American University Business Law Review

Volume 9 | Issue 3 Article 4

2020

Big Tech Makes Big Data Out of Your Child: The FERPA Loophole EdTech Exploits to Monetize Student Data

Amy Rhoades
American University Washington College of Law, ar3628a@student.american.edu

BIG TECH MAKES BIG DATA OUT OF YOUR CHILD: THE FERPA LOOPHOLE EDTECH EXPLOITS TO MONETIZE STUDENT DATA

AMY RHOADES*

* Senior Staff Member, *American University Business Law Review*, Volume 9; J.D. Candidate, 2022, American University Washington College of Law; B.A., International & Comparative Politics, George Mason University. The author would like to express gratitude to the Honorable Dale Durrer, Eli Sulkin, and the *American University Business Law Review*'s staff for their time, effort, and assistance in preparing this Comment, and a sincere appreciation for her family's support and encouragement.

I. INTRODUCTION

The high cost of education and decreasing academic performance presented an opportunity for the education technology industry ("EdTech"), with a worldwide market exceeding $250 billion annually, to attract large investment and development in the United States.[1] Promising cost savings and productivity efficiency, EdTech companies offer educators big data analysis by collecting and providing access to student information, assessment results, and business intelligence tools.[2] As a result of the influx in datafication of students, the educational market is the third-highest target for data hackers, behind only the health and financial sectors.[3] Data breaches of education records place student safety at risk, ranging from immediate threats of danger and cyberbullying, to long-term risks of identity theft.[4]

1. *See* Jake Williams, *U.S. EdTech Market Is Biggest Globally, Reports Says*, EDSCOOP (Feb. 13, 2020), https://edscoop.com/u-s-edtech-market-biggest-globally-report-says/ (reporting worldwide EdTech market value is projected to reach $252 billion in 2020 with the United States, home to forty-three percent of EdTech companies, leading the world in EdTech venture capital funding); *see also* Mike Montgomery, *Edtech: The Savior Our Schools Need Should Be a Startup Gold Mine*, FORBES (May 7, 2019, 6:03 PM), https://www.forbes.com/sites/mikemontgomery/2019/05/07/edtech-the-savior-our-schools-need-should-be-a-startup-gold-mine/#337a1b9799c0 (arguing the need for clear standards and goals when implementing technology to effectively impact learning; mere presence of technology is not enough).

2. *See* OMIDYAR NETWORK, SCALING ACCESS AND IMPACT: REALIZING THE POWER OF EDTECH 4 (2019) (suggesting educational models integrating technology can be impactful and cost-effective); U.S. DEP'T OF EDUC., REIMAGINING THE ROLE OF TECHNOLOGY IN EDUCATION: 2017 NATIONAL EDUCATION TECHNOLOGY PLAN UPDATE 55 (2017) (describing how EdTech provides diverse data sets to create a more complete picture and provide feedback and personalized learning strategies). *But see* SOPHIE SHANK, ABDUL LATIF JAMEEL POVERTY ACTION LAB, WILL TECHNOLOGY TRANSFORM EDUCATION FOR THE BETTER? 9 (2019) (cautioning that the effectiveness of technology on education outcomes varies depending on the implementation strategy).

3. Meghan Bogardus Cortez, *Education Sector Data Breaches Skyrocket in 2017*, EDTECH MAG. (Dec. 1, 2017), https://edtechmagazine.com/higher/article/2017/12/education-sector-data-breaches-skyrocket-2017 (showing a 103% increase in education data breaches in the first half of 2017).

4. *See id.* (noting that seventy-four percent of data breaches in higher education were caused by outsiders with malicious intentions).

High investigation costs and ransomware payments also present financial consequences for students.[5]

With the increase of technology use in schools, parents, students, and privacy advocates have growing concerns that current regulation is inadequate to meet the rapidly advancing technology EdTech companies employ.[6] Commercial companies must abide by the Children's Online Privacy Protection Act ("COPPA"), which regulates online operators' collection and use of children's personally identifiable information ("PII").[7] However, the Federal Trade Commission ("FTC"), the enforcement agency overseeing COPPA, issued an exception for data disclosed by schools to online operators acting as authorized educational partners.[8] The FTC maintains that student PII disclosed as an education record is regulated by the Family Educational Right and Privacy Act ("FERPA").[9] The legislation's overly broad definition of education records, combined with the 2011 Amendments expanding FERPA to permit schools to disclose data to third parties, creates a loophole for the EdTech industry to avoid COPPA regulation regarding student data.[10] As a result, commercial companies can

5. *See* Bob Sullivan, *FBI Warns EdTech Needs Stronger Defenses for Students' Personal Data*, SECURITY INTELLIGENCE (Jan. 11, 2019), https://securityintelligence.com/fbi-warns-edtech-needs-stronger-defenses-for-students-personal-data/ (reporting that hackers used stolen student data to extort parents and schools).

6. *See* Sara Friedman, *Survey: More Teacher Training Needed for Ed Tech Tools*, JOURNAL (Oct. 14, 2019), https://thejournal.com/articles/2019/10/14/survey-more-teacher-training-needed-for-ed-tech-tools.aspx (attributing increased use of classroom technology to schools replacing aging technology with cloud-based solutions and integrated learning experiences).

7. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (2018).

8. 16 C.F.R. § 312.3 (2020); *see also* Isaac Mamaysky, *The FTC Has Its Sights on COPPA, and Edtech Providers Should Take Notice*, EDSURGE (Oct. 8, 2019), https://www.edsurge.com/news/2019-10-08-the-ftc-has-its-sights-on-coppa-and-edtech-providers-should-take-notice ("[S]chools can currently consent as the parents' agent when websites collect information solely for the benefit of the students or the school and not for a commercial purpose.").

9. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N [hereinafter FED. TRADE COMM'N, *Complying with COPPA*], https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions (last visited Feb. 28, 2020) (follow "N. COPPA and Schools" hyperlink); *see* Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(b)(1)(F) (2018); *see also* JOEL REIDENBERG ET AL., FORDHAM LAW SCH. CTR. ON LAW & INFO. POLICY, PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 11 (2013) (explaining COPPA does not apply to data obtained directly from a school).

10. *See* 34 C.F.R. § 99.31(a)(1)(i)(B)(2) (2020) (permitting educational agencies to disclose student PII to contractors under direct control of the institution or providing services the institution would typically perform without the consent of students or parents); Henry Kronk, *Student Data Security Is at Risk. We Need to Update FERPA*,

quickly amass large amounts of data and potentially avoid the FTC's oversight of COPPA compliance by contracting directly with schools.[11] This practice runs afoul of legislative intent for both FERPA and COPPA, places student data at risk by creating a vacuum of oversight, and leaves little recourse for violations of data collection or use in the EdTech industry.[12]

This Comment argues that the EdTech industry is exploiting a loophole in federal regulations to grow the business sector by mining children's data online at the expense of student privacy. Part II provides background on current laws protecting student data, how the laws are applied to the EdTech industry, and how the acts are enforced. Part III analyzes the application of FERPA to the EdTech industry, finding the collection of PII incompatible with the education record standard, and arguing that the Department of Education ("ED") is ill-equipped to provide oversight or deterrence for commercial companies. Part IV presents solutions to increase security of student data. Part V concludes with a review of the growing imperative to address safety concerns of EdTech applications in schools and recaps how the regulation loopholes are increasing the risks to student privacy.

II. HOW EDTECH IS AMASSING STUDENT DATA IN THE UNITED STATES

Students, parents, and privacy advocates are raising concerns about data protection as an influx of capital in EdTech companies has led to more schools utilizing third-party commercial products such as cloud computing services, online applications, and data analytics tools.[13] As more commercial EdTech tools are integrated into the U.S. education system, schools struggle

---

ELEARNING INSIDE (Nov. 25, 2018), https://news.elearninginside.com/student-data-security-is-at-risk-we-need-to-update-ferpa/ (describing the loophole in FERPA regulation that permits schools to disclose student PII to EdTech companies without parental or student consent by considering the commercial entity an authorized school official).

11. *See* Natasha Singer, *How Google Took Over the Classroom*, N.Y. TIMES (May 13, 2017) [hereinafter Singer, *How Google Took Over*], https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html (showing that Google is amassing a substantial amount of user data on minors due to its use in more than half of primary and secondary schools).

12. *See* JODY FEDER, CONG. RESEARCH SERV., RS22341, THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA): A LEGAL OVERVIEW 6 (2013) (citing the need to revise data practices to increase transparency for students and parents, while closing current regulation loopholes).

13. *See* REIDENBERG ET AL., *supra* note 9, at 1–2 (finding parents have rising concerns with third-party cloud data collection); *see also* John Rogers, *Education Is the New Healthcare, and Other Trends Shaping Edtech Investing*, EDSURGE (Feb. 28, 2020), https://www.edsurge.com/news/2020-02-28-education-is-the-new-healthcare-and-other-trends-shaping-edtech-investing (predicting an increase in privacy concerns as a result of accelerated capital investments in EdTech).

to enforce student data protection due to intersecting federal regulations, COPPA, and FERPA, enforced through multiple agencies.[14]

a. Federal Regulations of Student Data Collection Practices

In 1974, Congress enacted FERPA to regulate schools' practice of releasing student information, and mandate a degree of parental oversight and transparency.[15] After the innovation of the internet and adoption of online services, Congress enacted COPPA to regulate business practices for collecting data from children online.[16] Today, FERPA governs the disclosure and use of student data from schools, and COPPA regulates collection and use of children's PII by online operators.[17] As a commercial industry conducting business with schools, EdTech operates within a cross-section of COPPA and FERPA.[18]

i. Overview of Family Educational Rights and Privacy Act

FERPA protects students' PII by regulating school policies involving disclosure of student information and requiring parental transparency regarding education records.[19] However, not all school records fall within FERPA regulation. To be considered a confidential FERPA record, the material must be directly related to a student and be maintained by the

14. *See* FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9 (describing how schools must consider obligations under FERPA, COPPA, and potentially state student privacy laws when disclosing information to online operators).

15. *See FERPA and Access to Public Records*, STUDENT PRESS L. CTR. (May 6, 2005), https://splc.org/2005/05/ferpa-and-access-to-public-records/ (describing FERPA co-author Sen. James Buckley's driving concerns behind presenting the legislation as the lack of both parental access to student records and consistency in schools' policies governing disclosure of student records); *see also* Zach Greenberg, *Let Ferpa Be Ferpa*, CHRON. HIGHER EDUC. (Jan. 14, 2018), https://www.chronicle.com/article/Let-Ferpa-Be-Ferpa/242232 (quoting Sen. James Buckley) (stating the reason for FERPA was "to protect the rights of students and their parents and to prevent the abuse of personal files and data in the area of federally assisted educational activities").

16. *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (2018); *see also* FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9 (stating the main purpose of COPPA under sub-header A "General Questions about the COPPA Rule").

17. 15 U.S.C. § 6502; Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232(a) (2018).

18. *See Student Privacy and Ed Tech*, FED. TRADE COMM'N, [hereinafter FED. TRADE COMM'N, *Student Privacy*] https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech (last visited Oct. 10, 2020) (focusing on how the rising integration of EdTech applications is causing schools to evaluate the intersection of FERPA and COPPA regulations).

19. 20 U.S.C. § 1232(g); 34 C.F.R. § 99.3 (2020).

school.[20] While FERPA does not define the direct link requirement for education records, schools can conduct a case-by-case analysis by applying guidelines from the ED.[21] When evaluating photos or videos containing students, the ED considers factors such as the activity depicted, the intended uses by the educational institution, and whether the image contains PII otherwise found in the student's record.[22] The ED further states that student images incidentally captured, as in the background of a photo, are not considered directly linked to a student.[23]

To be considered an education record under FERPA, the document or file must be maintained by the school or an agent of the school.[24] In *Owasso Independent School District v. Falco*,[25] the U.S. Supreme Court reasoned that FERPA's language implies schools are required to demonstrate a temperament of permanency or intent to retain a file for a student record to be considered maintained.[26] The Court held that peer-graded quizzes were not education records under FERPA because the grade was maintained by students rather than an institution.[27] Similarly, a federal court ruled in *S.A. v. Tulane County Office of Education*[28] that e-mails stored on individual teachers' hard drives are not education records until the document is centrally located.[29] Therefore, data collected online may be covered under

20. 20 U.S.C. § 1232g(a)(4)(A) ("'[E]ducation records' means . . . records, files, documents, and other materials which — (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution."). *But see What Records Are Exempted from FERPA?*, U.S. DEP'T OF EDUC., https://studentprivacy.ed.gov/faq/what-records-are-exempted-ferpa (last visited Aug. 16, 2020) (noting exceptions to education records, including personal observations).

21. *See FAQs on Photos and Videos under FERPA*, U.S. DEP'T OF EDUC., [hereinafter FAQS ON PHOTOS] https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa (last visited Aug. 16, 2020) (listing factors to consider when evaluating whether a photo or video is directly linked to a student).

22. *Id*.

23. *See id*. (hypothesizing that a photo capturing basketball players and spectators in the background is only directly linked to focused players; the image is not directly linked to students portrayed in the background); *see also* STUDENT PRESS L. CTR., *supra* note 15 (suggesting the FERPA authors did not intend for the law "to apply to documents that only tangentially refer to students" or do not influence school decision-making about students).

24. 20 U.S.C. § 1232g(a)(4)(A)(ii).

25. 534 U.S. 426 (2002).

26. *See id.* at 432–33.

27. *Id.*

28. No. CV F 08–1215 LJO GSA, 2009 U.S. Dist. LEXIS 93170 (E.D. Cal. Oct. 5, 2009).

29. *See id.* at *10 (reasoning that Congress did not "contemplate that educational records are maintained in numerous places," when enacting FERPA, but instead intended

FERPA if the information is maintained by the school, but the same information exchanged via an email or messaging application not maintained by the school is not covered.[30]

FERPA grants parents access and some control over education records, such as the right to inspect and the ability to amend inaccurate or misleading information.[31] Additionally, FERPA requires schools to obtain written parental consent prior to releasing non-directory student information.[32] However, FERPA permits exceptions to the parental consent requirement if schools are releasing records to officials for educational purposes, to accrediting organizations, to parties in connection with financial aid, or to organizations conducting studies on behalf of the school.[33] In 2011, the ED further revised FERPA guidelines to authorize schools to disclose student PII to third-party companies if the company is a designated school official.[34] The exception does not create privacy standards for the commercial companies; the law simply mandates that officials comply with the individual school's student data policy.[35]

The ED enforces FERPA; as a result, there are limited remedies for violations.[36] Schools in violation of FERPA may lose federal funding or become ineligible for future funding.[37] However, this remedy has never been used.[38] Students are unable to pursue private claims of action for FERPA violations because the statute failed to create any individual rights for

---

'maintain' to mean records kept in a single secure permanent storage space).

30. *Id.* at *11–12 (holding that emails are temporary and are only education records if printed and placed in a student file).

31. 20 U.S.C. § 1232g(a), (b); *see Family Educational Rights and Privacy Act (FERPA)*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/student/ferpa/ (last visited Aug. 10, 2020) (discussing the importance of parents' ability to access student information in order to protect their children's interests as a driving concern for proposing FERPA).

32. 20 U.S.C. § 1232g(b)(1) (requiring parental consent for schools to release education records or PII).

33. *Id.*; 34 C.F.R. § 99.31(a) (2020).

34. 34 C.F.R. § 99.31(a)(6) (granting schools the right to disclose student records to third parties providing services otherwise performed by the school, if under direct control of the school and subject to FERPA rules).

35. *See id.* § 99.31(a)(1)(i)(B)(3)(ii).

36. *See id.* § 99.67(a) (listing the remedies for FERPA violations as withholding federal funding, compelling compliance by cease and desist orders, or ending funding eligibility).

37. *Id.*

38. *See Student Privacy, FERPA, and Its Weakening by the US Department of Education*, PARENT COAL. STUDENT PRIVACY [hereinafter PARENT COAL.], https://www.studentprivacymatters.org/ferpa-changes/ (last visited on Aug. 16, 2020).

enforcement.[39] If a student believes his FERPA rights were violated, he can file a complaint with the ED.[40] The ED reviews each complaint on a case-by-case basis to determine if a school violated disclosure of student PII.[41] The ED may determine a school did not violate FERPA if the disclosed information falls outside of the Act's regulation, such as data that does not meet the requirements of education records.[42]

ii. History of Children's Online Privacy Protection Act

In 1998, Congress passed COPPA to govern the collection of children's PII from online operators.[43] The law specifies business responsibilities when collecting and using children's PII online.[44] A core element of the law, COPPA requires online operators to provide notice and receive parental consent prior to collecting PII from children under the age of thirteen.[45]

When first enacted, COPPA focused on PII used to contact a child, such as name, address, and phone number.[46] In 2012, the FTC amended COPPA regulations to include persistent identifiers, such as cookies or fingerprints;

39. *See* Gonzaga Univ. v. Doe, 536 U.S. 273, 288–89 (2002) (ruling an individual cannot sue to enforce FERPA); *see also* Tarka v. Franklin, 891 F.2d 102, 104 (5th Cir. 1989) (noting there is no language in FERPA indicating congressional intent for a private right of action); Smith v. Duquesne Univ., 612 F. Supp 72, 80 (W.D. Pa. 1985) (holding there is no private remedy for FERPA violations because the underlying purpose was to stop careless policies of releasing records, not ensuring student individual privacy).

40. 34 C.F.R. § 99.63 (instructing eligible individuals to file FERPA complaints with the ED); *see* 20 U.S.C. § 1232(f) (2018) (requiring the ED to establish an office "to investigate, process, review, and adjudicate" all violations of FERPA).

41. *See* 34 U.S.C. § 99.64 (describing how FERPA complaints are individually investigated); FAQS ON PHOTOS, *supra* note 21 (confirming the need for case-by-case analysis for evaluating potential education records such as photographs and video recordings).

42. *See, e.g.*, Owasso Indep. Sch. Dist. No. I–011 v. Falvo, 534 U.S. 426, 432–33 (2002) (holding peer-graded papers are not education records because schools do not maintain them).

43. *See* 15 U.S.C. §§ 6501–6506 (2018); *see also* Laurel Jamtgaard, *Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act*, 16 SANTA CLARA COMPUTER HIGH TECH. L.J. 385, 387 (2000) (summarizing COPPA's enactment as a response to concerns regarding online collection of children's data without parental consent).

44. 15 U.S.C. § 6502(b)(1)(A) (regulating when website operators can collect a child's personal information); *see also* INTERACTIVE ADVERT. BUREAU, GUIDE TO NAVIGATING COPPA: RECOMMENDATIONS FOR COMPLIANCE IN AN INCREASINGLY REGULATED CHILDREN'S MEDIA ENVIRONMENT 2 (2019), https://www.iab.com/wp-content/uploads/2019/10/IAB_2019-10-09_Navigating-COPPA-Guide.pdf (summarizing COPPA's parameters and defining identifiers regulated by the law).

45. 15 U.S.C. § 6502(b)(1)(A).

46. *See* Act of Oct. 21, 1998, Pub. L. No. 105-277, § 1303, 112 Stat. 2681 (1998); 15 U.S.C. § 6501(8).

IP address and geolocation; and a range of media files now prevalent online such as photos and video recordings.[47] Online services that target children are required to comply with COPPA regulations, regardless of the device used to access the service.[48]

Under the statute, the FTC enforces COPPA compliance.[49] Online operators who fail to comply with COPPA regulations may face civil penalties of up to $43,280 per violation.[50] The FTC can also require a company to change business practices as a remedy for a COPPA violation.[51] Currently, the FTC only investigates COPPA compliance by businesses; the FTC excludes schools from COPPA enforcement, stating that FERPA regulates the enforcement of school data disclosure.[52]

b. The Information EdTech Is Collecting on Students

EdTech businesses offer schools access to big data, which can drive learning initiatives for students as well as financial decision making for administrators.[53] A prime example of EdTech's presence is Google's integration into public schools: in 2017, more than half of K-12 students used Google's education apps, and Google Chromebooks accounted for more than fifty percent of mobile devices in schools.[54] Similarly, EdTech

47. 16 C.F.R. § 312.2 (2020); *see also* FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9.

48. *See* INTERACTIVE ADVERT. BUREAU, *supra* note 44, at 2 (explaining COPPA applies to all online services, including shared devices).

49. 15 U.S.C. § 6502(c); 16 C.F.R. § 312.9 (stating violations of COPPA will be enforced by the FTC).

50. FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9 (outlining the penalties for violating COPPA); *see also* Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (reporting the record settlement Google will pay the FTC and New York for violating COPPA rule).

51. *See, e.g.*, Press Release, Fed. Trade Comm'n, TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program (Nov. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its (describing that settlement requirements include prohibiting misrepresentations about TRUSTe practices in messaging).

52. *See* 20 U.S.C. § 1232g(f) (2018); FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9 (noting school operators need to consider FERPA regulations, adding that compliance is administered by the ED).

53. *See* Benjamin Herold, *How (and Why) Ed-Tech Companies Are Tracking Students' Feelings*, EDUC. WK. (June 12, 2018), https://www.edweek.org/ew/articles/2018/06/12/how-and-why-ed-tech-companies-are-tracking.html (describing how data analytics are driving adaptive learning, developing personalized programs to identify knowledge gaps, and increasing efficacy).

54. *See* FRIDA ALIM ET AL., ELEC. FRONTIER FOUND., SPYING ON STUDENTS:

company ClassDojo claims that more than ninety-five percent of U.S. K-8 schools are actively using its application.[55] Many EdTech applications provide big data insights driven by student's PII, including behavioral data, such as tracking student actions and engagement with others.[56]

There is a wide range of data collected by EdTech applications.[57] Direct data is voluntarily entered or transferred from schools to EdTech companies, such as account information submitted to create a user profile within the application.[58] Examples of direct information include student names, student IDs, contact information, or grades.[59] Direct information can be supplied by schools, teachers, parents, or student users.[60] When using online applications for educational activities, a potential pitfall for schools is students' tendency to share PII.[61] A 2013 study found that teens under the age of eighteen exhibit a high likelihood of revealing PII online, and that teens are more likely to share information about themselves online than in the past.[62] The study also found that only nine percent of teens had "a high level of concern about third-party access to their data."[63]

Beyond direct data, EdTech companies collect indirect or trace data.[64] Indirect data is information collected in the application itself, such as

SCHOOL-ISSUED DEVICES AND STUDENT PRIVACY 5 (2017) (detailing the heavy use of school-issued devices for K–12 students).

55. *Press*, CLASSDOJO, https://www.classdojo.com/press/ (last visited Aug. 16, 2020) (describing the prevalent use of ClassDojo by teachers to share photographs and videos of students, creating a communication hub for teachers, students, and parents).

56. *See* ALIM ET AL., *supra* note 54, at 7–8 (stating the ED is encouraging schools to adopt the use of big data from EdTech applications to improve assessments of learning objectives and educational innovation).

57. *See* CHILDREN'S COMM'R, WHO KNOWS WHAT ABOUT ME? 5–8 (2018), https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2018/11/Childrens-commissioner-Who-Knows-What-About-Me-i-internet-matters.pdf (explaining the types of children data being collected online).

58. *See id.* at 6 (describing the "direct data" collected on students).

59. *Id.*

60. *See id.* at 5–6 (providing examples of "direct data" that schools provide to EdTech companies).

61. *See* Perry Drake, *Is Your Use of Social Media FERPA Compliant?*, EDUCAUSE REV. (Feb. 24, 2014), https://er.educause.edu/articles/2014/2/is-your-use-of-social-media-ferpa-compliant (imagining various scenarios of data sharing online).

62. *See* Mary Madden et al., *Teens, Social Media, and Privacy*, PEW RES. CTR. (May 21, 2013), https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/ (finding that ninety-one percent of teens report posting photos of themselves, ninety-two percent share their name online, eighty-two percent share their birth date, and seventy-one percent reveal the town or city they live in).

63. *Id.*

64. *See* CHILDREN'S COMM'R, *supra* note 57, at 6 (explaining the types of child data collected online includes "inferred" data and "data that is 'given off'").

metadata, geolocation, IP address, and browser data.[65] The programs capture user interactions within the application and automatically upload the data.[66] For example, Summit Learning's platform collects geolocations, IP addresses, and browsing behaviors.[67] Many companies are working on applications to capture students' eye movements to measure engagement, whether through sensors in classrooms or cameras on laptops.[68] The Paris School of Business is already utilizing laptop webcams to analyze student eye movements in its online program and alert students when interest decreases.[69]

Potentially the most valuable data within the EdTech industry is inferred data, which combines direct and indirect information to create predictive models based on algorithms.[70] By providing access to big data and applying predictive analytics, EdTech businesses capitalize on advancements in technology data-mining to present trends and patterns within student data.[71]

c. Safety Risks and Privacy Concerns for EdTech Data Collection

Schools generate a substantial amount of valuable data with more than fifty million students in public school each year, which can entice hackers to the EdTech industry's large collection of student data.[72] In September 2018, the Federal Bureau of Investigation ("FBI") issued a warning that the "rapid proliferation of education technologies in U.S. schools poses privacy and

---

65. *Id.*

66. *See, e.g.*, *Privacy Policy*, SUMMIT LEARNING, https://www.summitlearning.org/privacy-center/privacy-policy (last updated June 22, 2020) (clarifying that Summit Learning automatically collects certain types of visitor information).

67. *See id.*

68. *See* Erika Gimbel, *Biometric Tech Can Track How Well Students Are Paying Attention*, EDTECH MAG. (Feb. 23, 2018), https://edtechmagazine.com/k12/article/2018/02/biometric-technology-tracks-students-attention (describing the potential uses of biometric tracking in education and predicting they will emerge in U.S. classrooms by the year 2028).

69. *See id.* (describing the program Nestor, an application that uses AI-software to analyze students' eye movements in remote learning classes and generate alerts and create custom quizzes based on a student's attentiveness to the online program).

70. *See* CHILDREN'S COMM'R, *supra* note 57, at 6.

71. *See* Samuel Greengard, *How Predictive Analytics Will Improve Learning*, EDTECH MAG. (Oct. 31, 2006), https://edtechmagazine.com/k12/article/2006/10/how-predictive-analytics-will-improve-learning (predicting the increase and impact of predictive modeling in education); *see also* CHILDREN'S COMM'R, *supra* note 57, at 6, 9 (explaining that privacy policies for inferred data are often the least transparent, with many parents and students often lacking awareness of the data collected).

72. *See Back to School Statistics*, NAT'L CTR. FOR EDUC. STATS., https://nces.ed.gov/fastfacts/display.asp?id=372 (last visited Aug. 16, 2020) (reporting that 50.7 million students would attend public schools for the 2019–2020 school year).

safety risks for children."[73] Cybercriminals find the education sector an appealing target because it presents a large amount of data, collected in disparate, often ill-managed systems.[74] Parents and privacy advocates fear EdTech companies are further placing student data at risk due to the high concentration of data aggregation, lack of transparency on data collection, and poor security protocols.[75]

Moreover, studies show that schools are often unprepared to protect student data collected in EdTech applications.[76] Research conducted by the Fordham Center on Law and Information Policy ("Fordham CLIP") in 2013 suggested schools are not prepared to adequately address data governance or protection when data collection is outsourced to third-party services.[77] Ninety-five percent of school districts in the study utilized cloud computing solutions for data mining, but fewer than seven percent of the school contracts restricted companies' use of student data for marketing purposes.[78] The study also found many schools are ill-prepared to support FERPA regulations related to contracts with online operators.[79] Unsecured services lead to potential data breaches, which place students' safety at risk.[80]

---

73. Benjamin Herold, *FBI Raises Alarm on Ed Tech and Student Data Privacy, Security*, EDUC. WK. (Sept. 13, 2018, 11:18 AM) [hereinafter Herold, *FBI Raises Alarm on EdTech*], https://blogs.edweek.org/edweek/DigitalEducation/2018/09/fbi_raises_alarm_ed_tech_privacy.html; *see* Press Release, Fed. Bureau of Investigation, Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx (warning of malicious use of sensitive PII after uncovering two large data breaches resulting in public access to millions of students' data in 2017).

74. *See* Herold, *FBI Raises Alarm on EdTech*, *supra* note 73 (warning that school districts were being targeted and that "most data disclosures are caused by human error"); *see also* Cortez, *supra* note 3 (characterizing universities as a "juicy target" for hackers due to the large quantity of users).

75. *See* Barbara Kurshan, *The Elephant in the Room with EdTech Data Privacy*, FORBES (June 22, 2017, 1:51 PM), https://www.forbes.com/sites/barbarakurshan/2017/06/22/the-elephant-in-the-room-with-edtech-data-privacy/#37d57d7e57a5 (arguing EdTech applications that consolidate data create security risks by "mak[ing] it possible for a single hacked administrator login to reveal a swath of student data").

76. *See* REIDENBERG ET AL., *supra* note 9, at 24 (finding many school districts in the study failed to have adequate data governance policies for outsourced data collection, twenty percent of which had no policies addressing teacher's use of these services).

77. *See id.* (noting that poor documentation of vendor contracts and limited access to the full terms, in some instances, has serious implications for student data protection).

78. *Id.* at 19, 51–52 (finding school districts are using cloud services for reporting, data analytics, and classroom functions).

79. *See id.* at 26–27 (finding sixty-six percent of schools surveyed did not include the ability to audit or inspect vendors' practices).

80. *See* CHILDREN'S COMM'R, *supra* note 57, at 12 (detailing security risks caused by data breaches, including identity theft, cyberbullying, online impersonation, and stranger danger of identifying physical locations of children through metadata).

Data breaches risk student safety, lead to cyber bullying, contribute to identity theft, and generate financial burdens on schools and parents.[81] Beyond physical safety for abduction or harm from disclosing a child's location, online identifiers expose children to cyberbullying and online impersonation.[82] Bullying and online impersonation harm a child's wellbeing, and statistics show almost a third of U.S. children experience cyberbullying.[83] More troubling is that children who experience cyberbullying are nine times more likely to become a victim of online scams.[84] Long-term impacts of data breaches like identity theft, may actualize years after the breach, when bad actors use the information to open accounts or steal the identity of a child when he or she reaches the age of eighteen.[85]

Beyond future repercussions of identity theft, data breaches cause significant financial hardships for schools and parents in the present.[86] Due to poor regulation and vendor agreements, schools pay a higher cost for security breaches than other industries.[87] In spite of warnings against it, school districts have admitted to paying cybercriminals thousands of dollars to regain control of student data in response to ransomware attacks.[88] Even parents are susceptible to financial extortion attempts from hackers. In 2018, school districts closed classes after parents received text messages

81. *See id.*; *see also, e.g.*, Mamaysky, *supra* note 8 (finding a majority of 6,000 popular children's Android apps reviewed potentially violate COPPA).

82. *See* CHILDREN'S COMM'R, *supra* note 57, at 5–6, 20 (explaining types of data being collected online).

83. *See* Christo Petrov, *47 Alarming Cyberbullying Statistics for 2020*, TECHJURY, https://techjury.net/stats-about/cyberbullying/#gref (last updated June 23, 2020) (detailing how online "threats, mean comments, identify theft, racism, or attacks based on their looks or religion" lead to depression, anxiety, and stress amongst children and young people).

84. *Id.* (finding a direct correlation between cyberbullying and the likelihood of falling victim to identity theft).

85. *See* Jessica Baron, *Posting About Your Kids Online Could Damage Their Futures*, FORBES (Dec. 16, 2018, 8:00 AM), https://www.forbes.com/sites/jessicabaron/2018/12/16/parents-who-post-about-their-kids-online-could-be-damaging-their-futures/#398a258127b7 (discussing Barclays's estimate that two-thirds of identity theft by 2030 will be a result of oversharing information online).

86. *See* Sullivan, *supra* note 5 (describing how hackers use stolen student data to extort parents or school districts).

87. Ramona Carr, *The Rise of Education Data Breaches*, ZETTASET, https://www.zettaset.com/blog/education-data-breaches/ (last visited Aug. 16, 2020) (detailing a Ponemon Institute study showing that schools pay a higher cost to remedy data breaches than other industries, averaging $200 per student record).

88. *See, e.g.*, Sullivan, *supra* note 5 (reporting "a Massachusetts school district paid cybercriminals $10,000 in bitcoin to regain control" after a 2019 ransomware attack).

threatening to expose their students' PII.[89]

In addition to criminal activity, privacy advocates are concerned with EdTech's impact on student privacy. In November 2018, high school students in Brooklyn walked out of school to protest the school's disclosure of student PII to the Summit Learning platform.[90] The student organizers published a letter written to Mark Zuckerberg, co-founder of Summit Learning, detailing concerns about the extent of PII collected by the EdTech, and Summit's policy of disclosing this information to corporations.[91] Similarly, privacy advocacy groups commissioned studies, published reports, and filed lawsuits to further expose the student privacy issues arising from schools' implementation of EdTech applications.[92]

d. How EdTech Passes Off Regulation Compliance to Schools

While there are EdTech applications or services that fall outside of FERPA's education record definition, both the FTC and the ED rely on schools to determine whether an online service meets the statute's standards.[93] The FTC further states that online operators are responsible for determining whether the collection and use of student data by third parties complies with FERPA.[94]

Perhaps following the FTC's lead, EdTech companies will often assign schools the responsibility of determining whether all services provided fully comply with FERPA through the company's contract.[95] To mitigate risk, EdTech companies often include a contract provision requiring schools to obtain verifiable consent from parents.[96] This provision is designed to

89. *See, e.g.*, *id.* (noting that school districts in Alabama, Montana, and Texas had to close schools after parents were texted "ominous, personalized messages").

90. Kronk, *supra* note 10 (detailing a walk out of almost 100 students from the Secondary School for Journalism in Brooklyn in protest of the school's disclosure of PII to Summit Learning).

91. *Id.* ("Summit also says on its website that they plan to track us after graduation through college and beyond. Summit collects too much of our personal information, and discloses this to 19 other corporations.").

92. *See* FEDER, *supra* note 12, at 6 (noting the legal challenges to the 2011 revised FERPA guidelines allowing schools to disclose student information to third-party companies).

93. *See id.* at 5–6.

94. FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9.

95. *See id.*

96. *See* Natasha Singer, *Privacy Concerns for ClassDojo and Other Tracking Apps for Schoolchildren*, N.Y. TIMES (Nov. 16, 2014), https://www.nytimes.com/2014/11/17/technology/privacy-concerns-for-classdojo-and-other-tracking-apps-for-schoolchildren.html (noting that commercial companies can offload COPPA compliance for parental consent to schools within their service contracts).

protect the online operator from COPPA violations and any resulting financial repercussions in the event that an application or service exceeds the educational context.[97]

In lieu of clear FERPA guidelines, parents and privacy advocates are leading the movement for increased transparency and security protocols for EdTech companies.[98] Following public outcry over their lack of transparency, EdTech company InBloom was forced to shut down due to revenue loss.[99] Similarly, Electronic Frontier Foundation, a privacy advocacy group, filed a lawsuit in 2014 forcing Google to acknowledge that it mined data from student accounts for core services outside of the Google Apps for Education.[100]

III. NO MAN'S LAND OF OVERSIGHT: HOW EDTECH IS OPERATING IN A REGULATION VACUUM

Due to outdated regulatory definitions and counteracting enforcement guidelines, the EdTech industry is exploiting a loophole in federal regulations to mine children's online data for financial gain.[101] By connecting with schools as authorized educational partners, EdTech companies' data collection is governed by FERPA's education record guidelines.[102] However, today's online operators collect and store information that far exceeds the traditional school records FERPA was designed to protect, specifically the expansion to indirect and inferred data.[103] Furthermore, the very personal nature of this data exceeds FERPA's directory definition and, therefore, should require parental consent prior to disclosure.[104]

In addition to running afoul of FERPA's legislative intent, EdTech companies' data practices place student information at far greater risk than

97. *See* REIDENBERG ET AL., *supra* note 9, at 61.

98. *See* Kurshan, *supra* note 75.

99. *Id.*

100. *Id.*

101. *See* Kronk, *supra* note 10 (describing the loophole in FERPA regulation that permits schools to disclose student PII to EdTech companies without parental or student consent by considering the company an authorized school official).

102. *See* 20 U.S.C. § 1232g(a)(1) (2018); 34 C.F.R. § 99.31(a)(1)(i)(A) (2020) (expanding FERPA's permitted disclosure of education records to third-party entities if they are authorized educational partners).

103. *See* CHILDREN'S COMM'R, *supra* note 57, at 5–8 (describing the expansive list of data used today, including vast amounts of data collected automatically from online applications).

104. *See* 34 C.F.R. § 99.30(a) (requiring written parental consent prior to disclosing information). *But see* Drake, *supra* note 61 (providing scenarios where schools' online interactions would not be considered education records regulated under FERPA).

traditional education records housed and maintained by individual schools.[105] The large-scale data collected online feeds into the datafication of children, placing their safety and online identities at risk of improper mining, use, or theft.[106] Neither individual schools nor the ED are adequately prepared to oversee FERPA compliance within the EdTech industry.[107] Unlike schools, commercial companies are not subject to financial repercussions or disciplinary actions by ED for violating FERPA.[108] Subsequently, FERPA provides no regulatory incentive for EdTech companies to provide adequate transparency and privacy protection.[109] Outside of school education records, COPPA governs the data collection for children by online operators.[110] COPPA is well-positioned for oversight enforcement because the FTC investigates complaints and can impose financial penalties and business restrictions upon companies found to be in violation of the Act.[111]

a. EdTech's Expansive Collection of Student Data Transcends the Realm of FERPA's Education Records

EdTech companies exploit FERPA's overly broad definition of education records to mine enormous amounts of children's online data, largely without notice and absent parental consent.[112] FERPA limits school disclosure

105. *See* Sullivan, *supra* note 5 (comparing traditional and digital files to advocate for heightened EdTech security).

106. *See id.* (relaying events where student PII was stolen and used for extortion); *see also* FEDER, *supra* note 12, at 5–6 (noting that privacy advocates are concerned about the risks to student privacy that data sharing poses).

107. *See* 34 C.F.R. § 99.1(a) (limiting FERPA enforcement to educational institutions that receive federal funds administered by the Secretary of Education).

108. *See* Brandon Wong, *FERPA: The Joke with No Punchline*, AM. ENTER. INST.: BLOG (Feb. 23, 2015), https://www.aei.org/education/ferpa-joke-punchline/ (noting that FERPA only applies to institutions that are recipients of federal funds, not for-profit EdTech companies).

109. *See* 34 C.F.R. § 99.1 (indicating that FERPA regulations are limited to educational institutions receiving federal funding).

110. 15 U.S.C. § 6502(a)(1) (2018); 16 C.F.R. § 312.3 (2020).

111. *See, e.g.*, Alexi Pfeffer-Gillett, *Peeling Back the Student Privacy Pledge*, 16 DUKE L. & TECH. REV. 100, 130 (2018) (discussing how the FTC's investigations and consumer oversight align with consumers' right to accurate information, and the FTC has the ability to hold companies accountable with financial and procedural remedies); *see also* Mamaysky, *supra* note 8 (predicting increased investigation of online operators' adherence to COPPA is signaled by the FTC's record-setting 2019 YouTube settlement for COPPA violations).

112. *See* Kronk, *supra* note 10 (describing the loophole in FERPA regulation that permits schools to disclose PII to EdTech companies without parental or student consent by considering the commercial entity an authorized school official).

policies to information directly linked to a student, related to their education, and maintained by the school as an education record.[113] However, EdTech applications often fail to meet all of these FERPA requirements for education records.[114] EdTech companies are indiscriminately gathering information not directly linked to students' education.[115]

First, the technological advancements of online applications have negated the protections of limiting FERPA to records directly linked to a student.[116] If a student's image is captured incidentally or as part of the background at a school event, the ED does not consider the image to be directly related to a student and, therefore, not an education record.[117] In that instance, schools can still publish or share the image without obtaining the consent of the student by reasoning that the inadvertent peripheral image contained no PII data beyond directory information.[118] There is little risk of harm or invasion of privacy for a student if he appeared anonymously in the background of a photo printed in a newspaper.[119]

However, unlike the traditional directory information disclosed by a school, online operators present more tangible risks to a student's privacy if caught in the background of an image due to the technological advancements of the application.[120] EdTech companies place student privacy at risk because they make student PII more obtainable when online applications can use machine learning and AI algorithms to identify individuals in the

113. 20 U.S.C. § 1232g(b) (2018).

114. *See* Jackie Gharapour Wernz, *Are Emails, Texts, Tweets, and Other Digital Communications Student Records Under FERPA and State Law?*, JD SUPRA (Feb. 20, 2013), https://www.jdsupra.com/legalnews/are-emails-texts-tweets-and-other-dig-60950/ (discussing the ambiguous area of applying FERPA to digital communication records when the files are not considered education records under the Act).

115. *See* ALIM ET AL., *supra* note 54, at 5 (detailing how EdTech applications data-gathering goes beyond traditional PII to include behavioral information, search terms, contact lists, location data, and browsing history).

116. *See id.* (highlighting the exponential increase in data as a result of technology applications' ability to generate new data).

117. *See* FAQS ON PHOTOS, *supra* note 21 (describing how images are not directly linked to students captured in the background, but the school still must obtain parental consent to disclose the photo or alternatively classify the image as directory information).

118. *See id.*

119. *See id.*

120. *See* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (last updated Feb. 10, 2020) (explaining the ability for computer programming to collect images online and then use algorithms to convert the images into vectors, mathematical formulas, that are grouped together to identify individuals; a technology being used to eliminate anonymity of faces in background or surveillance images by more than 600 law enforcement agencies with Clearview AI).

background or tag the image's geolocation to expose the child's location.[121] Applications such as Google Photos also use AI technology to scan images to identify any faces captured in photos, even faces in the background or indirect focus of the image.[122]

In those instances, there is an equivalent risk of privacy invasion for both the directly linked student and any children incidentally captured because the online application is equally collecting and tracking student PII.[123] Due to these technological advancements, FERPA's guidelines to determine direct linkage to a student in traditional media are incompatible with the enormous capabilities of online applications.[124]

Second, EdTech companies' capability to capture and generate new types of data is testing the limits of educational context required under FERPA.[125] Data simply obtained by an educational institution or agent is not automatically considered to be within the educational context of FERPA regulation.[126] Under the Act, education records are limited only to

121. *See, e.g.*, Matthew Lynch, *U.S. PreK-12 Schools Explore Adopting Facial Recognition Software*, TECH EDVOCATE (Sept. 6, 2019), https://www.thetechedvocate.org/u-s-prek-12-schools-explore-adopting-facial-recognition-software/ (highlighting EdTech applications' use of facial recognition, including measuring student engagement in China by scanning faces to determine if a student is engaged, tired, or distracted).

122. *How Google Uses Pattern Recognition to Make Sense of Images*, GOOGLE, https://policies.google.com/technologies/pattern-recognition?hl=en (last visited Aug. 11, 2020) (describing how computers use pattern recognition to identify faces in photos); *see* Dale Smith, *Google Knows What You Look Like. Here's What it Means and How to Opt Out,* CNET (Feb. 4, 2020, 5:00 AM), https://www.cnet.com/how-to/google-knows-what-you-look-like-heres-what-it-means-and-how-to-opt-out/ (explaining ways Google is acquiring, storing, and using facial data).

123. *Compare* 34 C.F.R. § 99.1 (2020) (requiring FERPA education records to be directly linked to the student and maintained by the school), *with* FAQS ON PHOTOS, *supra* note 21 (describing how incidental images are not regulated by FERPA).

124. *See* Thomas Germain, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, CONSUMER REPS., https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/ (last updated Dec. 6, 2019) (describing how images capture location through GPS data). *Compare* FAQS ON PHOTOS, *supra* note 21 (arguing children included in the background of an image are not covered under FERPA because there is little likelihood of an invasion of privacy), *with* Lily Hay Newman, *AI Can Recognize Your Face Even if You're Pixelated*, WIRED (Sept. 12, 2016, 11:54 AM), https://www.wired.com/2016/09/machine-learning-can-identify-pixelated-faces-researchers-show/ (describing how machine learning can be used to defeat privacy protection technologies by identifying pixelated or obfuscated faces in images and videos).

125. *See* ALIM ET AL., *supra* note 54, at 24 (explaining how EdTech applications are gathering indirect and inferred information found solely in online applications).

126. *See What Records Are Exempted from FERPA?*, U.S. DEP'T OF EDUC., https://studentprivacy.ed.gov/faq/what-records-are-exempted-ferpa (last visited Aug. 11, 2020) (listing files that are not considered education records collected by schools).

information collected relating to a student's education.[127] However, a feature that distinguishes online applications from traditional school records is the ability to collect vast amounts of engagement data that schools did not collect previously.[128]

The indirect and inferred data EdTech applications collect often exceeds the traditional PII found within the permanent student file directly maintained by the school.[129] Online applications collect geolocations of users, IP addresses, and biometric data such as heart rate or activity levels.[130] Additionally, many online applications retain information generated from online messaging, file sharing, and email communication between users.[131] The expanding universe of indirect data EdTech companies are amassing is then compiled with direct information disclosed by schools, such as grades, attendance, or test scores, to predict behavior or develop learning strategies.[132] Unlike grades or attendance, the relationship between browser preferences, geolocation, or social communications with other users in web chats is, at best, tenuously related to a student's education.[133]

Third, schools can fail to maintain the data collected by EdTech companies as required by FERPA. The ED requires documents to be

127. 20 U.S.C. § 1232g(a)(4)(A) (2018).

128. *See* CHILDREN'S COMM'R, *supra* note 57, at 6 (distinguishing the various types of data collected online, specifically new data "given off" unknowingly by users online, such as cookies). *Compare* 20 U.S.C. § 1232g(a)(5)(A) (defining traditional directory information such as name, address, and school activities), *with* 16 C.F.R. § 312.2 (2020) (tailoring the personal identifiers for COPPA regulation to online services and applications by including online contact, persistent identifiers, and geolocations).

129. *See* ALIM ET AL., *supra* note 54, at 24.

130. *See* CHILDREN'S COMM'R, *supra* note 57, at 3 (arguing the data collected on children through connected devices, monitoring equipment, and social media is exponentially expanding the amount of data harvested compared to previous generations).

131. *See, e.g.*, CLASSDOJO, HOW DOES CLASSDOJO BUILD A POSITIVE SCHOOL COMMUNITY? 1–2 (n.d.), https://static.classdojo.com/docs/TeacherResources/SchoolLeaderPack/ClassDojo-SchoolLeaderPack.pdf (last visited Aug. 11, 2020) (highlighting application features that allow for officials to share stories, images, and messages with parents); Jeff Knutson, *Essential Tips and Tools to Improve the Parent-Teacher Communication Loop*, COMMONSENSE EDUC. (Aug. 23, 2016), https://www.commonsense.org/education/articles/6-tech-tools-that-boost-teacher-parent-communication (promoting EdTech messaging applications that increase communication between students, teachers, and parents).

132. *See* CHILDREN'S COMM'R, *supra* note 57, at 6 (defining inferred data as an analysis combining direct and indirect information to then form a prediction).

133. *Compare* 20 U.S.C. § 1232g(a)(4)(A) (limiting education records to files that contain information directly linked to a student and are maintained by the educational agency or institution), *with* Wernz, *supra* note 114 (discussing the ambiguous area of applying FERPA to digital communication when the files are not considered education records).

maintained and stored by a school, or its agent to be regulated by FERPA.[134] In addition to storing data, schools must demonstrate the file was retained with some degree of permanency to be considered an education record, such as retaining the record in a filing cabinet or permanent secure database.[135] Even while EdTech companies collect information as agents for schools, there is still a requirement to show an intent to hold the data as part of a permanent record.[136] Otherwise, the electronic data can be considered temporary in nature and outside FERPA regulation.[137] Guidelines for demonstrating a deliberate action to retain, such as attaching an email to a permanent file, also apply to agents of schools.[138] However, the limitless availability of storage nullifies the permanency requirement as previously presented to schools.[139] By transitioning education records from physical mediums to digital files offsite in cloud servers, schools have virtually unlimited storage space and digital data is being captured at exponentially higher rates due to ease.[140]

Without physical constraints, vast amounts of data collected through EdTech applications fail to meet FERPA requirements because they are generated and shared between users instead of with schools.[141] User-provided information such as profile submissions and webchat discussions between classmates are more closely analogous to peer-graded assignments, classmate feedback, or group projects than school records because the data originates outside of the educational context.[142] The ED has determined that peer-graded assignments are not considered education records under FERPA

134. 34 C.F.R. § 99.3 (2020); *see* 20 U.S.C. § 1232g(a)(4)(A).

135. *See* Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426, 432–33 (2002) (holding that FERPA suggests a method of permanency or intent to retain files as a statutory requirement).

136. *See* S.A. v. Tulare Cty. Office of Educ., No. CV F 08-1215 LJO GSA, 2009 U.S. Dist. LEXIS 93170, at *9–10 (E.D. Cal. Oct. 5, 2009) (holding emails are temporary and only education records if printed and placed in a student file).

137. *See* Drake, *supra* note 61 (discussing when email communications can be education records governed by FERPA).

138. 34 C.F.R. § 99.31 (a)(1)(i)(B); *see also* Kronk, *supra* note 10 (describing risks associated with FERPA's extension of authorized school officials to third-party commercial companies).

139. *See* CHILDREN'S COMM'R, *supra* note 57, at 11 (describing the increase of connected devices gathering information, paired with advancements in data processing to generate predictive inferred data, which means online data is exponentially growing).

140. *See* REIDENBERG ET AL., *supra* note 9, at 1–2.

141. *See* Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426, 433–35 (finding peer grades are not education records because school officials did not capture the data or create it with the intent of retaining in a permanent file).

142. *See* Wernz, *supra* note 114 (highlighting the ambiguous area of applying FERPA to classroom applications, specifically the characteristics of user-submitted information).

because the documents originate outside of school officials.[143] Similarly, online communication between peers should not be considered education records protected by FERPA.[144] Furthermore, the records must be maintained by FERPA standards, preventing disclosure to non-authorized parties.[145] While offsite servers may still be considered secure by enlisting password authentication, many applications feature the ability for end users to view other users' accounts, activity, and records.[146]

Further compounding the issue of maintaining records, many EdTech companies disclose student data to additional third parties to capture, store, and process the collected data.[147] The vast network created through EdTech services is multi-layered and far more complex than schools' traditional record keeping practices.[148] As a result, EdTech operators are comingling traditional educational information, such as attendance and grades, with data generated from social features such as peer messaging or photo sharing.[149] Information generated from social features in the online applications is more analogous to temporary email communications that are not considered education records.[150]

Finally, even if information meets FERPA's education record standards,

143. *See* 20 U.S.C. § 1232g(a)(4)(B)(ii) (2018) (limiting FERPA education records to files "maintained" by a school); 534 U.S. at 434–35 (confirming that the ED interpretation of "maintained" education records to be "kept by a single central custodian" through "describing a 'school official' and 'his assistants' as the personnel responsible for the custody of the records").

144. 534 U.S. at 432–33 (explaining that education records are not "maintained" when students grade their peers' work because student graders are not acting on behalf of an educational institution).

145. 34 C.F.R. § 99.31(a)(6) (2020).

146. *See* Erin Klein, *5 Apps to Share Class Work Beyond the Classroom!*, SCHOLASTIC: TOP TEACHING BLOG (Mar. 25, 2014), https://www.scholastic.com/teachers/blog-posts/erin-klein/5-apps-share-class-work-beyond-classroom/ (describing online applications that can be used to share classroom and student information with parents).

147. *See* REIDENBERG ET AL., *supra* note 9, at 17 (reporting that ninety-five percent of selected school districts shared student information with third parties through cloud computing arrangements).

148. *See* GIRARD KELLY ET AL., COMMON SENSE MEDIA, 2019 STATE OF EDTECH PRIVACY REPORT 47 (2019), https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-state-of-edtech-privacy-report.pdf (finding that seventy-nine percent of EdTech applications or services share student information with third parties for analytics and data tracking).

149. *See id.* at 50 (discussing that more than half of surveyed applications risk data being shared through social or federated logins on third-party sites such as Facebook).

150. *See* S.A. v. Tulare Cty. Office of Educ., No. CV F 08-1215 LJO GSA, 2009 U.S. Dist. LEXIS 93170, at *9–10 (E.D. Cal. Oct. 5, 2009) (holding that because emails have a "fleeting nature," they are only education records if printed and placed in a student file).

EdTech companies are collecting metadata, behavioral observations, and predictive classifications that exceed student directory information.[151] Like disclosing non-directory information, such as social security numbers, schools are required to obtain parental consent prior to using EdTech applications to generate and disclose a student's non-directory information.[152] A grounding principle of FERPA is the strong foundation in promoting parental transparency.[153]

b. Disclosure of Student Information to EdTech Runs Afoul of FERPA's Intent

Congress enacted FERPA to protect the process for disclosing students' education records.[154] As emphasized in a letter from the cosponsors, FERPA's intent is to protect student data by regulating how schools release records and promote transparency through parental access.[155] The ED erred by loosening the guidelines for schools to release student education records to authorized third parties because this extension does not align with the original intent of the statute.[156]

First, the 2011 Amendments decrease transparency for students and parents regarding school records.[157] FERPA originally limited disclosure to educational institutions and agencies for financial aid, but the 2011 Amendments permit disclosure to commercial companies in the tech industry.[158] Additionally, many tech companies rely on several third-party applications or services to run analytics, store data, or partner services.[159]

---

151. *See* REIDENBERG ET AL., *supra* note 9, at 24 (finding that several school districts inadvertently entered contractual agreements that permitted the outsourcing of student information to third parties).

152. 34 C.F.R. § 99.30 (2020).

153. *See* ELEC. PRIVACY INFO. CTR., *supra* note 31 (clarifying that schools must notify parents of their rights under FERPA annually, including their right to review their children's education records).

154. *See* STUDENT PRESS L. CTR., *supra* note 15.

155. *See id.*; Greenberg, *supra* note 15.

156. *See, e.g.*, Kronk, *supra* note 10 (describing that the expansion of FERPA permits schools to disclose student PII to EdTech companies without parental or student consent); *see also* STUDENT PRESS L. CTR., *supra* note 15 (describing that the driving factors for Sen. James Buckley in coauthoring the FERPA legislation were the lack of parental access to student records and a lack of consistency in schools' policies governing disclosure of student records).

157. 34 C.F.R. § 99.31(a)(1)(i)(B).

158. *Id.*

159. *See* REIDENBERG ET AL., *supra* note 9, at 24 ("Fordham CLIP's research revealed . . . [that] many [district schools] did not seem to understand the nature of the services that they outsourced to third-party providers.").

Schools are not required to notify parents if disclosing student information that does not require prior parental consent, including data disclosed to third-party commercial companies acting as authorized educational partners.[160] As a result, the amendments expose student data to a wide range of entities beyond educational institutions, including commercial technology companies such as Google, Amazon Web Services, and Apple.[161]

Second, by not limiting approved authorized third parties to educational institutions or non-profit companies, schools can release information to commercial companies who provide a service or product.[162] The 2011 Amendments permit schools to release records to commercial companies who may then profit from the monetization of student data.[163] However, the penalty for violating FERPA regulations is limited to the withholding of federal funding to schools or educational institutions, and does not extend to any financial penalty for commercial companies.[164] The ED has no oversight or enforcement power over commercial companies.[165] Data collected through online applications from individual consumers instead of schools face stricter regulations under COPPA.[166] However, the FTC's decision to not investigate online applications receiving information from schools permits commercial companies to effectively operate without oversight.[167] Under this gap, EdTech companies can collect and use data disclosed from student accounts, obtained without parental consent, that the ED may determine were not in fact education records and thus should instead require

160. *See* DEP'T OF EDUC., THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT GUIDANCE FOR ELIGIBLE STUDENTS 3 (2011) [hereinafter DEP'T OF EDUC., FERPA GUIDANCE], https://www2.ed.gov/policy/gen/guid/fpco/ferpa/for-eligible-students.pdf (describing schools' notification obligations for data disclosed without parental consent).

161. *See* Greenberg, *supra* note 15 (discussing how FERPA guidelines do not limit the type of entity a school can authorize as an educational partner and receive student data).

162. *See* Kurshan, *supra* note 75 (warning conflicts can arise when commercial companies that rely on data mining and advertising to raise revenue have access to vast amounts of student information).

163. 34 C.F.R. § 99.31(a)(1)(i)(B).

164. *See* Wong, *supra* note 108 (positing that FERPA creates no mechanism for enforcement on companies because the law's drafters did not envision commercial purposes for disclosing student data).

165. *See id.*

166. *Compare* 34 C.F.R. § 99.67(a) (listing the remedies available to the ED to enforce FERPA that are all tied to withholding or prohibiting federal funding for school programs), *with* 16 C.F.R. § 312.9 (2020) (stating the remedies available to the FTC for COPPA violations include financial penalties to commercial companies).

167. *See* 20 U.S.C. § 1232g(b)(1)(F) (2018); *see also* REIDENBERG ET AL., *supra* note 9, at 11 (explaining that COPPA does not apply to information about a child that is obtained directly from a school).

parental consent as governed under COPPA.[168] The exception allowing schools to grant consent, on behalf of parents, under the assumption that the information pertains to education records, regardless of its actual nature, makes this analysis only retrospective with the result that EdTech companies receive such information to use at will without constraint or oversight. [169]

As a result of the 2011 Amendments, school guidelines have reinstated the wide disparity in school disclosure policies for releasing student records.[170] Congress enacted FERPA to address school disclosure policies that were inconsistent and unregulated.[171] However, the ED's decision to expand authorized disclosure to include third-party commercial companies, such as EdTech companies, as authorized educational partners creates a wide range of data exposure and enforcement concerns.[172] The original FERPA guidelines limited the release of student records to educational institutions, parties for financial aid, and governments.[173] Today, schools can release information to EdTech companies who, in turn, share the information with additional partners.[174] Since the 2011 Amendments to FERPA, EdTech companies collect and use children's PII without prior parental consent.[175] FERPA, created in response to school's inconsistent and irregular practices of disclosing information, now authorizes schools wide latitude in disclosure of student PII.[176]

168. REIDENBERG ET AL., *supra* note 9, at 2; *see* Kronk, *supra* note 10 (explaining that EdTech programs collect unlimited personal information and disclose it to other third parties).

169. 34 C.F.R. § 99.31(a) (limiting FERPA violation investigations by the ED to educational institutions receiving federal funding, which does not include commercial EdTech companies).

170. *See* Carr, *supra* note 87 (highlighting the disparity within school systems and the challenge it poses for implementing security protocols in school systems); *see also* REIDENBERG ET AL., *supra* note 9, at 21.

171. *See* Greenberg, *supra* note 15 (discussing FERPA's intent to increase transparency and parental oversight of student data).

172. Kronk, *supra* note 10.

173. 34 C.F.R. § 99.1(a); *see also* Kronk, *supra* note 10.

174. *See* 34 C.F.R. § 99.31(a) (allowing schools and educational partners to share student data with third parties).

175. *See id.* (noting that schools may disclose information without prior parental consent to third parties if a school has outsourced institutional services to the company).

176. *Compare* ELEC. PRIVACY INFO. CTR., *supra* note 31 (discussing Sen. James Buckley's and Sen. Claiborne Pell's intent for FERPA), *with* FEDER, *supra* note 12, at 5–6 (noting the impact of the 2011 FERPA amendment, which allows schools to disclose student information to third-party companies).

c. Schools and the Department of Education Are Ill-Equipped to Enforce FERPA Compliance in EdTech

The wide latitude in school data policies, combined with the ED's inability to enforce FERPA regulations on commercial companies, creates a zone of unaccountability.[177] Schools are ill-equipped to oversee data mining by EdTech companies.[178] Consequently, EdTech companies exploit the gap in oversight created by the combination of the ED's inability to enforce FERPA violation penalties against commercial companies and the FTC's refusal to oversee student data disclosed by schools.[179]

Given the proliferation of data generated by online services, it is unreasonable for schools to complete a case-by-case determination on whether inferred or indirect data meets the education record definition.[180] Direct information is shared with EdTech applications and online operators daily by school administrators, teachers, and students.[181] Beyond the direct information, online applications are collecting vast amounts of indirect and inferred data that schools, parents, and users are simply unaware of.[182] However, the ED relies on the individual context of each record to determine if FERPA applies.[183] Because many schools are implementing third-party applications due to lack of resources, it follows then that schools with limited resources do not have the bandwidth to oversee educational partners' FERPA compliance.[184] Thus, there is little to no oversight of data collection,

177. *See* Kronk, *supra* note 10 (explaining a gap in FERPA regulation created by expanding disclosures to third parties).

178. *See id.*; *see also* REIDENBERG ET AL., *supra* note 9, at 24 (finding many districts had inadequate data governance policies for outsourced data collection, including twenty percent of study respondents with no policies addressing teacher's use of services).

179. *See* Kronk, *supra* note 10.

180. *See* FAQS ON PHOTOS, *supra* note 21 (explaining the case-by-case process by which the ED reviews whether a photo or video is an education record governed by FERPA).

181. *See* DELOITTE, 2016 DIGITAL EDUCATION SURVEY 4 (2016), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-digital-education-survey.pdf (finding that more than fifty percent of teachers use three digital devices every week in their classrooms, with forty-two percent of teachers reporting they use at least one device daily).

182. *See* ALIM ET AL., *supra* note 54, at 15; *see also, e.g.*, Singer, *How Google Took Over*, *supra* note 11 (reporting that Google declines to disclose details for how it gathers and uses student data, and whether student data is comingled with commercial applications).

183. *See* Drake, *supra* note 61 (explaining the various ways digital data on social media may be considered education records).

184. *See* Sullivan, *supra* note 5 (noting that schools lack funds and resources to provide the latest security technology).

retention, and use by third-party companies partnering with schools.[185]

Furthermore, while schools may own the data EdTech companies collect from students, these records are metadata, behavioral observations, and predictive classifications; none of these categories are considered directory information under FERPA.[186] Similar to disclosing non-directory information such as social security numbers, schools should obtain parental consent prior to using EdTech applications to generate non-directory information on students.[187] The adoption of third-party commercial companies as authorized educational partners is alarming because of the widespread use of EdTech applications in schools and the lack of transparency companies provide about their data practices.[188] This lack of transparency and lax oversight ultimately result in increased risks to student privacy and risk of data breach.[189]

Another flaw with FERPA regulating school disclosure to EdTech companies is the non-existent threat of enforcement.[190] During the forty-five years since FERPA's enactment, ED has never withheld federal funding from a school in violation of the statute.[191] Without an actual risk of funding loss, there is little incentive for schools to diligently verify that commercial partners, and any third-party commercial companies they share information with, are FERPA compliant.[192]

By implementing a case-by-case approach instead of clearly defining the education record parameters, the ED creates a self-serving opportunity for schools to assert a broad application of FERPA to student data collected through authorized EdTech applications.[193] Schools avoid the logistics of

185. *See* FEDER, *supra* note 12, at 5–6 (noting the response to the ED's 2011 revised FERPA guidelines and the impact of expanding access of personal information to third parties allowed schools to disclose PII without parental consent).

186. *See* REIDENBERG ET AL., *supra* note 9, at 4 (defining directory information to include details such as the "student's name, address . . . date and place of birth, major field of study," and attendance information).

187. *See* 20 U.S.C. § 1232g(b)(1) (2018) (requiring parental consent prior to disclosure of non-directory information).

188. *See* FEDER, *supra* note 12, at 2.

189. *See* Kurshan, *supra* note 75 (describing threats to student privacy from EdTech applications, recommending EdTech products require more monitoring, and emphasizing the need for clarity regarding when companies should be allowed in classrooms).

190. *See* PARENT COAL., *supra* note 38 (stating that as of 2019, the ED has never rescinded funding or issued a financial penalty against a school for violating FERPA regulations).

191. *Id.*

192. *See* 34 C.F.R. § 99.31(a)(1)(i)(B) (2020) (requiring schools to verify that third-party vendors are FERPA compliant).

193. *Id.*; *see also* STUDENT PRESS L. CTR., *supra* note 15 (arguing the lack of guidance

obtaining parental consent, and online operators avoid FTC oversight for COPPA compliance by painting a broad education record umbrella.[194]

This circular logic leaves parents and students with little recourse for privacy violations resulting from schools granting consent on an individual's behalf and sharing student data with an EdTech company.[195] Without a private right of action to sue in courts, parents can only file complaints with the ED.[196] To further complicate the matter, the ED only investigates education record determinations after a valid complaint is filed, and the ED requires parents to specify what records they are seeking for review from the school.[197]

IV. HOW TO CLOSE THE SCHOOL CONSENT LOOPHOLE GRANTING EDTECH ACCESS TO CHILDREN'S PII

The gap in oversight of the EdTech industry's collection and use of student data can be addressed by amending FERPA guidelines to narrowly tailor the disclosure of student data to non-commercial companies or requiring notification and clear parental consent.[198] Alternatively, the loophole can be closed by revoking the school exemption to COPPA enforcement and empowering the FTC to address commercial company violations with monetary fines and remedial efforts.[199]

---

by the ED has led to a pattern of abuse by schools using FERPA's individual review of education records definition to avoid requests for records).

194. *See* REIDENBERG ET AL., *supra* note 9, at 24–25 (summarizing studies showing that school contracts with cloud services often lack compliance and have weak data governance).

195. *See* Greenberg, *supra* note 15 ("The U.S. Supreme Court held . . . that individuals and organizations cannot sue to enforce F[ERPA]. The flawed decision effectively closed the courts to students [and] parents . . . harmed by F[ERPA] fouls."); *see also* Tarka v. Franklin, 891 F.2d 102, 104 (5th Cir. 1989) (noting that there is no language in the statute or legislative history indicating congressional intent for a private right of action); Slovinec v. DePaul Univ., 222 F. Supp. 2d 1058, 1060–61 (N.D. Ill. 2002) (affirming that there is no congressional intent to create private right of action under FERPA).

196. *See* Ashford v. Edmond Pub. Sch. Dist., 822 F. Supp. 2d 1189, 1200 (W.D. Okla. 2011) (upholding dismissal of student claim because FERPA fails to confer individually enforceable rights).

197. *See* DEP'T OF EDUC., FERPA GUIDANCE, *supra* note 160, at 6 (describing the ED investigation process of valid FERPA complaints); *see also* Wernz, *supra* note 114 (referencing ED instructions clarifying parent's responsibility to specify the records he is seeking access to).

198. *See* Kronk, *supra* note 10 (describing the loophole in FERPA regulation permitting schools to disclose student PII to EdTech companies without parental or student consent).

199. *See* Pfeffer-Gillett, *supra* note 111, at 134 (discussing the FTC's ability to hold EdTech companies accountable with financial and procedural remedies).

a. Limit the Reach of FERPA by Narrowly Tailoring Disclosure of Education Records

The ED can amend FERPA guidelines to narrow the definition of education records. By tailoring the definition of education records to data necessary for education, the ED can release more oversight of PII back to the FTC for COPPA enforcement. Today's broad definition of education records permits EdTech companies to collect and store all data captured through school contracts by stating the service or application is used for an educational context, including new types of indirect and inferred data generated and stored only within the application.[200] By narrowing the scope of education records, EdTech companies and schools will be required to notify and obtain parental consent for collection and use of student data that exceeds an educational context, such as geolocation or IP addresses.[201]

The ED could further decrease safety risks to students by limiting the information shared without parental consent. Recognizing the increased risk of disclosing sensitive online information such as images and location identifiers, the ED could limit the information shared with online operators to traditional directory information.[202] Requiring parental consent for non-directory information may increase awareness about student privacy concerns, promote parent engagement, and increase corporate accountability.[203]

b. Eliminate the FTC's School Exemption for COPPA Compliance

To create accountability for the EdTech industry, the FTC can amend the COPPA school exemption to apply strictly to educational institutions. Today, commercial EdTech businesses can collect student information with only the consent of the school when acting as authorized educational partners.[204] However, even when acting as an agent of a school, EdTech companies remain commercial online operators.[205] By revoking the FTC

200. *See* 34 C.F.R. § 99.31(a)(1)(B)(1) (2020) (allowing EdTech applications to capture student PII if the company asserts that the information is part of the service or function the company was contracted to provide as a school official).

201. *See* 20 U.S.C. § 1232g(b)(1) (2018) (allowing the disclosure of education records to a broad range of entities, including other educational institutions, courts, and consultants acting on behalf of the school).

202. *See id*. § 1232g(a)(5) (defining traditional directory information such as name, address, and school activities).

203. *See* REIDENBERG ET AL., *supra* note 9, at 30 (suggesting that requiring parental consent could improve data compliance with FERPA).

204. 34 C.F.R. § 99.31(a).

205. *See* 15 U.S.C. § 6501(2)(A) (2018) (limiting operators regulated under COPPA to services "operated for commercial purposes").

school exception or, at a minimum, narrowing the restriction to non-commercial online operators, the FTC can ensure the privacy protection safeguards of COPPA remain intact for all online businesses.[206]

To ensure COPPA compliance, the FTC encourages adherence by providing guidance through rules, statements, and settlements for violations.[207] Unlike FERPA's vaguely defined education record standards, COPPA provides detailed categories of the types of data that fall within the legislation.[208] COPPA also recognizes the evolving nature of technology and prescribes to regular reviews to keep the legislation current.[209]

Finally, the potentially most effective tool to increase security of student data would be to have the FTC enforce COPPA compliance to all commercial companies collecting and using children's PII.[210] Regardless if EdTech companies contract directly with schools, if the company is providing a commercial service, it should be COPPA compliant. The FTC is better suited to review data violations by online operators because it can consistently apply the same investigation and analysis processes for potential COPPA violations, regardless of whether the online operator receives consent from a school or parent.

Moreover, remedies available for COPPA violations are not limited to federal funding restrictions, which do not apply to commercial companies.[211] In addition to applying financial penalties, the FTC can affect industry change through remedial requirements as part of a settlement.[212] Currently, the lack of financial penalties in FERPA's history provide little deterrence for malfeasance or bad actors in the EdTech industry.[213] Paired with the lack

206. *See* FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9 (describing how companies are not required to obtain parental consent for student PII obtained from a school district if the information is for "use and benefit of the school" because school districts are governed by FERPA).

207. *See* 15 U.S.C. § 6505(b) (listing relevant provisions for compliance enforcement).

208. *See id.* § 6501(8) (outlining personal information covered by COPPA).

209. *See FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule*, FED. TRADE COMM'N (Dec. 19, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over (noting the FTC's 2010 review of COPPA and the subsequent 2012 amendment to reflect the changes in technology).

210. *See* Pfeffer-Gillett, *supra* note 111, at 130 (arguing that the FTC can hold educational service providers accountable).

211. *See id.* at 134 (noting two examples of FTC remedies for COPPA violations).

212. *See* Press Release, Fed. Trade Comm'n, *supra* note 51 (discussing FTC's settlement with TRUSTe Inc.).

213. *See* PARENT COAL., *supra* note 38 (suggesting the lack of financial penalties for FERPA violations do not promote compliance but instead invite lackluster oversight).

of access to an individual right of action, FERPA gives little recourse for individuals. By revoking the school exception to COPPA enforcement, the FTC can ensure adequate oversight of online operators in the EdTech industry by holding all commercial online operators to the same standards for collection and use of student data.[214]

V. CONCLUSION

By expanding disclosure of student records to third-party commercial companies, the current FERPA guidelines decrease transparency, place student data at risk, and are askew with the legislative intent. To close the loophole, the ED can amend FERPA guidelines to limit schools' disclosure of student data to non-commercial third parties or require parental consent. Alternatively, the FTC can amend the school exemption to investigate and enforce COPPA violations of commercial companies that receive student data from schools. The FTC is better equipped to classify and enforce data privacy protections for online operators and provide effective deterrence measures against commercial EdTech companies.

214. FED. TRADE COMM'N, *Complying with COPPA*, *supra* note 9 (discussing online operators' requirements to meet COPPA and FTC enforcement regulations).