CENTER FOR DEMOCRACY & TECHNOLOGY

March 11, 2024
Via Regulations.gov

To: Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW, Suite CC–5610 (Annex E)
Washington, DC 20580

Re: COPPA Rule Review, Project No. P195404

The Center for Democracy & Technology (CDT) respectfully submits these comments regarding the Federal Trade Commission's proposed modifications to the Children's Online Privacy Protection Rule (COPPA Rule).[1] CDT is a nonprofit, nonpartisan organization that works to advance civil rights and civil liberties in the digital age. CDT's priorities include promoting privacy safeguards that protect children's personal data while supporting their access to information and communities online.

Our comments address the following issues:

- Providing more effective data minimization limits.
- Supporting and strengthening the proposed amendments regarding direct notice, verifiable parental consent methods, and retention and deletion.
- Recommendations to clarify the proposed amendments regarding biometric data and inferred data in the definition of "personal information" and obligations regarding content personalization.
- Supporting the COPPA Rule's approach to deeming a website or service to be "child-directed" and the Commission's proposed requirement to obtain separate verifiable parental consent for disclosure of personal information.
- Offering detailed recommendations for how to scope the proposed exception to allow schools to consent for the collection of children's information for educational purposes.

[1] Federal Trade Commission, Notice of Proposed Rulemaking on Children's Online Privacy Protection Rule (Jan. 11, 2024), https://www.govinfo.gov/content/pkg/FR-2024-01-11/pdf/2023-28569.pdf [https://perma.cc/X8YK-ZY6B] [hereinafter "COPPA NPRM"].

CENTER FOR DEMOCRACY & TECHNOLOGY

I. The FTC should ensure that the COPPA Rule includes strong data minimization limits

(Responds to Questions 1, 17(b), 18)

The Commission states that §312.7 "serves as an outright prohibition" on collecting more personal information than "reasonably necessary" for a child's participation in an activity, even if consent was obtained for information beyond what is reasonably necessary. The COPPA Rule should be clear that the reasonably necessary standard imposes a genuine substantive limit on data collection and does not allow operators to collect irrelevant, superfluous, and non-useful data.

As an initial matter, the Commission should consider increasing the "reasonably necessary" standard to "strictly necessary." Data about children has long been considered private and sensitive. Increasingly, there are bipartisan calls in Congress for increased privacy protections for children.[2] In the bipartisan American Data Privacy and Protection Act, children's data was considered "sensitive," and therefore its collection and use was required to be "strictly necessary" to the service provided.[3] The term "reasonably necessary" represents a lower standard that gives operators fairly significant interpretive power, whereas "strictly necessary" would be more likely to limit data collection and use to that data without which the service could not function.

In the alternative, the Commission should specify that operators may meet the "reasonably necessary" standard only when not collecting or using children's data in the proposed way would prevent the product or service from functioning. This interpretation of "reasonable" represents the best interpretation to limit collecting and using personal information about children.

Moreover, the current language of §312.7 says that operators may not condition a child's participation in an "activity" on the child's disclosing more personal information than reasonably necessary to participate in that activity. Operators with narrow views on "activity" may conclude that this limit does not apply to browsing their website or service more broadly, unless actively engaging with a particular aspect of that website or service. In that regard, we support the Commission's proposed updated definition of "activity," which would include engaging with the entirety of the website or online service.

---

[2] Ashley Gold, *Bipartisan Lawmakers Make New Push to Protect Kids Online*, Axios (Feb. 14, 2023), https://www.axios.com/2023/02/14/congress-kids-online-safety [https://perma.cc/F29Y-KSBK].

[3] Sec. 2(28)(A)(xiii), Sec 102(2), American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

CENTER FOR DEMOCRACY & TECHNOLOGY

II. Additions to direct notice, verifiable parental consent methods, and retention and deletion requirements are helpful but should be made stronger *(Responds to Question 1)*

The modifications regarding the contents of direct notice to parents, accepted methods for obtaining verifiable parental consent, and retention and deletion help make operators' responsibilities clearer, though some of these provisions could be strengthened further.

A. *Notice to parents*

The Commission proposes expanding the required contents of the direct notice to parents under §312.4(c)(1)(iii) to include not only how the operator intends to collect personal information from the child and how the operator might disclose personal information, but also how the operator intends to use the personal information. Additional information about the intended uses of the child's data is vital for ensuring the parent gives fully informed consent for the operator to collect their child's data, and therefore should be included in the notice.

To further ensure informed consent from parents, the notice required in §312.4(d) should require disclosing the uses and purposes for each type of children's data, not simply children's data more broadly. The same applies to the requirement in §312.10, which would require operators to have a written children's personal data retention policy specifying when the operator plans to delete children's data. This additional specificity would avoid a situation where a company lists various types of data collected from children, then separately lists a variety of uses, with no indication of the purposes for which the specific data types are used.

Additionally, the children's data retention policy mandated by §312.10 should require operators to disclose that they will share personal information only with third parties that also abide by the retention and deletion requirements in COPPA, as already required under §312.8. Disclosing this information will help parents better understand the potential consequences of disclosures to third parties so they can make more informed decisions and provide additional accountability.

B. *Expansion of enumerated methods for obtaining verifiable parental consent*

The COPPA Rule requires any method that operators use to obtain verifiable parental consent to be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[4] The proposed amendments incorporate the use of facial recognition technology into the COPPA Rule's enumerated list of methods that would satisfy this requirement. The new provision explains that an operator may use facial recognition to compare "an image of the parent's face taken with a phone camera or webcam" to an authenticated government-issued photo identification submitted by the parent. The proposed language adds that trained personnel must confirm that the captured image and photo identification match, and that the image and identification must be deleted after confirmation.

By specifying how facial recognition may be used and conditioning such use upon human review and deletion, the Commission makes an important distinction from recent applications for the use of facial analysis to obtain verifiable parental consent. Unlike these applications, which rely on facial age estimation to conclude that the person providing consent is likely old enough to be a parent, the method described in the proposed language would verify both the age and identity of the person providing consent and create enough friction to discourage unauthorized actors from providing consent without being too burdensome for parents.[5] To further clarify the conditions for using this method, the COPPA Rule should state that the operator is responsible for ensuring that deletion processes are incorporated into the children's personal information security program required under §312.8. In addition, the Commission should provide guidance to operators regarding how to confirm that government-issued IDs submitted pursuant to this method are authentic.

C. *Retention and deletion*

The Commission proposes additional language under §312.10 to clarify the COPPA Rule's restrictions on operators' storage of personal information. This language states that operators may retain personal information only for as long as is reasonably necessary for the *specific* purpose for which the information was collected and must delete the information once it is no

[4] 16 CFR §312.5(b)(1).
[5] Center for Democracy & Technology, *Comment on Application for Parental Consent Method, Project No. P235402*, at 4-5 (Aug. 21, 2023), https://cdt.org/wp-content/uploads/2023/08/CDT-Comment-to-FTC-on-Application-for-Parental-Consent-Method-Project-No.-P235402.pdf [https://perma.cc/6AET-4KFJ].

longer reasonably necessary for that purpose. Operators are also explicitly prohibited from retaining the information for a secondary purpose or retaining it indefinitely. Further, the amended section would articulate minimum requirements that operators must include in the notice they must provide on their online services. Specifically, the policy must at least identify the purposes for collection, the business need for retention, and the timeframe for deletion.

We agree that these additions to §312.10 better emphasize operators' data minimization responsibilities. Data retention and deletion requirements go hand-in-hand with up-front minimization requirements like those in §312.7. Even when an operator legally collects data, there is little reason for indefinite retention of that data. Therefore, it is good policy to ensure that operators incorporate soup-to-nuts data practices that begin with collection limits and end with retention limits.

III. The definition of personal information should be further clarified *(Responds to Questions 5, 7, and 8)*

The Commission proposes expanding the definition of "personal information" under §312.2 to include "biometric identifiers that can be used for the automated or semi-automated recognition of an individual." This provision goes on to offer examples of biometric identifiers, including fingerprints, retina and iris patterns, genetic data, and data derived from voice, gait, or facial data. As the Commission rightly observes, coverage of biometric data is necessary because its sensitivity creates a heightened risk to privacy.[6]

To further ensure that biometric data remains adequately covered under this definition, and is not interpreted to be synonymous with the "photograph, video, or audio file" provision of the definition, we would recommend adding clarifying language preceding the examples to describe biometric information. For instance, the Commission can look to the American Data Privacy and Protection Act, which defines biometric information as personal data "generated from the technical processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual."[7]

The Commision declines to refer to inferred data or proxies for personal data explicitly in the definition of "personal information" because COPPA covers only information collected *from* a

[6] COPPA NPRM at 2042.
[7] Sec. 2(3)(A), American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

child.[8] The agency then states that the definition's "catch-all" provision could apply to inferred data when operators collect that data and combine it with another identifier listed in the regulations.[9] However, the catch-all provision includes only when data is collected *from* a child and is combined with other identifiers.[10] Thus, the rule's language would appear to effectively exclude inferred data, even in the catch-all section. The Commission should clarify when the catch-all provision applies to inferred data, and how.

IV. The rules should ensure restrictions on data collection for content personalization purposes *(Responds to Questions 9 and 10)*

The Commission proposes prohibiting operators who use the exception for providing support to internal operations from using personal information in processes that encourage or prompt the use of an online service, including, for example, notifications that prompt the user to engage with the service, without parental consent. In defining the processes subject to this prohibition, we encourage the Commission to consider excluding processes that might be beneficial to children's experience, like filters that direct educational content or features that ensure children can only communicate with people they already know. Such care will ensure that services can continue to create features that are useful to children or personalize their experience of a service in ways that are helpful to children.

The Commission also inquires whether the COPPA Rule's exception allowing persistent identifiers to be used without parental consent for the purpose of personalizing a user's experience on the website or online service should apply only to "user-driven" personalization or also include personalization driven by an operator, for purposes of establishing whether each should fall within the COPPA Rule's exception. We agree with the Commission's proposal that the exception should apply only to user-driven personalization. User-driven personalization is based on a user-initiated act to demonstrate the user's interest in particular content of that website or service. For example, a user may choose to sign into their account on an app where they select an option to see more of a particular type of content or creator, so it is the user's affirmatively expressed choice. By contrast, if an operator wants to personalize the experience on their child users' behalf, that should fall outside the exception and require parental consent.

[8] COPPA NPRM at 2042.
[9] *Id*.
[10] *Id.* at 2072.

Relatedly, the Commission also asks whether changes should be made to the COPPA Rule's treatment of contextual advertising, considering that the Rule currently treats contextual advertising as a type of "support for the internal operations of the website or service" for which persistent identifiers can be collected without obtaining parental consent. Most of the identifiers listed under "personal information" should not be necessary to deliver contextual advertising, which should be based on the content or subject of the web page or app being visited and not the visitor's personal information. Therefore, the Commission should state explicitly that operators should restrict the personal information collected for this purpose to only what is strictly necessary to deliver contextual advertising.

V. The Commission's proposal for evaluating whether operators should be deemed "child-directed" strikes the right balance *(Responds to Question 11)*

We support the COPPA Rule's application of a "totality of the circumstances" standard through the multi-factor test described in the definition of "website or online service directed to children." Whether an operator is deemed "child-directed" should be based on the intended audience demonstrated by the content and context of its website or service, and not just on what the operator states about its audience composition.

We support the Commission's decision not to adopt a constructive knowledge standard to determine whether websites come under COPPA's jurisdiction. The statutory text clearly indicates an actual knowledge standard is required.[11] Any change to that standard should be made by Congress. Moreover, a constructive knowledge standard raises significant free expression and privacy concerns, as it could lead websites to collect additional data about their users to attempt to assess their ages and could also lead sites to remove content directed to older youth in an effort to make their services less attractive to children.

The Commission inquires about whether there should be an exemption in the COPPA Rule for operators that perform an analysis of their audience composition and determine that no more than a specific percentage of users are likely under the age of 13. Much like a constructive knowledge standard, this analysis would incentivize, if not obligate, operators to collect additional data about all of their users to determine the likelihood that the user is a child, which would undermine the children's privacy rights that COPPA is intended to protect and subject

[11] 15 U.S.C. §6502(a)(1).

adult users to increased collection of their personal data.[12] The privacy concerns present in various existing age assurance proposals show that it is premature to mandate an analysis of the ages of an online service's users.[13]

VI. The Commission rightly requires separate verifiable parental consent for disclosure of personal information *(Responds to Question 14)*

The strongest guardrail around disclosure of personal information is to restrict it altogether. To the extent that disclosure may be necessary in certain circumstances, we support the Commission's explicit requirement for operators to obtain separate verifiable parental consent for disclosure so that parents are not automatically agreeing to disclosure when verifiable parental consent is obtained for collection and use.[14] Personal information may present fewer risks when collected and used to support a website or service's internal operations, but could be misused and reshared when disclosed to third parties. Limiting consent to only collection and use forces parents to either accept those risks of disclosure so children can access a website or service, or to deny children a service's benefits to avoid the risks that come with disclosure.

VII. The Commission should add an exception to parental consent for educational purposes with appropriate guardrails *(Responds to Question 16)*

We support the Commission's proposal to codify an exception to allow schools to consent for the collection of children's information for educational purposes.[15] CDT advocated for this exception in our comments in response to the Commission's 2019 rulemaking.[16] Harmonizing federal laws aimed at protecting student privacy is critical to supporting school leaders in their efforts to use data and technology responsibly. We restate that advocacy here, with additional suggestions to retain distinct protections in the COPPA Rule regarding parents' rights that should be preserved and brought into alignment with federal student privacy laws.

---

[12] Center for Democracy & Technology, *Comment to NTIA on Initiative to Protect Youth Mental Health, Safety, and Privacy Online* 9-11 (Nov. 16, 2023), https://cdt.org/wp-content/uploads/2023/11/CDT-Comments-NTIA-to-Protect-Children.pdf [https://perma.cc/P7LM-EZFG].

[13] *Id.* at 11.

[14] 16 CFR §312.5(a)(2).

[15] COPPA NPRM at 2075.

[16] Emma Llansó, Michelle Richardson, and Elizabeth Laird, *Comments to the FTC on the 2019 COPPA Rule Review*, Center for Democracy & Technology (Dec. 12, 2019), https://cdt.org/wp-content/uploads/2019/12/CDT-COPPA-2019-Rule-Review-Comments.pdf [https://perma.cc/77VM-F77F].

As CDT has previously commented, requiring schools to obtain parental consent for each individual use of education technology would be unduly burdensome for schools, undermine their decision-making authority, and would not effectively protect student privacy. Some schools do not have the resources or the time to ask for consent from parents every time they rely on an educational technology product, just as they do not ask for consent from parents around the curriculum that is used or other instructional and operational decisions that a school makes in the course of educating students. Schools are responsible for a number of functions like transportation, state and federal reporting, meal services, and most importantly, delivering high-quality instruction. Education data and technology may be required to support some of this important work, so schools need to be able to responsibly and ethically use data and technology in support of these efforts. Schools are already regulated and responsible for meeting privacy and security standards in how they collect and use student data under the Family Educational Rights and Privacy Act (FERPA) and various state laws.

We support the proposed education exception provided it is accompanied by appropriate guardrails, discussed below, including the following: a clear definition of school-authorized education purpose, with explicit designated exclusions; standards and limitations on the use of student data for product improvement; guidance on who can authorize the collection of student data; strong written agreements between operators and schools; maintaining the rights of a parent to provide or withhold consent for the collection of particularly sensitive information; and maintaining the rights of a parent to review the data collected about their child.

A. *Defining school-authorized education purpose*

We commend the Commission for posing the important question of what types of services should be covered under a "school-authorized education purpose."[17] In the interest of harmonizing COPPA and FERPA, we suggest using a standard similar to that of the exception to parental consent for disclosure in FERPA: the standard for a "legitimate educational interest" under the school official exception.[18]

According to the U.S. Department of Education, a "school official" has a "legitimate educational interest" in the information if the official needs to review the education record in order to fulfill

[17] COPPA NPRM at 2043-44, 2056-57.
[18] 34 CFR § 99.31(a)(1).

their professional responsibility.[19] However, the criteria for what constitutes a "legitimate educational interest" will vary by school and/or locality. An example of the criteria for what constitutes a "legitimate educational interest" might include: the information requested is necessary for that official to perform appropriate tasks that are specified in their position description or by a contract agreement; the information is to be used within the context of official agency or school business and not for purposes extraneous to the official's areas of responsibility or to the agency or school; the information is relevant to the accomplishment of some task or to a determination about the student; or the information is to be used consistently with the purposes for which the data are maintained.[20]

Similarly, the criteria for who qualifies as a "school official" will also vary by school and/or locality, as FERPA requires schools and local education associations (LEAs) to establish and publicly notice their own criteria for both of these elements. An example of the criteria schools and LEAs might set for who can be a "school official" might be a person employed by the agency or school in an administrative, counseling, supervisory, academic, student support services, or research position, or a support person to these positions; or a person employed by or under contract to the agency or school to perform a special task.[21]

Because these criteria may vary based on locality, the Commission should consider using language that accounts for this potential variation and honors the interpretation set forth by that school or locality. For example, a rule could provide that, "Information collected for a school-authorized education purpose shall include any information in which a 'school official' has a 'legitimate educational interest'. The operator shall rely on the definition of 'school official' and 'legitimate educational interest' set out in the school's annual FERPA notice when assessing the validity of the authorization."

Additionally, we believe the Commission has an opportunity here to both align with FERPA and to retain distinct aspects of COPPA relative to parental rights and further strengthen student privacy where commercial third-parties are involved by retaining parental consent requirements

[19] U.S. Department of Education, *Under FERPA, May An Educational Agency Or Institution Disclose Education Records To Any Of Its Employees Without Consent?*, https://studentprivacy.ed.gov/faq/under-ferpa-may-educational-agency-or-institution-disclose-education-records-any-its-employees [https://perma.cc/XYB5-282D].

[20] National Forum on Education Statistics, *Defining "Legitimate Educational Interests", in* Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies (2004), https://nces.ed.gov/pubs2004/privacy/section_4b.asp [https://perma.cc/6CWF-W95A].

[21] *Id*.

for the collection of especially sensitive information even when it will be used for school-authorized education purposes.

1. *Retaining parental consent requirements where detailed in other federal and state student privacy laws*

Rather than transferring all consent rights to schools, it is important to retain parental consent rights regarding particularly sensitive, non-academic information to be consistent with other federal and state student privacy laws. To that end, the Commission should consider exclusionary language either in the definition of school-authorized education purpose or in the broader exception language that would offer additional protection for the most sensitive types of data.

Strong precedent for this can be found in both federal and state law, where parental consent is already required to collect certain types of information. For example, the Protection of Pupil Rights Amendment (PPRA) under the General Education Provision Act (GEPA) (34 CFR Part 98 implementing section 445) requires that written parental consent be given prior to the administration of a survey, analysis, or evaluation "in which the primary purpose is to reveal information concerning one or more of the following":

1. political affiliations or beliefs of the student or the student's parent;
2. mental or psychological problems of the student or the student's family;
3. sex behavior or attitudes;
4. illegal, anti-social, self-incriminating, or demeaning behavior;
5. critical appraisals of other individuals with whom respondents have close family relationships;
6. legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
7. religious practices, affiliations, or beliefs of the student or student's parent; or
8. income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

Similar language can also be found in Utah and Louisiana's student privacy laws.[22] Citing to this list in the PPRA (34 CFR §98.4 (a)(1)-(8)) as a carve-out to the school consent exception (where an operator would require schools to attest in writing that they have collected parental consent for the collection of this information) would protect students' privacy and prevent harms like outing or unwanted disclosure/collection of other sensitive information.[23]

One particularly concerning data element not listed in PPRA (but one that can be found in state law and is being contemplated as an update to the COPPA Rule's definition of personal information) is biometric data. Given the particularly sensitive and permanent nature of biometric data, it should be excluded from any exception for a school-authorized education purpose.

The PPRA was written in the 1970s when the primary method of collecting information about students was conducting paper surveys. The law at that time did not contemplate automated collection of student data and thus in its current form, PPRA does not require operators to obtain parental consent before collecting that type of information.

The Commission has an opportunity now to both bring the COPPA Rule into alignment with longstanding federal student privacy laws (as well as the forward trend of state privacy laws) and close the gap that automated data collection has created in protecting student privacy under these laws by making clear that any exception for school authorization does not encompass these sensitive types of information. For example, a school-authorization exception could include a carve-out such as the following: "This exception shall not apply to the collection of biometric information or the information described in 34 CFR §98.4(a)(1)-(8) (the Protection of Pupil Rights Amendment)." In implementing this, operators and schools will need to work together to verify the identity of the parent(s) for whom they would need to seek consent for the collection of this information.

---

[22] Utah Code 53E-9-203 (2018), https://le.utah.gov/xcode/Title53E/Chapter9/C53E-9_2018012420180124.pdf [https://perma.cc/QJ5L-PSCA]; Louisiana Revised Statutes §17:3914(C)(1) (2022), https://legis.la.gov/legis/Law.aspx?d=920124 [https://perma.cc/S279-WMXR].

[23] 19 percent of students in 2023 reported that they or someone they know has been outed as a result of student activity monitoring. This figure is up 6 percentage points from the previous year, and is expected to continue to rise without intervention to protect this type of data. *See* Elizabeth Laird, Maddy Dwyer, and Hugh Grant-Chapman, *Off-Task: EdTech Threats to Student Privacy and Equity in the Age of AI* at 28, Center for Democracy & Technology (2023), https://cdt.org/wp-content/uploads/2023/09/091923-CDT-Off-Task-web.pdf [https://perma.cc/3Z6Z-WXSA].

2. *Apply guardrails to student data use for product improvement*

We generally support the Commission's proposal that an operator be permitted to use student data to improve the service those students are receiving under the "school-authorized education purpose" definition. However, the use of this data for product improvement requires guardrails around de-identification and limits on reuse and sharing.

While there is value in using student data for product improvement, keeping large amounts of identifiable student data for this purpose creates more risk of harm in the event of a breach. Currently under FERPA, student information that has been de-identified is not protected and thus is not subject to FERPA's use and re-disclosure limitations. To meet the definition of de-identification in FERPA, education entities must remove enough student information such that "a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information."[24] However, as the Commission is aware, this is more complicated than it might seem. For example, approaches to de-identification can range from simply deleting direct identifiers like student name or ID number (which is typically not sufficient to prevent the data from being re-identified) to more sophisticated techniques like shuffling or adding noise to the data that make recovery more difficult (these more complex approaches are generally referred to as "anonymization" in computer science).[25]

In reality, it is very difficult to properly de-identify any information with certainty that it will never be re-identified, as is evident from the examples below.

- New York City officials accidentally revealed the detailed comings and goings of individual taxi drivers in a case of a public release of data that was poorly de-identified, with just a handful of random location data points being uniquely identifiable 95 percent of the time.[26]

[24] Elizabeth Laird & Hannah Quay-de la Vallee, *Balancing the Scale of Student Data Deletion and Retention in Education*, Center for Democracy & Technology (Mar. 2019), https://cdt.org/wp-content/uploads/2019/03/Student-Privacy-Deletion-Report.pdf [https://perma.cc/JQ5R-P8RH].
[25] Llansó, Richardson, & Laird, *supra* note 16.
[26] Dan Goodin, *Poorly Anonymized Logs Reveal NYC Cab Drivers' Detailed Whereabouts*, ARS Technica (June 23, 2014), https://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ [https://perma.cc/75C5-ZS8E].

- In 2016, the Australian government released an anonymized dataset of medical billing records, including prescriptions and surgeries. Researchers quickly noted "the surprising ease with which de-identification can fail" when additional datasets are cross-referenced.[27]
- Looking at 200 tweets, researchers were able to use associated metadata like timestamps, number of followers, and account creation time to identify anyone in a group of 10,000 Twitter users 96.7 percent of the time.[28] Even when muddling the metadata, a single person could still be identified with more than 95 percent accuracy.

To that end, we ask that the Commission be explicit in the text of a school-authorized education purpose that the use of student data for product improvement requires that the data be sufficiently de-identified in line with FERPA guidance from the Privacy Technical Assistance Center (PTAC) at the U.S. Department of Education, which reads:

> *De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. [The provider will] not attempt to re-identify de-identified Data [nor] transfer de-identified Data to any party unless that party agrees not to attempt re-identification.*[29]

B. *Creating and enforcing written agreements between operators and schools*

In the Commission's proposed language for the school authorization exception, it requires there be a written agreement between the operator and school that:

- Indicates the name and title of the person providing authorization and attests that the person has the authority to do so;

---

[27] Chris Culnane, Benjamin I. P. Rubinstein, Vanessa Teague, *Health Data in an Open World*, Cornell University arXiv (December 15, 2017), https://arxiv.org/abs/1712.05627 [https://perma.cc/77F6-QWE5] (finding that de-identified patient data can be re-identified).

[28] Chris Stokel-Walker, *Twitter's Vast Metadata Haul is a Privacy Nightmare for Users*, Wired (July 9, 2018), https://www.wired.co.uk/article/twitter-metadata-user-privacy [https://perma.cc/2KKR-FY38].

[29] *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service*, Privacy Technical Assistance Center (Mar. 2016), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf [https://perma.cc/S58E-YPG2].

- Limits the operator's use and disclosure of the personal information to a school-authorized education purpose only and no other purpose;
- Provides that the operator is under the school's direct control with regard to the use, disclosure, and maintenance of the personal information collected from the child pursuant to school authorization; and
- Sets forth the operator's data retention policy with respect to such information in accordance with §312.10.[30]

We support a written agreement requirement between operators and schools, as it is a fundamental best practice in governing and enforcing expectations about how sensitive information is handled and used.

The Commission has previously inquired about whether the COPPA Rule should specify who at the school can provide consent. We advocated then, as we do now, that the COPPA Rule should align with FERPA's "school official" exception, as described above in Section A.

Written agreements are only as effective as the terms within the agreement and the extent to which they are enforced. The agreements should not only designate responsible parties, as put forth in the proposed rule, but also include terms needed to maintain direct control of student information. Simply requiring schools to designate a point of contact and attestation of authority to sign is insufficient protection for students and families when replacing their ability to consent with that of the school. While the proposed rule requires that schools maintain direct control over information shared with third parties, it should include requirements elaborating on what such control entails. To that end, written agreements should also be required to include standard components of data sharing agreements necessary to effectively govern student information. Those components include: (a) assurances against further disclosure; (b) clear retention and deletion policies; (c) maintaining the right to audit the operator's policies, procedures, and systems; (d) specified points of contact/data custodians; (e) school ownership of PII from education records; (f) identified penalties for noncompliance; (g) specified modification or termination procedures; and (h) maintaining the right to verify FERPA training of operator's employees.[31]

---

[30] COPPA NPRM at 2075.

[31] *See The Family Educational Rights and Privacy Act: Guidance for Reasonable Methods and Written Agreements*, Privacy Technical Assistance Center, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Guidance_for_Reasonable_Methods%20final_0_0.pdf [https://perma.cc/X3E2-N6WK].

Without enhancing the requirements in written agreements, we are concerned that the prescribed language does not require any protective language on the school's behalf–the school's only contribution to the written agreement is a name and attestation of authority to sign. Currently, a common practice is for operators to provide schools with clickwrap agreements,[32] which may or may not include terms that sufficiently protect student information. As it stands, schools, especially those that have fewer resources and lack dedicated legal counsel, would face significant obstacles to ensure that operators amend agreements such that they protect students and their families. Requiring that these agreements include effective governance of student information will harmonize the COPPA Rule with other federal student privacy laws, as well as hold operators accountable for protecting student privacy, in addition to schools.

C. *Maintain a right for schools and parents to review personal information provided by the child*

When a school is allowed under the COPPA Rule to consent to a child's use of an educational technology product in lieu of parental consent, the school should also receive the COPPA rights to ensure control and access to that information.[33] Those rights include the right to review and request amendments and delete student data. Ensuring that these parental rights, as described under the COPPA Rule, carry over to the school would firmly align the statute with FERPA, where the entities that the school allows to collect and store student information because they are stepping into the role of school officials must be "under the direct control of the agency or institution with respect to the use and maintenance of education records."

Although the school would be given the rights of a parent under the school authorization exception, FERPA still provides parents with the right to request amendments of children's records through the school if they believe the "education records relating to the student contain information that is inaccurate, misleading, or in violation of the student's right to privacy." For parents to effectively exercise this right, they need to be able to access information that is not

[32] "A form of agreement that "requires the user to agree to terms and conditions before using a website or completing an installation or online purchase process. These agreements typically present the terms and conditions followed by a check box with the words "I agree" or "I accept" that the user must deliberately click." Glossary, *Clickwrap Agreement*, Thomson Reuters, https://content.next.westlaw.com/practical-law/document/Ia2a8736d216911e89bf099c0ee06c731/Clickwrap-agreement?viewType=FullText&transitionType=Default&contextData=(sc.Default) [https://perma.cc/RGU9-CBNV].

[33] COPPA NPRM at 2059, 2075.

only maintained by the school, but also by operators who are providing services on behalf of the school.

Although it seems straightforward that a parent could request this information through the school, it has unfortunately proven difficult, and parents have been refused access to this vital information. For example, in Maryland, a parent was seeking access to the information held about their child by an edtech vendor. The parent first went to the school with the request but was told they'd need to request that information from the vendor directly. When the parent went to the vendor, they were directed right back to the school, with no resolution.[34] In Nevada, a parent was reportedly given a $10,000 bill to view data about their child held in the state's longitudinal data system because the school argued that this information did not fall under the definition of an "education record" and thus was not subject to parental access under FERPA (this was later addressed and remedied by the Department of Education).[35]

While shifting the responsibility for providing access to student data held by edtech vendors to schools is likely easier for operators, it is not necessarily easier for parents (as illustrated by the above examples). Given these frustrations, the language in §312.6(b) in the proposed amendments should be explicit that parents will retain the right to review data collected about their child directly from the vendor if attempts to access it through the school have been unsuccessful.[36] In this instance, the operator should consult with the school to verify that the parent or guardian is legally entitled to exercise their right to review per the school's records.

VIII. Conclusion

We appreciate that the FTC is updating its COPPA Rule to keep up with technology. We support the agency's efforts and look forward to engaging on these important issues.

---

[34] Caitlynn Peetz, *MCPS Parents Help Lead Push for Better Federal Student Privacy Protections*, MoCo 360 (Jul. 9, 2021), https://moco360.media/2021/07/09/mcps-parents-help-lead-push-for-better-federal-student-privacy-protections/ [https://perma.cc/3ATZ-F2Y3].

[35] Karen Gray, *Federal Education Officials: Nevada Can't Charge Dad to Look at Children's Records*, Nevada Journal (Dec. 30, 2014), https://www.npri.org/nevadajournal/federal-education-officials-nevada-cant-charge-dad-look-childrens-records/ [https://perma.cc/AJ53-TFWS].

[36] COPPA NPRM at 2075.