collection used to support targeted advertising.[8] Just last year, social media companies in the United States made over $11 billion in advertising revenue from children.[9] Through this rulemaking, the Commission is taking important steps to bring COPPA up to date with the current reality for kids online.

This comment will introduce several recommendations to improve the efficacy of the proposed modifications to the Rule. In Section I, we focus on the scope of covered entities and information, urging the Commission to include any category of sufficiently identifiable information that is linkable to a child in the Rule's "personal information" definition. Additionally, we recommend that any guidance the Commission provides for measuring the likely ages of users in a "mixed audience" call for privacy-protective methods that do not require additional data collection.

In Section II, we address the Commission's proposed changes to rein in behavioral advertising targeting children. In particular, the section will focus on how to reduce the flow of data from operators to external parties, which fuels behavioral advertising and causes other privacy and security harms. While the Commission has proposed positive changes to the Rule to address these issues—including an obligation to secure separate verifiable parental consent ("VPC") prior to sharing children's personal data with third parties—we provide specific

[8] *See* EPIC Commercial Surveillance Comments, *supra* note 4 at 171.
[9] Amanda Raffoul et. al, *Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model*, 18 PLoS ONE 12 (Dec. 27, 2023), https://doi.org/10.1371/journal.pone.0295337.

recommendations to make those proposed changes most effective in practice. These recommendations include: (1) removing "personaliz[ing] . . . content," "contextual advertising," from the internal operations exception, and (2) amending the definition of "third party" so that the term includes operators and other external parties that would encompass all ad tech tools.

Finally, in the third section we highlight the proposed Rule's enhanced data security and data retention sections. We recommend changes to strengthen the data security program and require a privacy program. We also urge the Commission to incorporate data minimization tenets, like purpose limitation, in both the data security and data retention sections of the proposed rule.

I. Expanding the Scope of Covered Entities and Information

Responsive to Questions 3, 5, 6, 7, 11

The Commission's proposed modifications to the definition of "personal information" and "mixed audience" are an important step for modernizing COPPA's scope.[10] Updating the personal information definition will improve the clarity and efficacy of the Rule. For example, enumerating "biometric identifiers" as a category of personal information reflects the vastly increased collection of biometric data from children online. The Commission is also right to revise the "online contact information" subset of personal information to specify that mobile telephone numbers are covered. Indeed, to maximize COPPA's privacy and security protections, the Commission should further augment the list of data types explicitly covered by the Rule to include government-issued identifiers, avatars generated from a child's image, and any other data type that is linkable to the identity of a child in the Commission's view.

[10] RFC, *supra* note 1 at 2702 (proposed modifications to §312.2).

The Commission should also ensure that whatever methods are authorized or recommended for operators to measure the composition of mixed audiences do not inadvertently inflict even greater privacy harms. The Commission should require that operators use privacy-protected age estimation methods to determine the likely ages of users, making clear that the "measurement" of children in a mixed audience is an estimation—not an age verification requirement that would require additional personal data collection and management.[11] Many operators already have detailed profiles or information about their users' age ranges, and children should not be required to disclose more information than necessary for an operator to evaluate a mixed audience.[12]

II. Curbing Behavioral Advertising and Limiting Data Flow to External Parties

The advertising technology industry has evolved beyond what the drafters of COPPA and the existing COPPA Rule could have foreseen. The status quo permits actors within the behavioral advertising ecosystem—operators, data brokers, advertising firms, and others—to evade COPPA or take advantage of loopholes in the Act, leaving children and their parents

[11] Scott Babwah Brennen & Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?*, Utah State University 3 (June 2023), https://www.thecgo.org/wp-content/uploads/2023/06/Age-Assurance_02.pdf ("[...] age estimation, refers to 'the process of assessment that an individual is likely to fall within a category of ages, over a certain age or under a certain age by reference to assurance components, inherent features, or behaviours related to that individual.'") (citing ISO Working Draft Age Assurance Systems Standard).

[12] *See* Erica Finkle et al., How Meta Uses AI to Better Understand People's Ages on Our Platforms, Meta (June 22, 2022) https://tech.facebook.com/artificial-intelligence/2022/06/adultclassifier/; Sarah Perez, TikTok CEO Says Company Scans Public Videos to Determine Users' Ages, TechCrunch (Mar. 23, 2023) https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/.

powerless against various privacy and data security harms.[13] The Commission has taken important steps in the proposed COPPA Rule to close those loopholes and to regulate data collection and use in line with COPPA's original intent and scope. This section will discuss the proposed changes to rein in behavioral advertising—and more generally, the disclosure of children's personal data to outside parties—and highlight the outstanding issues that the Commission must address for those proposed change to be fully effective.

a. Narrowing the Internal Operations Exception Loophole
Responsive to Questions 9 and 10

The Commission should revise the use and purpose limitations in the internal operations exception significantly to bar any secondary use of the information collected for the internal operations of a website. The definition for "support for the internal operations of the Web site or online service" in § 312.2 includes a list of activities for which data can be collected, retained and used without notice, disclosure, or VPC.[14] But two of these activities—personalizing content and serving contextual advertising—effectively make this exception into a loophole facilitating harmful data collection and use. Although Subsection (2) provides a use restriction against using information collected to "contact a specific individual,"[15] the restriction is far too narrow to be effective, as the information collected for personalizing content and contextual advertising can be used in other ways that are harmful to the privacy and wellbeing of children online.

[13] *See* Katie Joseff et al. *Behavioral Advertising Harms: Kids and Teens*, Common Sense Media 3 https://www.commonsensemedia.org/sites/default/files/featured-content/files/behavioral_-surveillance-advertising-brief.pdf (last visited Mar. 11, 2024).
[14] 16 C.F.R. §§ 312.2, §312.5(c)(7)-(8) (2013).
[15] 16 C.F.R. § 312.2.

Relatedly, the Commission should also excise persistent identifiers collected for the support for internal operations from the list of exceptions for data collection and use prior to parental consent in §312.5(c)(7). Currently, verifiable parental consent is not required prior to collecting or using persistent identifiers for the purpose of providing support for the internal operations of the website. In practice, this means that operators can sidestep VPC to collect and use persistent identifiers if their use supports one of the many categories in the internal operations exception. A persistent identifier is defined as one "that can be used to recognize a user over time and across different Web site or online services. Such persistent identifier includes, but it no limited to, a customer number held in a cookie, and Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[16] Persistent identifiers contain sensitive personal information that fuel the targeted advertising ecosystem through profiling and attribution.[17] If persistent identifiers are used in support of an internal operation, like contextual advertising or personalization, then the operator is not obligated to obtain prior parental consent under the current text of the Rule.[18] The commission should close this loophole and obligate operators to obtain VPC, and in doing so disclose information to parents, about their use of persistent identifiers for internal operations purposes.

Finally, the Commission should narrowly define contextual advertising to include only advertising that does not vary based on personal data collected from, or related to, the viewer or other children. Despite its plain meaning, the term "contextual advertising" is often used to describe advertising built on user-level data and inferences that closely resemble what we know

[16] *Id.*
[17] *See* Comments of Fairplay and CDD for extended discussion of the targeted advertising ecosystem.
[18] 16 C.F.R. § 312.5(c)(7).

as targeted advertising.[19] Without guardrails, contextual advertising can be susceptible to manipulation.

b. Limits on Sharing Personal Information with External Entities
Responsive to Q12

Although the proposed Rule significantly reinforces COPPA's limits on sharing children's personal information with third parties, the proposed definition of "third party" is too narrow and risks inadvertently undermining those same limits. We urge the Commission to address this shortcoming.

The Commission has introduced multiple important changes to the Rule addressing sharing data with external parties. First, where an operator shares personal information with third parties, it must disclose the identities of the third parties and the purposes for the disclosure.[20] This information must be included in both the direct notice to parents as well as notice posted on the website.[21] While notice to parents can help with the consent process, required disclosures on the website itself increase transparency into an operator's data management practices, including harmful data sharing practices. The second proposed requirement is that operators must obtain additional, *separate* VPC prior to disclosing a child's information to third parties.[22] This is an

[19] Katharina Kopp, *Is So-Called Contextual Advertising the cure to Surveillance-Based "Behavioral" Advertising?*, Tech Policy Press (Sept. 26, 2023), https://www.techpolicy.press/is-so-called-contextual-advertising-the-cure-to-surveillance-based-behavioral-advertising/; *see also* Girard Kelly, *Kids are Exposed to Targeted Advertising Across the Industry*, Common Sense Education (Mar. 21, 2022), https://www.commonsense.org/education/articles/kids-are-exposed-to-targeted-advertising-across-the-industry.
[20] RFC, *supra* note 1 at 2073 (proposed modification to §312.4(c)(1)(iv)).
[21] *Id*. (proposed modification to §312.4(c)(iv)).
[22] *Id*. at 2074 (proposed modification to §312.5(a)(2)).

important mechanism for increasing friction and slowing down the flow of children's data to external parties, including advertisers.

However, the Commission's effort to curb the free flow of personal data to external entities risks coming up short unless the Commission broadens the definition of "third party." For these additional requirements to be effective, they must apply to sharing of children's personal information with *all* external entities. To explain, there are three key terms at play here: operator, person, and third party. The statute defines "person" as "any individual, partnership, corporation, trust, estate, cooperative, association, or other entity."[23] Next, "operator" is defined as "a person who operates a website […] who collects or maintains personal information from or about the users or visitors of such website […]"[24] While these terms are appropriately broad, "third party" is narrowly defined (in relevant part) as a "person who is not: (1) an operator with respect to the collection or maintenance of personal information on the website or online service[…]"[25] While the natural sense of the term "third party" would seem to include any party external to the operator, the definition in the proposed Rule excludes any entity that qualifies as an operator. This would except at least some advertising technology tools and entities like cookies and software development kits (SDKs), which can qualify as operators to the extent that they collect and maintain information about child visitors of the website.[26] Similarly, comingling personal information in clean rooms with data collected by other advertisers or companies may

[23] 15 U.S.C. § 6501(11) (1996).
[24] 15 U.S.C. § 6501(2).
[25] 16 C.F.R. §312.2.
[26] *See* Comments of Fairplay and CDD for extended discussion of ad tech tools.

constitute operator-to-operator sharing.[27] This activity would necessarily fall outside of the third-party definition because a third party cannot be an operator.

The Commission should amend the "third party" definition to more tightly regulate the flow of children's data to parties external to the operator. For the proposed Rule to be most effective in mitigating privacy and data security harms to children, the term "third party" should be revised to encompass *any* external entity—including operators. Currently there is no mechanism to regulate sharing with an external entity that is not a third party (as that term is defined by the Rule). Closing this gap by amending the "third party" definition would be the easiest way to address the operator-to-operator sharing loophole. Alternatively, the Commission could add "or other persons" or "operators" to the term "third party" each time it appears, or it could introduce a new term like "third party operator" or "external operator" to the relevant disclosure requirements.

As it stands now, any external entity that could be considered an operator would not be a third party. The consequences for excluding operators and other external entities from the definition of third party are significant. For example, the proposed requirements to (1) disclose sharing activities with, and identities of, third parties and (2) obtain separate VPC prior to disclosing information with third parties may not apply to large swaths of the adtech ecosystem. It is critical that the Commission revise the proposed Rule to prevent this result.

[27] *See*, e.g., Joseph Duball, *Data Clean Rooms: An Adtech Privacy Solution?*, IAPP (Jan. 24, 2023) https://iapp.org/news/a/data-clean-rooms-an-adtech-privacy-solution/ (additional information about trending use of clean rooms).

c. Security Standards for Sharing Personal Information with External Entities

EPIC commends the Commission's proposed expansion of §312.8 requiring strong data management practices for operators independent of what is required for notice and VPC. Although parental consent is a central pillar of COPPA, the collection, use, and disclosure of personal data in today's online ecosystem far exceeds what a parent can understand and meaningfully consent to.[28] Currently an operator is responsible for maintaining and establishing "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[29] The Commission's proposed additions to this section illustrate what that responsibility should mean in practice. As it applies to sharing with external entities, section §312.8(c) smartly expands on what is already required in section §312.8: operators must determine whether the external entity can maintain the same confidentiality and security standards and "obtain written assurances that such entities will employ reasonable measures to maintain the confidentiality, security and integrity of the information."[30] Where the current Rule only requires an external entity to "provide assurances,"[31] the proposed Rule would require written assurances.

Relatedly, EPIC applauds that the required preauthorization applies to sharing with *any* external entity—not just third parties. The proposed Rule mandates due diligence "before allowing other operators, service providers, or third parties to collect or maintain personal

[28] *See* EPIC Commercial Surveillance Comments, *supra* note 4 at 153 ("We have moved beyond the notion that notice and consent alone can legitimize commercial surveillance practices when those practices are too complex and numerous for even the most sophisticated consumer to understand.").
[29] 16 C.F.R. §312.8.
[30] RFC, *supra* note 1 at 2705 (proposed modification to add §312.8(c)).
[31] 16 C.F.R. §312.8.

information from children on the operator's behalf, or before releasing children's personal information to such entities."[32] In doing so, this provision explicitly avoids the limiting third-party definition, ensuring equal application to sharing of personal data with any external entity.

III. Strengthening Data Security Programs, Privacy Programs, and Data Retention Policies

The proposed modifications to the Rule include strong data security and data management obligations for operators. Importantly, an operator is required to comply with these obligations independent of other notice or parental consent requirements. If an entity is an operator under the Rule, then their data security, privacy and data management policies must meet the proposed COPPA Rule's standards set forth in §312.8 and §312.10. Although operators are already obligated to "maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children,"[33] the Commission is right to provide more specificity as to what qualifies as "reasonable procedures."

EPIC supports this revision to the Rule and highlights three additional points. First, we recommend changes to strengthen the data security program, like identifying baseline data security measures and monitoring the efficacy of self-audits. Second, we strongly encourage the Commission to mandate that operators implement a privacy program in addition to a data security program. Finally, we offer several recommendations to more fully incorporate data minimization into the data security and data retention sections of the proposed Rule.

[32] RFC, *supra* note 1 at 2705 (proposed modification to add §312.8(c)).
[33] 15 U.S.C. § 6502 (b)(1)(D).

a. Bolstering Data Security and Privacy Programs

In the proposed Rule, the Commission takes significant steps to require that operators maintain data security procedures. It puts the existing obligation into practice, requiring a written personal information security program as well as a risk assessment program. This focus on data security, especially for sensitive data like children's personal information, builds on the Commission's long history of bringing enforcement actions against companies for insufficient or misleading data security practices.[34] In subsection §312.8(b), the proposed Rule outlines the requirements for a strong personal information security program. The iterative nature of the required steps, from identifying and mitigating risks to testing and monitoring the efficacy of those safeguards, is a significant improvement from the broader language that currently exists in the rule requiring just "reasonable procedures."

The Commission should consider strengthening or expanding a few key elements of the required security program. First, the Commission should make clear that it will take action if the operator's self-audits or pen-testing are inadequate. There is remarkable consistency among regulatory regimes as to what constitutes baseline cybersecurity guidelines and data security measures.[35] From data mapping to vulnerability management and threat detection, the Commission should consider identifying baseline categories of risk for operators to monitor as a part of the security program. Additionally, consistent with the statutory requirement for operators to protect the confidentiality, security, and integrity of children's personal information, the

[34] EPIC Commercial Surveillance Comments, *supra* note 4 at 181-82.
[35] Comments of EPIC, RFI to ONCD on Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations 22-30 (Oct. 31, 2023), https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/ (appendix).

Commission should require that operators orient their security program to mitigate harm to individuals, not to the business. In other words, the operator should center their efforts to mitigate any harm to children whose data has been accessed without authorization, not on mitigating harm to the operator.[36]

The Commission should also require operators to implement a full-scale privacy program consistent with those previously mandated under FTC consent decrees. The proposed Rule requirement for an "information security program" and annual risk assessment stems from the statutory obligation for operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[37] In the same way that the Commission proposes to require an information security program as a "reasonable procedure" to protect security of personal information, the Commission should require a full-fledged privacy program as a "reasonable procedure" to protect the "confidentiality" of children's personal information. The Commission regularly requires privacy programs as an element of consent orders, including order resulting from COPPA violations.[38] For example, the 2023 stipulated order resulting from Amazon's alleged COPPA violations

[36] *See* Draft Cybersecurity Audit Regulations for California Privacy Protection Agency (CPPA) Sept. 8, 2023 Board Meeting, at 10 Section 7123, available at https://cppa.ca.gov/meetings/materials/20230908item8.pdf (last visited Mar. 11, 2024) ("The cybersecurity audit shall assess and document any risks from cybersecurity threats, including as a result of any cybersecurity incidents, that have materially affected or are reasonably likely to materially affect consumers.").

[37] 15 U.S.C. § 6502(b)(1)(D).

[38] Stipulated Ord. for Permanent Injunction, Civ. Penalty Judgment, & Other Relief at 10–13, United Sates v. Amazon.com, No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1923128amazonalexaorderfiled.pdf; Stipulated Ord. for Permanent Injunction, Civ. Penalty Judgment, & Other Relief at 19–22, United Sates v. EPIC Games, No. 5:22-cv-00518-BO (E.D.N.C. Feb. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1923203epicgamesfedctorder.pdf.

included a robust "mandated privacy program."[39] The Commission should draw on this model to impose more detailed privacy program requirements on operators beyond the "confidentiality, security, and integrity" obligations already set forth in the proposed Rule.

b. Data Minimization as Data Security

The Commission should more explicitly incorporate data minimization principles into the proposed data security program and data retention requirements. Data minimization provides that data should only be collected, used, or disclosed to the extent reasonably necessary and proportionate to provide the service requested by the consumer.[40] Data security is intrinsically tied to data minimization: the higher volume of data that a company collects and retains, the higher data security risk.[41] In the COPPA context, operators pose a higher data security risk the more they collect, retain, and process children's personal information. The proposed risk assessment requirement instructs operators to identify and assess data security risks and sufficient safeguards "to control such risks."[42] The excessive data collection of personal data—here, the collection of a child's personal beyond what is necessary and proportionate to provide the service requested by the child or parent—is a well-established data security risk, and data minimization is an effective safeguard to mitigate or control that risk.[43]

[39] Stipulated Ord. for Permanent Injunction, Civ. Penalty Judgment, & Other Relief at 10–13, United Sates v. Amazon.com, No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1923128amazonalexaorderfiled.pdf.
[40] *See* EPIC Commercial Surveillance Comments, *supra* note 4 at 34.
[41] *See* John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too,* EPIC (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.
[42] RFC, *supra* note 1 at 2075 (proposed modification to add §312.8 (b)(2)).
[43] *See FTC,* FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket, FTC Technology Blog (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket.

Although the proposed Rule expands on data retention and deletion requirements, it should also incorporate stricter collection and purpose limitations. Specifically, the Commission should tether data collection and retention limits to the primary purpose for which the operator collected personal information—i.e., to provide the product or service requested by a child or parent. The current rule includes some data minimization language, instructing operators to only retain personal information "as long as reasonably necessary to fulfill the purpose for which the information was collected."[44] The proposed Rule adjusts that language slightly to include "purpose(s)."[45] But without limiting the permissible purpose or purposes for which a child's personal information may be collected in the first place, this seemingly minor adjustment could permit an operator to collect and retain vast amounts of children's personal data for an excessive length of time simply by burying a laundry list of collection purposes in a disclosure that few will read. If an operator does not actually "condition[] a child's participation"[46] on such broad-ranging data collection—for example, if an operator gives parents the nominal ability to opt out of non-essential collection purposes when it is first obtaining VPC—the operator may argue (contra the Commission's reading of the Rule)[47] that such collection is consistent with COPPA.

The Commission can and should forestall this argument by modifying the proposed Rule. First, the Commission should revise the proposed Rule to clarify that providing a service requested by a parent or child is the only permissible purpose for which a child's personal data may be collected or retained. Specifically, the Commission should amend §312.10 to read: "as

[44] 16 C.F.R. §312.10.
[45] RFC, *supra* note 1 at 2075 (proposed modification to §312.10).
[46] 16 C.F.R. §312.7.
[47] RFC, *supra* note 1 at 2062.

long as reasonably necessary to provide the service requested by a child or parent" instead of the current language ("to fulfill the purpose"). As a result, an operator would only be permitted to retain personal information for the primary purpose for which it was collected, which is to provide the requested product or service. Second, the Commission should add "proportionate" to make clear that the limiting phrase "as long as reasonably necessary and proportionate" imposes both a necessity and volume limitation.

Finally, EPIC commends other aspects of the expanded data retention section, including (1) the Rule's explicit prohibition on the indefinite retention of a child's personal information, and (2) the requirement for a written retention policy, posted on the operator's website, to effectuate the important data retention and deletion limits.[48]

IV. Conclusion

EPIC applauds the Commission's ongoing dedication to protecting the privacy and safety of children online. In its proposed changes to the COPPA Rule, the Commission takes critical steps to modernize COPPA's protections. Although we support this effort wholeheartedly, EPIC urges the Commission to (1) modify the definition of "personal information"; (2) amend the internal operations exception and the "third party" definition to bolster protections against behavioral advertising targeted at children, and (3) enhance the Rule's data security and privacy requirements to further mitigate the risks that unrestrained personal data collection and retention pose to children.

[48] *Id.*

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

Respectfully submitted,

/s/ John Davisson
John Davisson
EPIC Director of Litigation

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Law Fellow