

## COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

COPPA Rule Review, 16 CFR part 312, Project No. P195404

RIN 3084–AB20

December 11, 2019

---

By notice published on July 25, 2019, the Federal Trade Commission (“FTC”) has proposed revisions to the agency’s Children’s Online Privacy Protection Act (“COPPA” or “the Act”) Rule.<sup>1</sup> Pursuant to this notice, the Electronic Privacy Information Center (“EPIC”) submits these comments and recommendations to ensure that children’s privacy is adequately protected in response to changes in technology, business practices, and the use of the Internet.

EPIC recommends that (1) the FTC maintain the strong safeguards for children’s data that Congress intended, (2) the FTC reject the “school official exception”; (3) the FTC define the term “commercial purpose” and ensure that children’s personal data collected in schools is not transferred to EdTech companies; and (4) the FTC require notification within forty-eights of a data breach of children’s data by a company subject to COPPA.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and Constitutional values. EPIC has a particular interest in protecting children’s online privacy

---

<sup>1</sup> FTC, *Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule*, 84 Fed. Reg. 35,842 (proposed July 25, 2019) (to be codified at 16 C.F.R. pt. 312), <https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online>.

and has played a leading role in both the drafting of the COPPA and developing the authority of the FTC to address emerging children’s privacy issues.<sup>2</sup> Notably, EPIC President, Marc Rotenberg, contributed to the drafting of the Act in 1998. Since then, EPIC has filed comments with the FTC during its previous COPPA rulemaking with the goal of strengthening privacy protections for children under the Act.<sup>3</sup> In response, the Commission adopted changes to the definition of “personal information” to include photo, video, and audio files of children, which EPIC supported.<sup>4</sup>

Since enactment of the law and adoption of the regulation, EPIC believes the FTC must now establish clear safeguards for children’s data gathered in schools. While the Commission poses many questions encompassing changes to COPPA Rule definitions, appropriate ways to address general audience websites like YouTube, and a review of program requirements such as confidentiality, security, and integrity of personal information collected from children, we believe that advancement of EdTech in schools is the most pressing issue that must be addressed. The Commission “poses its standard regulatory review questions to determine whether the

---

<sup>2</sup> See EPIC, *Children’s Privacy Protection and Parental Empowerment Act: Hearing on H.R. 3508 Before the Subcommittee on Crime of the House Committee on the Judiciary*, 104th Cong (1996), (statement of Marc Rotenberg, Executive Director, EPIC), available at [https://epic.org/privacy/kids/EPIC\\_Testimony.html](https://epic.org/privacy/kids/EPIC_Testimony.html); EPIC, *EPIC Letter to Christine Varney on Direct Marketing Use of Children’s Data* (December 14, 1995), available at [http://epic.org/privacy/internet/ftc/ftc\\_letter.html](http://epic.org/privacy/internet/ftc/ftc_letter.html); EPIC, *Children’s Online Privacy Protection Act (COPPA)*, <https://epic.org/privacy/kids/>; see also EPIC, *In the Matter of Universal Tennis*, Complaint, Request for Investigation, Injunction, and Other Relief (May 17, 2017), <https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf>; EPIC, *In the Matter of Genesis Toys and Nuance Commc’ns*, Complaint and Request for Investigation, Injunction, and Other Relief (December 6, 2016), <https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf>; EPIC, *In the Matter of Facebook, Inc. and the Facial Identification of Users*, Complaint, Request for Investigation, Injunction, and Other Relief (June 10, 2011) [https://epic.org/privacy/facebook/EPIC\\_FB\\_FR\\_FTC\\_Complaint\\_06\\_10\\_11.pdf](https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf); EPIC, *In the Matter of Echometrics*, Complaint, Request for Investigation, Injunction, and Other Relief (Sept. 25, 2009), <https://epic.org/privacy/ftc/Echometrics%20FTC%20Complaint%20final.pdf>.

<sup>3</sup> Comments of EPIC, *Agency Information Collection Activities; Proposed Collection; Comment Request*, File No. 49557 (Dec. 3, 2018), <https://epic.org/apa/comments/EPIC-FTC-COPPA-Dec2018.pdf>; Comments of EPIC, *Children’s Online Privacy Protection Act Rule Review*, Project No. P104503 (Sept. 24, 2012), <https://epic.org/privacy/kids/EPIC-COPPA-2012-Rule-Rev-Cmts.pdf>.

<sup>4</sup> See Comments of EPIC, *Children’s Online Privacy Protection Act Rule Review*, Project No. P104503 (Sept. 24, 2012), <https://epic.org/privacy/kids/EPIC-COPPA-2012-Rule-Rev-Cmts.pdf>.

[COPPA] Rule should be retained, eliminated, or modified.”<sup>5</sup> The request for review is based on the “rapid pace” at which the online environment for children continues to develop, including the increase in education technology (“EdTech”) used in schools.

The FTC’s COPPA Rule review is a timely opportunity to help resolve these outstanding children’s privacy issues. On December 1, 2017, the FTC co-hosted a workshop with the Department of Education (“ED”) to examine student privacy and the intersection between the FTC’s COPPA Rule and the ED’s Family Educational Rights and Privacy Act (“FERPA”).<sup>6</sup> Panel speakers representing school districts, parental-rights organizations, and public interest groups brought to light significant children’s privacy issues related to the COPPA Rule in an education setting, and raised many unanswered questions. The one clear finding is that there are insufficient privacy safeguards for the personal data of students.

## **I. The Current COPPA Rule is Effective at Protecting Children’s Privacy.**

EPIC has long advocated for the FTC to place meaningful limits on data collection from children and has urged the Commission to vigorously enforce the COPPA Rule. The rule provides a sensible approach that recognizes both the unique vulnerabilities of young children and the limitations of a self-regulatory approach that would place an unreasonable burden on young minors to interpret privacy policies and make informed decisions about the disclosure and use of personal information.<sup>7</sup>

---

<sup>5</sup> FTC, *Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule*, 84 Fed. Reg. 35,842, 35,843 (proposed July 25, 2019) (to be codified at 16 C.F.R. pt. 312), <https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online>.

<sup>6</sup> *Student Privacy and Ed Tech*, FTC (Dec. 1, 2017) <https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech>.

<sup>7</sup> *An Examination of Children’s Privacy: New Technologies and the Children’s Online Privacy Protection Act (COPPA): Hearing Before the Subcommittee on Consumer Protection, Product Safety, and Insurance of the Senate Committee on Commerce, Science, and Transportation*, 111th Cong. (Apr. 29, 2009) (statement of Marc Rotenberg, Director, EPIC), at 2-5, [http://epic.org/privacy/kids/EPIC\\_COPPA\\_Testimony\\_042910.pdf](http://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf).

The benefits of the COPPA Rule are substantial. Children—who lack the ability to understand and assess sophisticated data collection practices—receive a heightened level of protection under COPPA compared to other privacy laws concerning adults. Parents benefit because operators are required to provide information about the kind of data collected about their children and the opportunity to limit data collection and use. Operators benefit because the COPPA Rule and the statute both set forth clear guidelines that enable companies to identify permissible business practices involving the collection, storage, and disclosure of children’s personal information.

The FTC’s 2013 amendments to the COPPA Rule expanded the types of information covered and correctly sought to keep pace with changes in technology.<sup>8</sup> EPIC supported the expanded definition of “personal information,” which now includes photo, video, and audio files that contain a child’s image or voice.<sup>9</sup> This updated definition was responsive to technological changes and new business practices that threatened children’s privacy. EPIC commends the Commission for conducting its ten-year review of the COPPA Rule early, recognizing again that changes in technology and new business practices have developed, which must be addressed to further protect children’s online privacy, particularly in the EdTech sector.

## **II. Operators and Schools Must Comply with COPPA**

COPPA applies to children everywhere, not just in the home. Students do not “shed their constitutional rights to freedom of speech or expression at the schoolhouse gate.”<sup>10</sup> Nor do they

---

<sup>8</sup> See *Children’s Online Privacy Protection Rule*, 78 Fed. Reg. 3,972 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312), <https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule>.

<sup>9</sup> See, e.g., Comments of EPIC, *Children’s Online Privacy Protection Act Rule Review*, Project No. P104503 (Sept. 24, 2012), <https://epic.org/privacy/kids/EPIC-COPPA-2012-Rule-Rev-Cmts.pdf>; Comments of EPIC, *Children’s Online Privacy Protection Act Rule Review*, Project No. P104503 (Dec. 23, 2011), <https://epic.org/privacy/kids/EPIC-COPPA-Rule-Comments-FINAL-12-23-11.pdf>.

<sup>10</sup> *Tinker v. Des Moines Indep. Cmty. School Dist.*, 393 U.S. 503, 603 (1969).

shed their “legitimate expectations of privacy.”<sup>11</sup> COPPA privacy protections and parental rights extend to school environments, and these rights and protections should not be disregarded as soon as students walk through the school door.

*A. The FTC’s Current School Policy Under the COPPA Rule Infringes on Parents’ Rights to Protect Their Children’s Personal Information.*

Operators in schools must be required to comply with parents’ rights to protect their children’s personal information granted by the Act. Under COPPA, operators are required to provide notice to parents on the collection of information of their children, how the information is being used, and the operator’s disclosure practices.<sup>12</sup> More importantly, operators are required “to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.”<sup>13</sup> Parents have the right to review their child’s personal information collected by operators, the right to revoke their consent and terminate the future use and collection of their child’s information by operators, and the right to request that operators delete their child’s personal information.<sup>14</sup> Operators must comply with these parent requests.

The FTC’s current policy on COPPA in schools should be eliminated because it conflicts with the Act’s requirement to obtain “verifiable parental consent.” In 2015, the FTC revised guidance on its *Complying with COPPA: Frequently Asked Questions* (“FTC FAQ”) website for how schools can maintain compliance with COPPA through best practices.<sup>15</sup> FTC FAQ M.1. recommends that “schools may act as the parent’s agent and can consent to the collection of kid’s information on the parent’s behalf” as long as the consent is limited to the “educational

---

<sup>11</sup> *New Jersey v. T.L.O.*, 469 U.S. 325, 326 (1985).

<sup>12</sup> Children’s Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

<sup>13</sup> 15 U.S.C. § 6502(b)(1)(A)(ii).

<sup>14</sup> 15 U.S.C. § 6502(b)(3); Children’s Online Privacy Protection Rule, 16 C.F.R. § 312.6 (2019).

<sup>15</sup> FTC, *Complying with COPPA Frequently Asked Questions; M. COPPA and Schools*, <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools> (last updated Mar. 20, 2015).

context.”<sup>16</sup> “Education context” is briefly described in the FTC FAQ as “where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose.”<sup>17</sup> Operators are then allowed to “presume that the school’s authorization is based on the school’s [sic] having obtained the parent’s consent,”<sup>18</sup> when many times no parental consent or notice has been given.<sup>19</sup> This FTC guidance is in direct conflict with the explicit language of the Act which requires “verifiable parental consent.”<sup>20</sup>

Schools that use EdTech products in the classroom are failing to obtain verifiable consent from parents, and further failing to notify parents when they have provided consent to operators on their behalf.<sup>21</sup> When a single school district may use between “200 to 600 [software] applications, . . . screening every classroom tool can be difficult.”<sup>22</sup> Even outside the classroom, a recent study has shown that children’s application operators fall short of obtaining verifiable parental consent.<sup>23</sup> The FTC should not recommend that schools act as agents for parents because it circumvents the Act’s requirement of *verifiable* parental consent. Additionally, data

---

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> See *Spying on Students: School-Issued Devices on Student Privacy*, ELEC. FRONTIER FOUNDATION 1, 10–11 (April 13, 2017), <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf>.

<sup>20</sup> 15 U.S.C. § 6502(b)(1)(A)(ii); see also Comments of the Nat’l School Boards Ass’n, *Children’s Online Privacy Protection Act Rule Review*, Project No. P195404 (Oct. 23, 2019),

<https://www.regulations.gov/contentStreamer?documentId=FTC-2019-0054-0280&attachmentNumber=1&contentType=pdf> (stating that there is “no basis in statute or regulations permitting” schools to obtain verifiable parental consent on parents’ behalf).

<sup>21</sup> *Spying on Students: School-Issued Devices on Student Privacy*, ELEC. FRONTIER FOUNDATION 1, 10–11 (April 13, 2017), <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf> (reporting survey findings from school districts in forty-five states and finding that “[t]he notice and disclosure process is broken. Parents who responded to the survey were overwhelmingly not notified when schools started using new softwares [sic] and devices, created email accounts for students, or posted pictures on school or teacher social media pages.”).

<sup>22</sup> Heather Kelly, *School apps track students from classrooms to bathroom, and parents are struggling to keep up*, WASH. POST BLOGS (Oct. 29, 2019), <https://www.washingtonpost.com/technology/2019/10/29/school-apps-track-students-classroom-bathroom-parents-are-struggling-keep-up/?arc404=true>.

<sup>23</sup> See Irwin Reyes, et al., “*Won’t Somebody Think of the Children?*”: *Examining COPPA Compliance at Scale*, 2018(3) PROCEEDINGS ON PRIVACY ENHANCING TECHS. 63, 69 (2018), <https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf> (“That the [automated simulator] was able to trigger [geolocation information] functionality with random taps and swipes implies that verifiable parental consent is not being obtained.”).

show that schools frequently do not obtain verifiable parental consent when required. As such, operators should not be allowed a presumption that schools have obtained consent from parents to collect and use children’s personal information because in practice schools frequently fail to obtain consent from parents.

*B. The FTC’s Current School Policy Under the COPPA Rule Violates the Congressional Goals of the Act.*

The FTC’s current school policy on COPPA in schools ignores parental involvement and their legitimate concerns to safeguard their children’s personal information online, which align with Congress’ intent of the Act. Congress passed COPPA:

(1) to enhance parental involvement in a child’s online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora . . . in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children’s privacy by limiting the collection of personal information from children without parental consent.<sup>24</sup>

EPIC recognizes the benefit of innovation and technology in education and “to accomplish these goals in a manner that preserves the interactivity of children’s experience on the Internet and preserves children’s access to information in this rich and valuable medium.”<sup>25</sup> Because innovation and children’s data privacy in education are not mutually exclusive, EPIC encourages operators in the EdTech space to engage in privacy by design principles, to use data privacy and protection best practices, and to promote parental rights of children’s privacy under the COPPA Rule.<sup>26</sup>

---

<sup>24</sup> 144 Cong. Rec. S12741-04 (statement of Sen. Bryan).

<sup>25</sup> *Id.*

<sup>26</sup> See *EPIC Letter to U.S. House Committee on Oversight & Government Reform* (Sept. 25, 2017), <https://epic.org/testimony/congress/EPIC-HOGR-CEBP-Sep2017.pdf>; Comments of EPIC, *Request for Information: National Privacy Research Strategy* (Oct. 17, 2014), <https://epic.org/apa/comments/EPIC-NITRD-Privacy-Research-Strategy.pdf>; EPIC, *Why is P3P Not a PET?* (Nov. 12, 2002), <https://www.epic.org/reports/p3pnotpet.pdf>.

ClassDojo, an EdTech application used by teachers to monitor child behavior in the classroom, raises both data privacy and child development concerns. The application is used by teachers to award children who behave well in class with positive points and children who misbehave with negative points. Teachers can directly message parents to share classroom “moments” and update them on their child’s progress and classroom behavior. Two in three schools in the United States use ClassDojo every day.<sup>27</sup> The ClassDojo application does not require children’s personal information to function; however, teachers often input student personal information.<sup>28</sup> The company subsequently shares children’s personal information, including behavioral data, photos, and videos, with thirty-one other organizations, each with its own privacy policy.<sup>29</sup> Further, concerns are raised that ClassDojo “contributes to a practice where children are increasingly being monitored and tracked around the clock, which may impact . . . their development and experience of childhood.”<sup>30</sup>

These legitimate parental concerns on child data collection in schools fall squarely within the scope of their rights under the Act and align with Congress’ original goals to “enhance parental involvement.” The FTC’s current policy ignores parent’s COPPA rights in a school-setting, and should address this gap in the COPPA Rule revision.<sup>31</sup> Instead of putting the burden on schools to obtain and provide consent on behalf of parents, which they are unauthorized to do

---

<sup>27</sup> CLASSDOJO, INC., <https://www.classdojo.com/about-old/> (last visited Nov. 12, 2019).

<sup>28</sup> *Who knows all about me?*, CHILD.’S COMM’R 1, 9 (Nov. 2018), <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf>.

<sup>29</sup> *Id.*; Mark Bridge, *ClassDojo is harvesting data on how British schoolchildren behave*, TIMES (April 28, 2018), <https://www.thetimes.co.uk/article/classdojo-is-harvesting-data-on-how-british-schoolchildren-behave-0nbc2qjh>.

<sup>30</sup> *Who knows all about me?*, CHILD.’S COMM’R 1, 9 (Nov. 2018), <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf>; *see also Spying on Students: School-Issued Devices on Student Privacy*, ELEC. FRONTIER FOUNDATION 1, 14 (April 13, 2017), <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf> (raising parental concerns that EdTech companies “are collecting and storing data to be used against [children] in the future, creating a profile before [they] can intellectually understand the consequences of [their] searches and digital behavior.”).

<sup>31</sup> *See* 144 Cong. Rec. S12741-04 (statement of Sen. Bryan).



under the Act, the burden should be shifted to operators, who are in a better position to do so given advancements in technology and greater availability of resources, to obtain verifiable parental consent.

*C. COPPA Should Not Have a “School Official Exception” like FERPA, and the FTC Should Revise Its Current COPPA School Policy*

The Commission should not use FERPA’s “school official exception” as a model for the COPPA Rule. Under FERPA’s “school official exception,” educational institutions “may disclose personally identifiable information . . . of a student without consent” so long as the disclosure is made to another school official determined to have “legitimate educational interests.”<sup>32</sup> However, the definition of “school official” under the ED’s regulation is exceedingly broad. The regulation extends the meaning of “school official” to include contractors and consultants to which schools have “outsourced institutional services or functions.”<sup>33</sup> This is then used by schools to designate operators as school officials, when in reality doing so is inappropriate and results in greater impropriety when combined with FERPA’s “directory information exception.”

EdTech providers use the “school official exception” and the “directory information exception” to take advantage of under-staffed and unsophisticated school districts. Directory information typically includes “name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance.”<sup>34</sup> Some schools have gone so far as to designate height and weight of school athletes and student ID as

---

<sup>32</sup> 34 C.F.R. 99.31(a)(1)(i)(A)(2019).

<sup>33</sup> 34 C.F.R. 99.31(a)(1)(i)(A).

<sup>34</sup> U.S. DEP’T OF EDUC., *Frequently Asked Questions; What is Directory Information?*, <https://www2.ed.gov/policy/gen/guid/fpco/faq.html#q4> (last visited Nov. 13, 2019).

directory information.<sup>35</sup> Legal consultants even recommend EdTech operators include specific language in contracts with schools that allow them “to use de-identified data, metadata or data that is shared under ‘directory information’ exception for its own purposes, including to share with third parties.”<sup>36</sup> These consultants also note the imbalance in bargaining power between schools and EdTech providers by telling EdTech companies that “[m]any schools are understaffed and lack legal counsel, and School representatives look to the Service Provider to confirm compliance with FERPA, COPPA, and state laws.”<sup>37</sup>

EPIC does not support any similarly constructed “school official” or “directory information” exceptions under the COPPA Rule that would create such a loophole for operators to collect information on children without parental involvement and consent. An example of this kind of improper collection of children’s data is exhibited in Google’s G Suite for Education platform which has over ninety million student and teacher users worldwide.<sup>38</sup> Google requires schools to agree to their *G Suite for Education (Online) Agreement* which designates themselves, Google, as a “school official” under FERPA.<sup>39</sup> When combined with FERPA’s “directory information” exception, operators like Google can collect enormous amounts of personal information on students without parental consent, which is a violation of COPPA.<sup>40</sup>

---

<sup>35</sup> Pam Dixon, *Student Privacy 101: Why school directory information sharing is a major privacy issue*, WORLD PRIVACY FORUM (updated April 17, 2015), <https://www.worldprivacyforum.org/2015/08/student-privacy-101-why-directory-information-and-ferpa-is-a-major-edu-privacy-issue/>.

<sup>36</sup> Emily S. Tabatabai, *Student Privacy Boot Camp for EdTech Companies: COPPA and FERPA*, ORRICK 1, 22 (2016), <https://fpf.org/wp-content/uploads/2016/03/COPPA-and-FERPA-Compliance-for-Companies-in-the-EdTech-Industry.pdf>.

<sup>37</sup> *Id.*

<sup>38</sup> *Google for Education*, GOOGLE, INC. 1 [http://services.google.com/fh/files/misc/google\\_for\\_education-shareable\\_devices\\_and\\_collaborative\\_tools.pdf](http://services.google.com/fh/files/misc/google_for_education-shareable_devices_and_collaborative_tools.pdf) (last visited Nov. 13, 2019).

<sup>39</sup> *G Suite for Education (Online) Agreement*, GOOGLE, INC. (Sept. 2018), [https://gsuite.google.com/terms/education\\_terms.html](https://gsuite.google.com/terms/education_terms.html) (“7.4 FERPA. The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA (“FERPA Records”); and (b) to the extent that Customer Data includes FERPA Records, Google will be considered a “School Official” (as that term is used in FERPA and its implementing regulations) and will comply with FERPA.”).

<sup>40</sup> 34 C.F.R. §§ 99.31(a)(11), 99.37.

*D. Commercial Purpose Includes Operators Who Sell Products and Services to Schools; Children’s Personal Information Should Not Be Collected by Operators for Product Improvement.*

The Commission should define “commercial purpose.” COPPA applies to commercial operators of online websites and services; however, neither the Act nor the COPPA Rule describes in detail what constitutes a “commercial purpose.” Operators who design products and services to be used in schools do so for commercial purposes—to sell to schools to make money. EdTech products, like Google’s G Suite for Education, should not automatically get a noncommercial designation simply because they are used in a public school environment. Just because an online product or service is educational in nature does not also automatically designate it as noncommercial.

In the FTC’s COPPA Rule revision, the commercial definition should also apply to operator product improvement. The Commission requests comment on whether operators should be allowed “to use the personal information collected from children to improve the product?”<sup>41</sup> All products used in school environments subject to COPPA are inherently commercial in nature, otherwise COPPA would not apply. While some personal information may need to be collected by operators to troubleshoot certain technical issues, personal information should not be collected by operators for product improvement. Allowing such a change to the COPPA rule would allow EdTech operators the ability to create virtual laboratories in schools to study child behavior and further develop commercial products for profit, unbeknownst to parents. Short of troubleshooting technical issues, no personal information should be collected to improve operator products, whether in or out of a school setting, without verifiable parental consent.

---

<sup>41</sup> FTC, *Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule*, 84 Fed. Reg. 35,842, 35,845 (proposed July 25, 2019) (to be codified at 16 C.F.R. pt. 312), <https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online>.

*E. The COPPA Rule Revision Should Require Operator Data Breach Notification*

The FTC should revise COPPA to require all operators to notify parents of data breaches within forty-eight hours. EdTech provides a unique environment in which bad actors can illegally obtain children’s personal information. Since January 2016 over 700 cyber incidents have occurred in schools.<sup>42</sup> In 2018, the Federal Bureau of Investigations (“FBI”) released a public service announcement explaining that EdTech “data collection and unsecured systems could pose risks to students” such as “malicious use of . . . sensitive data . . . result[ing] in social engineering, bullying, tracking, identity theft, or other means for targeting children.”<sup>43</sup> As part of their announcement, the FBI also directed parents to research COPPA, which applies to EdTech. Similar to our recommendation during the FTC’s 2013 COPPA Rule Revision, in order to strengthen COPPA and help protect children from these serious security and privacy concerns, the Commission should revise the COPPA Rule to require operators to notify parents of all data breaches involving children’s personal data within forty-eight hours of an event so that they may respond accordingly.<sup>44</sup>

### **III. Conclusion**

The current COPPA Rule is effective at protecting children’s personal information online, even with recent advancements in technology and new business practices. Nonetheless, the Commission can do more to protect children’s data privacy in schools. COPPA requires verifiable parental consent. Operators should not be allowed to presume schools have obtained

---

<sup>42</sup> *The K-12 Cyber Incident Map*, EDTECH STRATEGIES, LLC, <https://k12cybersecure.com/map/> (last updated Nov. 10, 2019).

<sup>43</sup> FED. BUREAU OF INVESTIGATION, *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students*, Alert No. I-091318-PSA (Sept. 13, 2018), <https://www.ic3.gov/media/2018/180913.aspx>.

<sup>44</sup> See Comments of EPIC, *Children's Online Privacy Protection Act Rule Review*, Project No. P104503 (Sept. 24, 2012), <https://epic.org/privacy/kids/EPIC-COPPA-2012-Rule-Rev-Cmts.pdf>; Comments of EPIC, *Children's Online Privacy Protection Act Rule Review*, Project No. P104503 (Dec. 23, 2011), <https://epic.org/privacy/kids/EPIC-COPPA-Rule-Comments-FINAL-12-23-11.pdf>.

verifiable parental consent when data shows that schools frequently fail to obtain it and fail to notify parents of EdTech products used in the classroom. Parents have legitimate data privacy and childhood development concerns when it comes to the collection of their children’s data in an education environment. The FTC’s current COPPA policy ignores these concerns, as well as parents’ rights under the Act.

In the COPPA Rule revision, the Commission should not create a “school official exception” similar to FERPA because it allows operators to designate themselves as schools officials, and when combined with the “directory information exception” it creates a loophole for operators to collect children’s personal information without parental involvement or consent. The Commission must also define what constitutes a “commercial purpose” and ensure that children’s personal information collected in schools is not used for EdTech product improvement purposes. Finally, the FTC should heed FBI warnings on the risks involved in student data collection by requiring all operators to notify parents of a data breach within forty-eight hours.

Sincerely,

/s/ Marc Rotenberg  
Marc Rotenberg  
EPIC President

/s/ Christine Bannan  
Christine Bannan  
EPIC Consumer Protection Counsel

/s/ W. Hunter Daley  
W. Hunter Daley  
EPIC Law Clerk