FUTURE OF PRIVACY FORUM

1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

March 11, 2024

Ms. April Tabor
Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex E)
Washington, D.C. 20580

Re: COPPA Rule Review, Project No. P195404

The Future of Privacy Forum ("FPF") welcomes the opportunity to submit comments in response to the Notice of Proposed Rulemaking ("NPRM") on the Children's Online Privacy Protection Act Rule ("COPPA" or "Rule"). FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.[1]

Children today are increasingly reliant on online services to connect with peers, seek out entertainment, or engage in educational activities, and while there is a great benefit to this, there are also risks to privacy and personal data protection, and we applaud the Commission for its ongoing efforts to find a balance between these tradeoffs. Our comments and recommendations focused on areas where we believe there is further opportunity to strike that balance. FPF's comments are divided into two main sections: considerations applicable to all operators covered by the COPPA Rule and unique considerations for schools and education technology.

Considerations applicable to all operators:

I. Clarify what role text messages can play in the consent process.
II. Clarify the proposed requirement for separate verifiable parental consent for non-integral third-party information disclosures.
III. Provide more specificity on what types of processes encourage or prompt the use of a website are of greatest concern to the FTC.
IV. Align the proposed security program language with the stated goal of the NPRM.

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

Unique considerations for schools and education technology:

V. Work with the Department of Education to create and maintain joint guidance on how operators and schools should interpret their obligations in light of the interaction between COPPA and FERPA.

VI. Align the school-authorized education purpose exception to prior parental consent to the requirements of FERPA and address potential conflicts that could cause the school to violate FERPA.

CONSIDERATIONS APPLICABLE TO ALL OPERATORS

I. Clarify what role text messages can play in the consent process.

In the proposed rule, the FTC amends the definition of "online contact information" by adding "mobile telephone number" as a form of contact information. FPF supports adding "mobile telephone number" to the definition of "online contact information." This addition aligns with how technology has evolved since the last Rule update and how parents expect to interact with technology.

The FTC asks whether "allowing operators to contact parents through a text message to obtain verifiable parental consent present[s] security risks."[2] FPF suggests that the appropriate framing for this modification is whether contact via mobile telephone number presents a greater security risk than the existing methods. Any online contact information method will likely present at least a trivial security risk. The pertinent question is whether the potential security risk of collecting a mobile phone number would be heightened to outweigh the potential benefit.

With this framing in mind, FPF recognizes that the collection of mobile telephone numbers and contact via mobile phone comes with risks, such as the possibility of SMS phishing or "smishing" or the possibility of collecting additional inferences about an individual based on area code. However, taking mobile telephone in the context of the Rule, text messages with links may be sent in the context of a company seeking to facilitate verifiable parental consent at the initiation of either the parent themself or a child. While there is a potential risk of "smishing," a key risk mitigation factor is that a parent can personally verify with their child whether they initiated this process. The risk of contact through a mobile telephone number is no greater than that of existing contact methods, such as email.

While the proposed modification does not present a greater security risk, FPF recommends the FTC clarify either in the Rule or in guidance how text messages may be used to obtain consent,

[2] *See Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2041 (Jan. 11, 2024).

as described in the NPRM.[3] While the proposed modification merely expands the definition of "online contact information," the text of the NPRM suggests that text messaging could be a new form of verifiable parental consent ("VPC"). In further guidance, it would be helpful to clarify whether text messages may be used to *facilitate* parental consent or *obtain* parental consent. As FPF interprets this addition in the Rule, including a new form of online contact information does not necessarily equate to a new method of verifiable parental consent. For example, while an operator may use email for both purposes under the Rule by using "email plus,"[4] not all forms of contact information have an equivalent. Even though the 1999 NPRM referred to "instant messaging user identifiers,"[5] there is no "instant messenger plus" under the Rule.

If the FTC intends to create a new method of parental consent, consider how text messages could fit into the process. For example, a text messaging method akin to the familiar "email plus" approach could be adopted, given the reasons the FTC highlighted about why text messaging and over-the-top messaging platforms are more prevalent forms of communication. As for the email plus example, the Commission could simply add "or mobile telephone number" after each use of the word "email" in (b)(2)(viii) of the Rule. Additional engagement of industry stakeholders could yield other solutions similar to the one exemplified here.

II. Clarify the proposed requirement for separate verifiable parental consent for non-integral third party information disclosures.

FPF appreciates the efforts of the Commission to protect children's data online, which is further demonstrated by the actions observed in this proposed rule to provide additional safeguards over children's data related to disclosures to third parties. Today, many children's favorite playgrounds are found online, and the increased reliance on online services, products, and features to connect with peers, seek out entertainment, or engage in online educational activities has become more essential than ever before. While there is great benefit to a child's access to online spaces, there are also grave risks to privacy and personal data protection.

One key risk to childrens' privacy online identified by the Commission in the proposed rule is disclosures to third parties, which the Commission noted "are among the most sensitive and potentially risky uses of children's personal information."[6] Currently, third-party disclosure of a child's personal information is addressed in Section 312.5(a)(2), which requires operators of online services to give the parent an option to consent to the collection and use of a child's information, without consenting to the disclosure of that information to third parties. To address increasing

[3] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2051 (Jan. 11, 2024) (to be codified at 16 CFR 312).
[4] See I.4 of the FTC's COPPA FAQ, available at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent.
[5] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2051 (Jan. 11, 2024) (to be codified at 16 CFR 312).
[6] Prohibition against conditioning a child's participation on collection of personal information, 16 C.F.R. § 312.7 (2023).

concern about this risk, the Commission proposes amending Section 312.5(a)(2) to require operators to obtain separate verifiable parental consent before disclosing a child's personal information to a third party, "unless such disclosures are integral to the nature of the website or online service."[7] Due to challenges already faced by parents and industry stakeholders in carrying out current VPC requirements for an operator to collect, use or disclose a child's personal information, FPF recommends against imposing additional, separate VPC for third-party disclosure because this would fail to meaningfully promote transparency, parental oversight, and data minimization. However, if the Commission decides to move forward with this amended requirement under Section 312.5(a)(2), FPF recommends additional considerations be taken into account in the final rule.

A. FPF recommends against requiring a separate VPC for third-party disclosures.

FPF appreciates the attempts of the Commission to ensure that a child's participation in a site or service is not conditioned on disclosing more information than necessary to participate in the activity. Notably, in the current COPPA rule there is already a prohibition on conditioning a child's participation in an online activity on the unnecessary disclosure of personal information.[8] The language of this Section 312.7 already implies that an operator may not condition a child's participation in online activities on the disclosure of personal information, either to the operator or a third party, that is not integral to the nature of the online site or service. The proposed change to Section 312.5(a)(2) appears to further the policy goal of Section 312.7 to minimize the amount of personal data provided by children when engaging in an online activity by not only prohibiting conditioning a child's participation on the unnecessary disclosure of information to an operator, but also requiring a separate VPC for the information disclosure by a parent. Since the rule already incorporates a prohibition on the exact conduct that the separate VPC requirement in Section 312.5(a)(2) of the NPRM seeks to address, it seems that it would be a redundant requirement that does not clearly add benefit to parents and children. Therefore, FPF recommends against requiring a separate VPC for disclosure of children's data to third parties because stakeholders already face significant challenges under current VPC requirements for an operator's collection and use of child data, which a secondary VPC requirement would augment.

Almost every online site relies on third parties to function, provide necessary data, or add additional performance features, among other uses.[9] Even though virtually all websites use third parties, not all third party uses or disclosures are necessary for the service, product, or feature offered by the website. While FPF agrees that using a service should not be conditioned on excessively handing over data to third parties, a separate VPC requirement on operators subject to COPPA would exacerbate existing challenges to the implementation of approved VPC

[7] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2051 (Jan. 11, 2024) (to be codified at 16 CFR 312).

[8] Prohibition against conditioning a child's participation on collection of personal information, 16 C.F.R. § 312.7 (2023).

[9] Barry Pollard, *Third Parties*, Web Almanac https://almanac.httparchive.org/en/2021/third-parties#third-party (last updated Jun. 12, 2023) (finding that 94.1% of desktop sites and 94.4% of mobile sites use at least one third party resource).

methods, including challenges around accessibility, privacy and security, and convenience and cost. Where considerable challenges in implementing current VPC requirements already exist, FPF recommends against establishing a sweeping imperative on operators to implement a separate VPC process to disclose a child's data to third parties because this would amplify the issues already involved in currently approved VPC methods and further complicate a child's access to age appropriate online sites, services, and features.

There are considerable challenges in implementing the current VPC requirement. One challenge to the implementation of approved VPC is accessibility. Accessibility challenges arise where some parents do not have the necessary proofs of identification to complete currently approved methods for obtaining VPC. Currently, parents often have to provide either credit or debit card information or government identification information for the verification process.[10] As a 2021 Federal Deposit Insurance Corporation survey found, roughly 5.9 million households in the United States lack accounts in a bank or other financial institution, which undermines their ability to complete VPC steps requiring such information.[11] Additionally, equity issues exist where certain segments of the population, such as undocumented immigrants, lack access to government identification, causing access issues for parents to complete the process and children to gain access to the online site or service.[12] To require an additional step on top of the current VPC process could lead to unintended consequences and a magnification of the accessibility and equity issues already associated with VPC implementation, barring access to age-appropriate services for various segments of the population.

Another challenge to implementing currently approved VPC methods involves privacy and security concerns around providing sensitive personal information for VPC purposes. As aforementioned, current approved VPC mechanisms require a parent to provide either credit or debit card information, or information related to government identification. When FPF engaged parents for their thoughts on COPPA-enumerated VPC methods, parents broadly demonstrated "discomfort" with requests to share sensitive personal information, such as financial information or government identification, and "having that information linked to their children's online presence."[13]

Along with generating discomfort among parents, the practice of using VPC methods which require collection of sensitive personal data of parents runs counter to the data minimization goals of the underlying and proposed rule. As the Electronic Privacy Information Center noted, using VPC methods which require parents to provide sensitive personal information such as banking or financial information and government identification, "exposes…parents to the same

[10] FUTURE OF PRIVACY FORUM, *The State Of Play: Is Verifiable Parental Consent Fit For Purpose?* 1, 12 (Jun. 2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf [https://perma.cc/EC4C-D4JH].
[11] Fed. Deposit Ins. Corp. *FDIC National Survey of Unbanked and Underbanked Households*, 1, 13 (2021) https://www.fdic.gov/analysis/household-survey/2021report.pdf.
[12] FUTURE OF PRIVACY FORUM, *supra* note 7, at 12.
[13] *Id*.

privacy risks they are trying to protect their children from", generating hesitancy among parents about whether to use the online service at all.[14] One parent FPF engaged about VPC expressed that requests to provide sensitive information during the VPC process cause them to question the appropriateness of the site or service for their child, regardless of how well the operator actually protects user privacy.[15]

Given the concerns and privacy challenges raised by the current VPC standards, requiring the separate VPC process under this proposed rule would exacerbate the concerns and hesitations of parents and increase compliance costs necessary for operators to keep the collected information secure. Having a separate process that secondarily prompts a parent to provide sensitive personal information would likely lead to greater user drop off and distrust of these age-appropriate sites and services. Even worse, without adequate access to age appropriate sites and services, children may seek ways to circumvent VPC mechanisms or turn to online experiences on general audience-facing or age inappropriate sites and services.[16]

Finally, another challenge to implementing currently approved VPC mechanisms is the convenience and cost barriers for parents tasked with completing these VPC processes. In addition to the aforementioned hesitations around privacy when providing sensitive personal information for these processes, a time-consuming VPC process requiring a parent to participate in a video call or provide credit card information generates a friction for users and parents, which may dissuade parents and children from using age appropriate services requiring VPC.[17] As some stakeholders have previously observed, when extra steps are added to the process for a parent to permit their child to access a service, product, or feature, combined with the time to clarify confusion around why certain sensitive information is required for VPC, parents and children turn away from COPPA-compliant services and instead opt to use services with lower barriers to entry.[18] Where the proposed rule seeks to impose a separate VPC for third party disclosures, the convenience and cost barriers will understandably increase as parents will be required to go through a VPC process twice in many cases to give their child access to age appropriate content. Consequently, under this rule change more parents and children may turn to COPPA-noncompliant services to gain access to experiences and avoid the increased time and effort costs associated with requiring two VPC processes.

The considerable challenges concerning accessibility, privacy and security, and convenience costs would be exacerbated by requiring a separate VPC process for third party disclosures, likely leading to greater parental confusion, hesitation around providing sensitive information for

---

[14] EPIC, *EPIC, CDD, Fairplay Comments to the FTC on Proposed Parental Consent Method Submitted by Yoti Inc. under COPPA Rule*, 4 (2023), https://epic.org/documents/epic-cdd-fairplay-comments-to-the-ftc-on-proposed-parental-consent-method-submitted-by-yoti-inc-under-coppa-rule/.

[15] FUTURE OF PRIVACY FORUM, *supra* note 7, at 12.

[16] FUTURE OF PRIVACY FORUM, *supra* note 7, at 12-13.

[17] FUTURE OF PRIVACY FORUM, supra note 7, at 13.

[18] *Id*. at 13.

children's access to services, and ultimately lead to user drop off for COPPA-compliant services due to greater time and effort costs.

Additionally, it is important to note that the challenges described above concern currently approved VPC methods. A potential solution is that the FTC plays a more proactive role in identifying novel methods of VPC which seek to ease the issues observed in the implementation of current approved methods. The current process of applying and getting approval for new VPC proposals has only resulted in two new methods in the last eleven years.[19], and some stakeholders have noted it is arduous and time-consuming for industry actors to engage in the VPC submission process.[20] This is further evidenced by the fact that the most recent submission for "Privacy-Preserving Facial Age Estimation" has had two decision deadline extensions by the FTC.[21] To this end, it would be beneficial for the FTC to take a more proactive approach to identifying novel methods of VPC for industry use or further create incentives for industry to develop novel methods that balance compliance and regulatory objectives while also taking into account any barriers to a parent's time and capacity for participating in the approved process.

B. Clarify the proposed change to Section 312.5(a)(2) incorporating the following considerations.

While FPF identifies that there are significant challenges with the implementation of VPC, FPF also understands that there is a heightened privacy risk with disclosing a child's information to third parties. As a result, FPF also recommends three considerations the Commission should consider when finalizing Section 312.5(a)(2) of the Rule, should the Commission decide to move forward with the separate VPC requirement.

First, further guidance or clarity on what disclosures are 'integral to the nature of the website or online service' will be critical for compliance with this provision. Without more guidance on what the agency considers integral, this provision lacks the clarity required for compliance. Alternatively, the Commission could provide operators the opportunity to define which disclosures are integral to their service, and the Commission could supplementarily provide guidance on what could be claimed as an integral third-party use and disclosure. As part of this alternative approach, operators could be required to state which disclosures are integral in their direct notice to parents.

Second, in evaluating this proposed language for the final Rule, FPF recommends the FTC consider what will meaningfully improve transparency and choice for parents about why the disclosure is happening and how it will be used in relation to the service. While FPF has outlined above the challenges and friction points with VPC, FPF also recognizes the policy goal currently

[19] *Id*. at 16.
[20] *Id*. at 24.
[21] *See* Press Release, FTC, *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.

articulated in the rule of not conditioning a child's participation in an activity on unnecessary data disclosures. In order to meet this goal and provide parents with a more meaningful level of transparency and choice, FPF recommends considering whether the separate consent must be *verifiable* parental consent. As written, the proposed language calls for separate verifiable parental consent, which is a term of art within the Rule, suggesting that a parent would be required to go through the VPC process twice. This would further exacerbate the challenges outlined above without meaningful improvements for parents and children. To meet the intentions of bolstering this section, it may be more appropriate to obtain the consent of a previously verified parent or further clarify that a parent would not have to go through a process such as providing a credit card, calling a toll-free number, or providing government-issued ID multiple times. This would still allow parents to have a choice over the data disclosure without heightening VPC challenges.

Finally, the Commission should avoid prescribing specific processes and flows for when and how the VPC for disclosure should occur. Operators' services, products, and features vary widely and thereby require different data processes and data flows which would necessitate the use of varying third parties at different times. As a result, prescribing particular processes and flows for the data in this rule should be avoided to prevent problematizing rule compliance across different industry actors. To promote a positive user experience, alleviate user drop-off, and promote data minimization principles, some operators choose not to deploy VPC until a child reaches a part of the experience where collection and use of the child's personal information is necessary, rather than at the outset of the experience. A prescriptive approach to when VPC for collection, use, and disclosure is required may lead to less creativity in how products are designed as well as less thoughtfulness about what personal information, if at all, is actually required for an experience.

III. Provide more specificity of what types of processes that encourage or prompt the use of a website are of greatest concern to the FTC.

FPF recommends striking the proposed modification to the internal operations exception to exclude "in connection with processes that encourage or prompt use of a website or online service." In its current form, the "support for internal operations" exception is a narrow exception with seven specifically permitted activities.[22] Section (2) of this exception makes certain activities that cannot be considered internal operations, including behavioral advertising or amassing a profile on a specific individual. However, this provision of the rule also contains the language "or for any other purpose." Continuing to add specific activities to this provision of the rule may be unnecessary and redundant. Instead, further FTC guidance on the seven enumerated activities of the internal operations exception may be a more appropriate avenue for providing this clarity.

[22] See Children's Online Privacy Protection Rule, 78 Fed. Reg. 3,972 (Jan. 17, 2013) (codified at 16 C.F.R. pt. 312),
https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule.

However, if the proposed language remains in the final rule, FPF recommends that the FTC consider potentially beneficial processes that encourage or prompt the use of a website or online service. As explained in the NPRM, the FTC seeks to "prohibit operators from using or disclosing persistent identifiers to optimize user attention or maximize user engagement" with a service. In contrast, the language used in the proposed rule is "encourage or prompt use." "Prompt" is potentially broader than the concerns of maximizing user engagement and could include something as infrequently as one notification per day. In crafting this restriction, the FTC should consider positive use cases of prompts. Examples can include reminders about meditation apps, homework assignment reminders, and notifications about language lessons.[23] The current proposed rule could restrict these types of prompts, which may not be the types of nudges the FTC is concerned about with this proposed change. Further specificity on the types of activities that cannot be considered support for internal operations would be useful.

IV. Align the proposed security program language with the stated goal of the NPRM.

FPF supports the FTC's proposed additions to Section 312.8 of the Rule. However, FPF recommends the deletion of the words "children's personal information" to instead read "written security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children." As currently drafted, it is unclear whether the FTC is calling for a child-specific security program, rather than a security program that appropriately safeguards children's data. Having a comprehensive written security program aligns with current industry best practices - having a written security program specific to one type of personal information does not. This proposed deletion would be in line with the explanation provided in the NPRM, which states that operators need "*a* written comprehensive security program" (emphasis added).[24] A child-specific plan would burden companies with no additional security benefit to parents and children. Ultimately, FPF supports what the Commission proposes within the written security program and a company with an existing written security program that meets these requirements should be considered to be in compliance with these proposed additions.

---

[23] Cassie Freeman Et al., *The Duolingo Method for App-based Teaching and Learning*, Duolingo (Jan. 11, 2023), https://duolingo-papers.s3.amazonaws.com/reports/Duolingo_whitepaper_duolingo_method_2023.pdf; PowerSchool, Respecting Your Student's Data Privacy is Critical to PowerSchool, https://www.powerschool.com/privacy/ (last visited Mar. 3, 2024); SCHOOLOGY, Parent Email Digest and Overdue Submissions Notification, 1-3 (2013), https://resources.finalsite.net/images/v1616014583/calvertnetk12mdus/zlvsawli1rddkvet3emz/Schoology_Parent_Email_Notifications.pdf; HEADSPACE, Meditation for kids, https://www.headspace.com/meditation/kids (last visited Mar. 3, 2024); Scratchjr, Coding for young children, https://www.scratchjr.org/ (last visited Mar. 3, 2024).

[24] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2065 (Jan. 11, 2024) (to be codified at 16 CFR 312), available at https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule.

UNIQUE CONSIDERATIONS FOR SCHOOLS AND EDUCATION TECHNOLOGY

COPPA has been an influential law in the fight to keep children and their personal information safe on the internet. However, where COPPA intersects with the privacy requirements of the Family Educational Rights and Privacy Act ("FERPA"), there has been widely acknowledged confusion.[25] In formalizing existing guidance, the proposed rule strengthens the protections for younger students when schools use education technology. However, there is also a risk of codifying long-standing confusion and misalignment between the two regulations.

The potential impact of confusion and misalignment is significant. There are more than 98,000 U.S. schools[26] and more than 9,000 education technology ("edtech") companies.[27] School districts accessed an average of 2,591 distinct edtech tools annually,[28] and the International Trade Administration estimates the size of the U.S. edtech market at more than $89.49 billion (USD)/year,[29] in which the under 13 population is a significant component.

Given the significant impact of the proposed school authorized education purpose exception to prior parental consent, FPF's comments address the need for joint guidance, clarity and definition, and understanding of the conflicts between COPPA and FERPA.

V. Work with the Department of Education to create and maintain joint guidance on how operators and schools should interpret their obligations in light of the interaction between COPPA and FERPA.

As part of the request for public comments for the 2017 Joint FTC and Department of Education workshop, the Agencies asked, "What practical challenges do stakeholders face in simultaneously complying with both COPPA and FERPA?"[30] During that workshop, a representative from the Department of Education's Office of Educational Technology noted that "[w]ith the continued proliferation of new ed tech products, new uses, and new questions about the intersection of COPPA and FERPA, both the FTC and the Department of Education believe further discussion and perhaps additional guidance is warranted."[31]

---

[25] *FTC and the Department of Education to Host Workshop on Student Privacy and Ed Tech Seeking Public Comments,* Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FTC%20ED%20workshop%20announcement_final.pdf.

[26] *Fast Facts*, National Center for Education Statistics, https://nces.ed.gov/fastfacts/display.asp?id=84.

[27] *EdTech Top 40,* LearnPlatform, https://www.instructure.com/edtech-top40.

[28] *2022 Edtech App Report,* Lightspeed Systems, pwp.lightspeedsystems.com/2022-edtech-app-report.

[29] *Education Technology*, International Trade Administration, https://www.trade.gov/education-technology.

[30] *FTC and the Department of Education to Host Workshop on Student Privacy and Ed Tech; Seeking Public Comments,* Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FTC%20ED%20workshop%20announcement_final.pdf.

[31] *FTC Workshop: Student Privacy and Ed Tech,* Federal Trade Commission, (December 1, 2017)

However, individual agency guidance is insufficient to address the interaction of these two complex regulations. Two years later, at a workshop on the future of the COPPA rule, Steve Smith, Chief Information Officer of Cambridge Public Schools, commented, "The number one question or kind of muddy issue is the overlap of COPPA and FERPA. That always comes up every time."[32] The increased adoption of education technology during the COVID-19 pandemic has only increased the demand for guidance.

While formalizing the previous convention of school as a limited "parent agent" will add much clarity, it also highlights potential areas where the abilities of an operator under COPPA and the schools' obligations under FERPA may conflict. To address this complexity, FPF recommends that the Commission work with the Department of Education to create and maintain joint guidance on how operators and schools should interpret their obligations in light of the interaction between COPPA and FERPA. This guidance should consider the perspective and expertise of operators and school stakeholders. A coordinated approach to guidance is essential, as the Department of Education announced plans to amend FERPA regulations in Spring 2023.[33]

VI. Align the school-authorized education purpose exception to prior parental consent to the requirements of FERPA and address potential conflicts that could cause the school to violate FERPA.

The proposed rule's school-authorized education purpose exception to prior parental consent builds on prior FTC guidance on schools' role in using online education technology and the COPPA rule. The preamble to the proposed rule describes the intention of the proposed school authorization exception as incorporating "the privacy protections contained in the FERPA school official exception."[34] FPF has identified several areas where actions permitted by the operator under the proposed school exception to prior parental consent could potentially cause the school to violate FERPA.

These differences are likely to create confusion for schools and operators and, if unresolved, could create the potential for an operator to cause a school to violate FERPA. The following section reviews areas of the proposed rule that may require special attention or clarification to address the impact on a school's FERPA compliance under the proposed school-authorized education purpose exception to prior parental consent.

A. Align the Definition of school-authorized education purpose with FERPA.

1https://www.ftc.gov/system/files/documents/videos/student-privacy-ed-tech-intro-opening-remarks-panel-1/ftc_student_privacy_and_ed_tech_transcript_segment_1.pdf.

[32] *Transcript The Future of the COPPA Rule: An FTC Workshop Part 2*, Federal Trade Commission, (October 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_2_1.pdf.

[33] Family Educational Rights and Privacy Act, Department of Education, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1875-AA15.

[34] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2055 (Jan. 11, 2024) (to be codified at 16 CFR 312).

The proposed rule's definition of school-authorized education purpose[35] is similar but not completely aligned with FERPA's school official exception.[36] FERPA permits schools to outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, volunteers, or other third parties provided that the outside party:

> (1) Performs an institutional service or function for which the agency or institution would otherwise use employees;
>
> (2) Is under the direct control of the agency or institution concerning the use and maintenance of education records; and
>
> (3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

In the preamble to the proposed rule, the Commission requested input on what types of services should be covered under a ''school-authorized education purpose'' which are "related to a child's education" and asked if this should "include services used to conduct activities not directly related to teaching, such as services used to ensure the safety of students or schools."[37]

While the rule's preamble refers to FERPA's school official exception, the proposed rule's language could be interpreted to be a more narrow, "teaching" interpretation of "related to a child's education" than in FERPA. FERPA's school official exception is clear that the scope of the exception applies to the use of third parties that perform "an institutional service or function for which the agency or institution would otherwise use employees" and concerning the "purposes for which the disclosure was made" specifically uses the example "to promote school safety and the physical security of students."

Since 2014, 41 states and the District of Columbia have passed student privacy legislation.[38] Many of these laws include versions of K-12 school purposes as "purposes that are directed by, or that customarily take place at the direction of a school, teacher, or school district; aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of the school."[39]

FPF recommends that the proposed exception mirror the intent, if not the exact language of FERPA's school official exception, to include services used to conduct activities not directly related to teaching. Any variation or lack of clarity in the alignment between the scope of FERPA and COPPA's exceptions in this regard will create considerable confusion and disruption for the more than 13,000 school districts and the edtech vendor community.

---

[35] *Id.*
[36] 34 C.F.R. §99.31(a)(1)(i)(B)).
[37] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2071 (Jan. 11, 2024) (to be codified at 16 CFR 312).
[38] *State Student Privacy Laws*, Future of Privacy Forum, https://studentprivacycompass.org/state-laws/.
[39] Illinois Statutes Chapter 105. Schools § 85/5. Definitions, https://codes.findlaw.com/il/chapter-105-schools/il-st-sect-105-85-5/.

B. Define the term written agreement.

FPF recommends defining the term written agreement. The rule's exception to prior parental consent, which requires a written agreement that provides that the operator is "under the school's direct control"[40], aligns with FERPA's school official exception that the contractor "[i]s under the direct control of the agency or institution concerning the use and maintenance of education records."[41] However, "written agreement" is not defined in the proposed rule, and this creates the potential for confusion for two reasons. First, the proposed COPPA Rule uses the term written agreement in the context of data sharing that is analogous to FERPA's school official exception. However, "written agreement" is a term defined in FERPA,[42] and it applies to two other FERPA exceptions: Studies, and Audit and Evaluation. Second, the proposed COPPA Rule does not make it clear if the term "written agreement" applies only to signed contracts or if it also applies to so-called "Click-Wrap" agreements that meet the requirements of the proposed rule's written agreements.

Defining written agreement will avoid unnecessary confusion for operators and schools. While FPF agrees with the long-standing guidance from the Commission and the U.S. Department of Education that "[a]s a best practice, FPF recommends that schools or school districts decide whether a particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher."[43] FPF recognizes the balance the Commission is attempting to strike for flexibility.

However, FPF recommends that the Commission consider additional guidance that takes into account the current state of school technology approval processes. The 2023 Project Unicorn's State of the Sector Report, which surveyed more than 208 school districts, reported that only 38 percent had a formal process for vetting edtech tools and less than 27 percent consulted third-party guidance when developing a privacy process for vetting applications. Several states have been successful in adopting written agreements in the form of the National Data Protection

---

[40] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2075 (Jan. 11, 2024) (to be codified at 16 CFR 312).

[41] *Who is a ''School Official'' Under FERPA?*, Department of Education, available at https://studentprivacy.ed.gov/faq/who-school-official-under-ferpa#:~:text=A%20%E2%80%9Cschool%20official%E2%80%9D%20includes%20a,and%20support%20or%20clerical%20personnel.

[42] 34 CFR §99.31(a)(3); *see also* 34 CFR §99.31(a)(6)(iii)(C).

[43] COPPA FAQ N.3 Who should provide consent – an individual teacher, the school administration, or the school district?, (Federal Trade Commission), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS.; *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, U.S. Department of Education, (February 2014), https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best, The best practice guidance notes that "It is particularly important that teachers and staff not bypass internal controls in the acquisition process when deciding to use free online educational services. To ensure that privacy and security concerns relating to these free services are adequately considered, the Department recommends that free online educational services go through the same (or a similar) approval process as paid educational services to ensure that they do not present a risk to the privacy or security of students' data or to the schools and district's IT systems."

Agreement from the Student Data Privacy Consortium, a collaborative of more than 123 edtech providers and 12,206 school districts and regional and state agencies in 31 states.[44]

FPF recommends that the Commission consider aligning with the Department of Education's recommendations in their 2014 guidance document Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices[45] that "with Click-Wrap agreements, the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to signing a contract."[46]

FPF recommends that Click-Wrap agreements be included in the definition of written agreement but encourages that further guidance be provided that the terms of the agreement meet or exceed the best practice guidance provided in the 2016 Protecting Student Privacy While Using Online Educational Services: Model Terms of Service[47] guidance document.

FPF expresses concern that the written agreement requirement to provide a title and a statement that the individual "has authority" does not meet the rigor of approved methods of VPC, given the broad use and collection envisioned under this proposed exception to VPC. This approach appears to be a less stringent requirement than the current COPPA guidance that "[w]here an operator gets consent from the school rather than the parent, the operator's method must be reasonably calculated, in light of available technology, to ensure that a school is actually providing consent, and not a child pretending to be a teacher, for example." Additionally, FERPA regulations require educational agencies and institutions to use reasonable methods to identify and authenticate the identity of parents, students, school officials, and other parties before disclosing or permitting access to personally identifiable information ("PII").[48] FPF recommends that the rule require that the school's acknowledgment of the written agreement be clear and conspicuous.

The proposed COPPA rule amends the notice provision to include the school in the direct notice requirement.[49] This creates a status where for the purposes of notice, the school is treated similarly to a parent, but for the purposes of consent (in the written agreement), the school is treated as an exception to prior parental consent. FPF encourages the Commission to consider if the limited role of the school would be better suited to a subset of parental consent for both notice and choice rather than as an exception to parental consent.

---

[44] Student Data Privacy Consortium, https://sdpc.a4l.org/.
[45] Ibid.
[46] Ibid.
[47] *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service,* U.s. department of Education (March 2016), https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service.
[48] 34 CFR §99.31[c].
[49] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2073 (Jan. 11, 2024) (to be codified at 16 CFR 312).

C. Require an updated school authorization upon a material change in the collection, use, or disclosure practices.

The proposed rule language regarding a school's authorization and written agreements should be revised to clarify that in addition to providing new notice when there is a "material change,"[50] the operator must obtain a new written agreement from the school. COPPA requires an operator to obtain new VPC to any material change in the collection, use, or disclosure practices to which the parent has previously consented. The Commission should address this in § 312.5(c)(10) exceptions to prior parental consent regarding schools.

D. Consider if special treatment or guidance is appropriate for free services marketed directly to teachers.

FPF also recommends that the Commission and the Department of Education consider what guidance is appropriate where operators market free services directly to teachers with services designed for a single teacher or class rather than a school or district. While this approach provides a method for "grassroots" adoption of new edtech products, particularly from small and new edtech companies, even in the limited circumstances where teachers have the authority to accept agreements, the nature of a classroom teacher's role is that any "legitimate educational interest" they have over a given student's educational records is typically confined to the current school year. FPF recommends that the Commission, in consultation with the Department of Education, consider additional guidance, such as limiting data retention to the current school year.

E. Address potential FERPA issues related to use and disclosure.

FERPA requires that a third party receiving educational records under the school official exception "will not disclose the information to any other party without the prior consent of the parent or eligible student." The school official exception's requirement for direct control by the school also means that a third party may redisclose student PII at the direction of the school, where permitted under FERPA.

The proposed COPPA rule contains two exceptions to prior parental consent that allow the operator to collect, use, or disclose personal information from a child, § 312.5(c)(5) and § 312.5(c)(6), that may conflict with a school's FERPA obligations.

§ 312.5(c)(5) of the proposed rule allows the operator to collect, use, or disclose personal information from a child where the purpose of collecting a child's and a parent's name and online contact information is to protect a child's safety. When applied to the school-authorized education purpose this disclosure as an exception to prior parental consent is very broad and appears to exceed the more narrow limitations of FERPA, wherein a school must (i) determine whether there is an articulable and significant threat to the health or safety of a student or other individuals and

[50] As discussed in Part IV.B.3.a under § 312.4 of the proposed rule; *see* https://www.federalregister.gov/d/2023-28569/p-416.

(ii) document the parties to whom the agency or institution disclosed the information.[51] It is unclear under FERPA whether third parties, such as COPPA-covered operators, could meet these requirements on the school's behalf.

FPF recommends that the Commission amend this exception to add the qualifier used in § 312.5(c)(6)(iv) to read "To the extent permitted under other provisions of law, where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child."

Section 312.5(c)(6) of the proposed rule allows the operator to collect, use, or disclosure personal information from a child where the purpose of collecting a child's name and online contact information is to:

> (i) Protect the security or integrity of its website or online service;
>
> (ii) Take precautions against liability;
>
> (iii) Respond to judicial process; or
>
> (iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not be used for any other purpose.[52]

FERPA allows the school to disclose information in response to judicial order or lawfully issued subpoena "only if the agency or institution makes a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, so that the parent or eligible student may seek protective action."[53] FERPA also permits the Secretary of Education to prohibit "access to personally identifiable information from education records for at least five years" on a third party that "fails to provide the notification required."[54]

FPF recommends that the Commission amend this exception to move the qualifier used in § 312.5(c)(6)(iv) to § 312.5(c)(6) to apply to the entire clause to read "To the extent permitted under other provisions of law, where the purpose of collecting a child's name and online contact information is to[…]" and remove the clause from §312.5(c)(6)(iv) and provide additional clarifying language and clear guidance on this in an updated COPPA FAQ.

FPF further recommends addressing similar disclosure-related issues in the proposed rule's treatment of support for internal operations.

---

[51] *Id*. at § 99.32(5).
[52] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2073 (Jan. 11, 2024) (to be codified at 16 CFR 312).
[53] FERPA (§ 99.31(a)(9)).
[54] *Id*. at § 99.67(e).

The proposed COPPA rule amends the requirements for the content of the direct notice to include "where the operator discloses personal information to one or more third parties (including making it publicly available)."[55] With the narrow exception of allowing parents to opt-out of the disclosure to third parties, including the public of Directory Information,[56] FERPA does not provide an exception for disclosing information from a student's education records to the public.

However, the COPPA rule's definition of disclose also includes activities such as "an electronic mail service; a message board; or a chat room" that, when done under a school-authorized education purpose include essential functions such as school-provided email and discussion board that are part of a learning management system, and chat features built into the tools that enabled online learning during the pandemic.

FPF recommends that the Commission, in coordination with the U. S. Department of Education, further clarify and address the nature of disclosure and the distinction between making information public and disclosing within a school-authorized education service or website.

F. Address potential FERPA issues related to COPPA's definition of personal information.

Under COPPA, personal information means "individually identifiable information about an individual collected online, including information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition." While it does not specifically state that it is limited to information collected from the child, this interpretation as "personal information collected online from children" is present throughout the COPPA FAQ.[57]

Where the operator relies on the school-authorized education purpose exception to prior parental consent, the scope of PII under FERPA must be considered. FERPA's education record includes all data directly and indirectly related to the student[58] and "records maintained by a third party acting on behalf of a school or district are also considered education records."[59] While COPPA applies to information collected from a child, a student's education record is all directly related information about a student,[60] and may be collected from other sources such as a teacher or counselor. It is unclear if, in the school-authorization context, the proposed rule only covers PI collected directly from the child and information combined with an identifier listed in the COPPA Rule's definition of PI.

---

[55] § 312.4(c)(1)(iv).
[56] FERPA 34 CFR § 99.3 and 34 CFR § 99.37.
[57] *Complying with COPPA: Frequently Asked Questions,* Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.
[58] Personally Identifiable Information (PII), https://studentprivacy.ed.gov/content/personally-identifiable-information-pii.
[59] *Responsibilities of Third-Party Service Providers under FERPA*, U.S. Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf.
[60] FERPA 34 CFR § 99.2.

FPF recommends that the Commission align the proposed rule's definition of personal information with FERPA, where information is collected for the school-authorized education purpose.

G. Address potential FERPA issues related to COPPA's data retention and deletion requirements.

FPF recommends additional clarification and guidance concerning retention where data is collected for a school-authorized education purpose. Previous FTC COPPA guidance has indicated that retention cannot be "indefinite".[61] Careful consideration is necessary for aligning this requirement with state-specific records retention requirements that many schools must adhere to. Notably, these retention requirements sometimes differ depending on the nature of the data collection. For example, academic progress records[62] including essays and projects, might require deletion at the end of the academic year, whereas records with historical value, like transcripts, typically need to be retained for several decades. Some records, such as english as a second language records, will fall in between, and the school will likely direct an operator to retain while the student is enrolled at the school, or a given number of years after the student graduates, transfers or withdraws.[63] FERPA prohibits schools from destroying data if there is a pending request from a parent or eligible student to access those data.[64] Part B of the Individuals with Disabilities Education Act requires public agencies to inform a student's parents when any PII collected, maintained, or used thereunder is no longer needed to provide educational services to the child.[65]

There is also a need for guidance or clarification on how the rule's retention requirement interacts with de-identification. This guidance should align with the current de-identification guidance from the Department of Education.[66]

H. Address potential FERPA issues related to the right to review and private schools.

The proposed COPPA rule adds that "[w]here personal information is collected from the child pursuant to [a school authorization purpose], the operator of the website or online service is required to provide the rights under paragraph (a) [to review] to the school and is not required to

---

[61] Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act, FTC, https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf.
[62] *Records Retention and Disposition Schedule GS-21*, Library of Virginia, https://www.lva.virginia.gov/agencies/records/sched_local/GS-21.pdf.
[63] *Ibid.*
[64] FERPA 34 CFR §99.10.
[65] Best Practices for Data Destruction, Department of Education, https://studentprivacy.ed.gov/resources/best-practices-data-destruction.
[66] *Data De-identification: An Overview of Basic Terms*, U.S. Department of Education (October 2012) https://studentprivacy.ed.gov/resources/data-de-identification-overview-basic-terms.

provide such rights to a parent whose child has provided personal information to the website or online service."[67]

This addition allows the school to facilitate the parent's right to review while maintaining the required FERPA direct control. This addition avoids a scenario where a parent could request deletion or prevent further collection of a school-authorized service.

However, the FTC should consider the school's "reasonable time period" requirement under FERPA. FERPA requires that educational agencies and institutions comply with a request by a parent or eligible student for access to education records within a reasonable time period, but not more than 45 days after receipt of a request.[68] Some States have laws that may require that parents and eligible students be granted access in a shorter time period.[69]

Another consideration for this proposed addition is how edtech products used by schools not subject to FERPA will be impacted. The proposed rule includes private schools in the definition of school. Including private schools under the operator's COPPA obligations is a meaningful enhancement as FERPA and many state student privacy laws do not cover private schools. However, in § 312.6(b), the proposed rule states that "where personal information is collected from the child pursuant to § 312.5(c)(10), the operator of the website or online service is required to provide the rights under paragraph (a) of this section to the school and is not required to provide such rights to a parent whose child has provided personal information to the website or online service."[70]

The Commission should acknowledge that private and parochial schools generally do not receive federal funding and are, therefore, not subject to FERPA, and additional measures may be needed to provide the parent with their COPPA rights.[71]

I. Address potential FERPA issues related to security and data breaches.

FPF commends the Commission on the proposed rule's significant additional requirements for security. The proposed rule does not address any requirements for data breach notification. It is unclear if the language in the proposed rule is sufficient to allow schools to fulfill their obligations under FERPA related to Data Breaches by third parties acting as school officials. "While FERPA

---

[67] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2075 (Jan. 11, 2024) (to be codified at 16 CFR 312).
[68] 34 CFR § 99.10(b).
[69] How long does an educational agency or institution have to comply with a request to view records?, U. S. Department of Education, https://studentprivacy.ed.gov/faq/how-long-does-educational-agency-or-institution-have-comply-request-view-records.
[70] *See Children's Online Privacy Protection Rul*e, 89 Fed. Reg. 2034, 2059 (Jan. 11, 2024) (to be codified at 16 C.F.R. pt.312. (The school's ability to review information and request the deletion of such information are addressed in Part IV.D. in connection with the proposed modification to §312.6.) https://www.federalregister.gov/d/2023-28569/p-773.
[71] *To which educational agencies or institutions does FERPA apply?* U.S. Department of Education, https://studentprivacy.ed.gov/faq/which-educational-agencies-or-institutions-does-ferpa-apply.

itself does not contain specific breach notification requirements, it protects the confidentiality of education records by requiring recordation of each incidence of data disclosure."[72] FPF recommends that the rule address this by requiring data breach notification to the school when following the school-authorized education purpose exception.

J. Provide additional clarification of "commercial purposes unrelated to a child's education."

The proposed rule makes clear that "a school-authorized education purpose does not include commercial purposes unrelated to a child's education, such as advertising."[73] Historically, schools have promoted certain types of third-party services to parents, such as school pictures, class rings, yearbooks, and fundraisers. Additionally, most of the State student privacy laws passed since 2014 include language clarifying that the State law does not prohibit an operator "from marketing educational products directly to parents if the marketing did not result from the use of covered information."[74] It is unclear whether these services would be considered unrelated to a child's education. The Commission should provide specificity on "commercial purposes unrelated to a child's education" to clarify the treatment of commercial services traditionally occurring in Schools, and whether parents may consent to the collection and use of child data where that data is treated separately from education record data collected under the school purpose exception.

K. Clarify limitations related to product improvement.

The proposed rule limits the use of child data to "operating[...]maintaining, developing, supporting, improving, or diagnosing the service, provided such uses are directly related to the service the school authorized."[75]

Many operators build edtech services using foundational technologies that are used in more than one product. For example, it would not be practical or beneficial to require an operator to build a separate user sign-on system for a 2nd-grade math app, and another for a 3rd-grade reading app in order to use login data to detect unauthorized login attempts. A similar scenario is likely where AI models are used and improved across multiple instructional applications.

FPF recommends that the FTC provide guidance on the interpretation of "directly related to the service the school authorized" and clarify that the definition of support for the internal operations in the case of school purposes includes this permitted use and related restrictions as applying to

---

[72] *Data Breach Response Checklis*t, U.S. Department of Education(September 2012). https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf.

[73] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2071 (Jan. 11, 2024) (to be codified at 16 CFR 312).

[74] *State Sutent Privacy Laws*, Future of Privacy Forum, https://studentprivacycompass.org/state-laws/. States that include the reference language include: North Carolina, Illinois, Nebraska, Tennessee, Iowa, Michigan, Vermont, Minnesota and California.

[75] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2074 (Jan. 11, 2024) (to be codified at 16 CFR 312).

the operator as well as any third-parties. Additionally, FPF recommends that the Commission provide guidance that avoids unnecessary limitations on using child data in the school context that would prohibit the use of data for legitimate educational research purposes.

I. Clarify the role, if any, of the school as an "intermediary" in the VPC process.

In 1999, the Commission noted in the Final Rule's preamble that "where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent."[76] This guidance appears to conflate the school as a "parent's agent" and the school as an "intermediary," as the two roles are mutually exclusive.

Given the focus on the proposed rule on the school-authorized exception as an exception to prior parental consent and the lack of reference to schools as intermediaries, this suggests it is the FTC's view that a school is a parent's agent rather than an intermediary between the parent and operator. However, it would be helpful if the Commission clarified whether schools may act as intermediaries and if so, the requirements for operators when using schools as intermediaries.

This question is critical when thinking about the interactions between FERPA and COPPA. FERPA requires that the parent or eligible student "provide a signed and dated written consent" before a school or LEA discloses PII from a student's education record unless one of the conditions in § 99.31 of the regulations applies. The written consent must: (1) Specify the records that may be disclosed, (2) state the purpose of the disclosure, and (3) identify the party or class of parties to whom the disclosure may be made. FPF believes there are only very few scenarios where an operator would require VPC that would not require a school to get parental consent under FERPA. One example is contextual advertising, which would be precluded under the proposed school-authorized education purpose, but is not prohibited under FERPA.

In cases where schools cannot provide the school-authorized purpose exception due to the nature of non-educational use or other commercial use, the school must likely facilitate and obtain parental consent under FERPA. Joint guidance would be helpful to clarify how operators and schools should address this circumstance to avoid requiring parents to provide consent twice.

FPF interprets the definition of school-authorized education purpose as the successor to the previous guidance for the school acting as a parental agent and excludes the intermediary use case because "intermediary" applies to cases with a non-educational commercial use. FPF recommends that the Commission clarify if the "intermediary" role exists and provide detailed guidance. In the Edmodo decision, the Commission declined to establish an approved process for a school to act as an intermediary. FPF believes that the intermediary role is inherently problematic, as many operators require schools to obtain consent from parents and retain that

[76] *See* 64 Fed. Reg. 59888, 59903.

consent rather than, as implied in the definition of intermediary, provide the consent to the operator. This practice potentially creates barriers to a parent exercising their COPPA rights, which, absent the school purpose exception, remain with the parent.

The current FTC guidance appears to conflate the “school as parent agent” and "school as intermediary” roles in stating in the COPPA FAQs that “the operator can presume that the school’s authorization is based on the school’s having obtained the parent’s consent.”[77]. As a result of this guidance, the conflation and confusion of the two roles is common in edtech company terms of service.[78] FPF recommends that the Commission provide clear guidance on if and how operators may use schools as intermediaries, and that the use of schools as intermediaries must conform to COPPA’s requirements for parental consent,[79] or update the guidance to remove references to the process.

Thank you for this opportunity to provide input on the proposed rule. We welcome any further opportunities to provide resources or information to assist in this important effort.

Sincerely,

Bailey Sanchez, Senior Counsel for Youth & Education Privacy
Jim Siegl, Senior Technologist for Youth & Education
Daniel Hales, Policy Fellow for Youth & Education Privacy

[77] *Complying with COPPA: Frequently Asked Questions,* Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS.
[78] *Obtaining parental consent (templates included),* Edpuzzle, https://support.edpuzzle.com/hc/en-us/articles/360012390292-Obtaining-parental-consent-templates-included.
[79] *Children's Online Privacy Protection Rule*, 89 Fed. Reg. 2034, 2074 (Jan. 11, 2024) (to be codified at 16 CFR 312).