



Via Online Submission November 17, 2017:

<https://ftcpublishcommentworks.com/ftc/studentprivacyedtechworkshop/>

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Suite CC-5610 (Annex A)  
Washington, DC 20580

Re: Student Privacy and Ed Tech and P175412

We submit the following comments on behalf of the Parent Coalition for Student Privacy, the Campaign for a Commercial-Free Childhood, and the Center for Digital Democracy in response to the Federal Trade Commission's notice regarding the FTC and Department of Education's workshop to explore privacy issues related to education technology. Our comments consist of responses to the questions posted in the FTC's comment form.<sup>1</sup>

**Question 1: Are the joint requirements of FERPA and COPPA sufficiently understood when Ed Tech providers collect personal information from students? Are providers and schools adhering to the requirements in practice?**

Response 1: The joint requirements of FERPA and COPPA are not sufficiently understood when operators of online services, including Ed Tech providers, collect personal information from students. There is huge confusion among parents about their rights under FERPA and COPPA. We have been approached by many parents who have concerns that their schools and providers are not adhering to these laws, but it is difficult to say in some cases because of the ambiguity of the guidance, and the lack of enforcement or oversight.

For example, according to one guidance document provided by the U.S. Department of Education's Privacy Technical Assistance Center, the question, "Is Student Information Used in Online Educational Services Protected by FERPA?" is answered with, "It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question."<sup>2</sup> The document provides a limited number of "examples" to illustrate the guidance, but there are dozens of other scenarios that are worthy of similar explanation, including whether an authorized "school official" can use student information for commercial purposes.

---

<sup>1</sup> See <https://ftcpublishcommentworks.com/ftc/studentprivacyedtechworkshop/>

<sup>2</sup> See

[https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29\\_0.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf)

COPPA's guidance is also unclear about an operator's use of a child's personal information for "commercial purposes." For example, under M.2. on the "Complying with COPPA: Frequently Asked Questions" ("COPPA FAQ") website, it states if an "operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent."<sup>3</sup> Yet "commercial purposes" are not clearly defined.

Without sufficient guidance, teachers and schools are adrift, and are using websites and apps that gather student information to develop and improve their own products and services, which we believe is a "commercial purpose" and should not be allowed. Online instructional programs or other kinds of apps also often link to other websites and programs like YouTube that gather personal information for marketing purposes or advertising to students. It's unclear if and how this practice is currently allowed under FERPA and/or COPPA, and we do not believe that it should be.

Parents also seek clarification on whether personally identifiable student information, including "other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information,"<sup>4</sup> collected by operators is considered an education record under FERPA. We believe if student data is to be collected by operators and included in the student grades, transcripts, or other critical functions it should be covered under FERPA. If it is not included in the student's education record that is stored by the school or district, then it should be under the control of the parent and subject to deletion upon their request, just as parents are allowed this right under COPPA outside of the school context.

Parents are also questioning the legal status of titular non-profits that are not bound by COPPA, but are being funded by for-profit partners or have for-profit contractors. If the non-profit is outsourcing its operation to a for-profit and/or disclosing this data to for-profit partners -- we believe they should be responsible for adhering to COPPA; for example, the partnerships between the PARCC Consortium and Pearson, and Summit Schools and Facebook/Chan Zuckerberg Initiative.

In addition, when parents suspect that the school or district and/or operators are violating FERPA or COPPA, the complaint process is difficult to navigate and often there is no response from the U.S. Department of Education or the FTC.

Finally, given the increased number of data breaches by districts and operators, and the rising incidence of ransomware attacks, strict security standards should be incorporated into both FERPA and COPPA regulations, because data privacy is meaningless without data security as well. For more on this, see the letter from EPIC dated June 6, 2016, to the US Department of Education, urging that 34 C.F.R. Part 99 ("Family Educational Rights and Privacy") be amended "to establish data security standards including administrative, physical, and technical safeguards to prevent the unauthorized disclosure of personally identifiable student information."<sup>5</sup> The Cyber Security Alert from the US Department of Education dated

---

<sup>3</sup> See <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools>

<sup>4</sup> See <http://ptac.ed.gov/glossary/personally-identifiable-information-education-records>

<sup>5</sup> Posted at <https://epic.org/privacy/student/ED-Data-Security-Petition.pdf>

October 16, 2017 urged schools and districts to adopt rigorous security practices, including security audits, audit logs, security staff trainings, and limiting access to sensitive data. These security protections should be **required**, not just suggested.<sup>6</sup>

## **Question 2: What practical challenges do stakeholders face in simultaneously complying with both COPPA and FERPA?**

Response 2: Parents need clarification on whether they have any substantive rights, including the right to know, when their children's schools assign them to work on online programs at school or for homework and the online program is collecting their personal data. For example, the COPPA FAQ page suggests that "As long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. However, as a best practice, schools should consider making such notices available to parents, and consider the feasibility of allowing parents to review the personal information collected." In reality, few if any schools obtain the parent's consent and even fewer are making the notices available to parents.

Parents are also confused and concerned about the revised COPPA guidance from March 20, 2015 – in which it was determined that operators "must provide the **school** a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information" rather than the parent. Parents should not have fewer rights in the school context than in a consumer space, and providers of online education websites and services should be held to stronger, enforceable security and privacy standards.

The U.S. Department of Education does not require schools to notify parents of which online websites, programs, apps and services their children are using at school or at home, and what data is being collected from them, but rather suggests they should do so as a "best practice."<sup>7</sup> COPPA guidance also suggests that schools should provide the required notices to parents as a "best practice." Yet few if any schools currently adhere to these best practices, nor are they likely to adhere unless they are written into guidance or regulations.

These are gaping holes in FERPA and COPPA, and parents don't know who to contact and who is responsible for data privacy and security when there are third parties collecting student information. Both FERPA and COPPA should require schools to provide this information to parents, not merely recommend that they do so.

Teachers are overwhelmed and do not have the time to wade through operators' Privacy Policies and Terms of Service to see if student data is being used improperly for commercial purposes, which are undefined. Although the COPPA FAQ recommends that "schools or school districts decide whether a

---

<sup>6</sup> See <https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html>

<sup>7</sup> See [http://ptac.ed.gov/sites/default/files/LEA%20Transparency%20Best%20Practices%20final\\_0.pdf](http://ptac.ed.gov/sites/default/files/LEA%20Transparency%20Best%20Practices%20final_0.pdf)

particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher," few are doing so and most lack the resources to do it thoughtfully.

**Question 3: Under what circumstances is it appropriate for a school to provide COPPA consent, and what process should the Ed Tech provider use to obtain consent? Who has the authority to provide and revoke consent and how?**

Response 3: Schools should be required to notify parents, and operators should be required to obtain their consent for use of online services subject to COPPA. The notice should include the names, websites, and Privacy Policy/Terms of Service of every applicable operator that the district has determined to be COPPA compliant, what specific data is being collected from students, and how it is being used, protected and secured. Operators should be required to obtain parental consent whether their services are used inside or outside of the school.

Currently, the COPPA FAQ website states: "As long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent." First, in most cases, schools are not able to limit an operator's use of a child's information to the educational context because they are simply agreeing to an operator's Terms of Service/Terms of Use, which can be changed unilaterally by the operator. Second, schools are not obtaining parental consent. Operators should be required to obtain parental consent whether their services are used inside the school context or outside.

Parents should be granted the rights under the law as COPPA guidance stated prior to the March 20, 2015 revision: operators "must provide parents, upon request, a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information,"<sup>8</sup> especially if the data is not to be incorporated into a child's education record.

**Question 4: COPPA and FERPA both limit the use of personal information collected from students by Ed Tech vendors. What are the appropriate limits on the use of this data?**

Response 4: COPPA currently only allows schools to consent on behalf of parents if student data is not going to be used for commercial or marketing purposes. But companies shouldn't be allowed to use student data collected in mandatory school activities or homework assignments for marketing purposes even if parental consent is obtained. Imagine, for instance, a school is using Amazon Echo for a project, so the school sends a form home requiring parents to consent to Amazon sharing the data with third-parties so their kids can participate in this activity. The FTC should make clear that compelling parents to consent so that their children can participate in a required educational activity is not meaningful consent as required by COPPA.

---

<sup>8</sup> See <https://web.archive.org/web/20150203040200/https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>

Further, even though there are provisions in COPPA requiring that the data not be used for commercial purpose without parental consent, there is no actionable definition of this. Much of the student data is being used to improve their products and services, which our organizations believe should be defined as a commercial purpose.

We also question any use of targeted advertisements in supposedly “educational” programs or services. We believe this is a commercial purpose, not an educational purpose. Ads of any kind, whether targeted or not, and whether based upon a child’s one-time online visit to a website or multiple visits, are a distraction to students, not an enhancement to their learning. Further, schools should not assign students to visit websites that use their personal information for marketing purposes, and vendors should not include links to such sites in their programs either. There needs to be a bright line definition and strong enforcement barring this common practice.

**Question 5: How should requirements concerning notice, deletion, and retention of records be handled and by whom and when?**

Response 5: As stated above, parents believe COPPA’s guidance prior to the March 20, 2015 revision should be restored, so that operators must provide “parents, upon request, a description of the types of personal information collected; an opportunity to review the child’s personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child’s personal information,” especially if the data is not incorporated in the child’s education record at the school or district.

**Question 6: Schools often use the “School Official Exception” to FERPA’s written consent requirement when disclosing personally identifiable information from education records to Ed Tech providers. In your experience, what are some of the ways in which schools maintain “direct control” over Ed Tech providers under FERPA’s “School Official Exception?” Should there be alignment between the “School Official Exception” and schools’ ability to provide consent for purposes of COPPA?**

Response 6: There should be a requirement in FERPA for written agreements under the “school official” exception, and all such agreements and/or contracts should be transparent and available to parents. There should be no non-disclosure agreements allowed in these contracts, limiting the right of the school or district staff to communicate with parents or members of the public about the vendor’s product or services. And if using the school official exception, the contracts should have to specify exactly what types of student data are collected, for what purpose the vendor needs access to the data and how exactly it will be used, and bar the vendor from making any disclosures of the data without parental consent

Sincerely,

Parent Coalition for Student Privacy  
Campaign for a Commercial-Free Childhood  
Center for Digital Democracy