BYU Education & Law Journal

Volume 2021 | Issue 1 Article 6

2021

Student Privacy in the Digital Age

Susan G. Archambault
William H. Hannon Library at Loyola Marymount University

Student Privacy in the Digital Age

Cover Page Footnote

30 Rhoades, supra note 1, at 454. 31 Doran, supra note 19. 32 Casey Waughn, Rethinking Video Mandates in Online Classrooms: Privacy and Equity Considerations and Alternative Engagement Methods, STUDENT PRIVACY COMPASS (December 2, 2020), https://studentprivacycompass.org/videomandates/. 33 Lauraine Genota, Data Privacy, EDUCATION WEEK (October 31, 2018), https://www.edweek.org/ technology/data- privacy/2018/10. 34 Id.

STUDENT PRIVACY IN THE DIGITAL AGE

Susan G. Archambault*

INTRODUCTION

Schools are increasingly relying on the educational technology industry (EdTech) for cloud computing services, online applications, and data analytics tools. In 2017, more than half of K-12 students used Google's education apps, and over 95% of U.S. K-8 schools use ClassDojo for sharing photographs and videos of students.[1] A 2013 study found that 95% of districts relied on cloud services for a variety of functions, including data mining related to student performance, support for classroom activities, student guidance, data hosting, cafeteria payments, and transportation planning.[2] Educational technology can offer many benefits for

*Susan Gardner Archambault is Head of the Reference and Instruction Department in the William H. Hannon Library at Loyola Marymount University (LMU). She has published and presented extensively on topics related to information literacy and academic library assessment. She is currently a doctoral student in LMU's Educational Leadership for Social Justice program, where her research explores algorithmic literacy.

[1] Amy Rhoades, Comment *Big Tech Makes Big Data Out of Your Child: The FERPA Loophole EdTech Exploits to Monetize Student Data*, 9 AM. U. BUS. L. REV., 445, 453-454 (2020).

[2] Joel Reidenberg, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier & Daniela Alvarado, *Privacy and Cloud Computing in Public Schools*, 2 CENTER ON LAW AND INFORMATION POLICY, 1, 17 (2013), https://ir.lawnet.fordham.edu/clip/2/.

schools, including discounted or free services, more efficient and effective teaching through classroom monitoring and management, more personalized learning, and easier and faster communication.[3] EdTech companies can also use student attendance data to allocate truancy resources, inform policy making, and make curriculum decisions.[4]

The Department of Education has encouraged schools to use "big data" to improve assessment and educational innovation.[5] Schools are attracted to companies like Google for giving away free products such as Google Workspace for Education (formerly GAFE, or Google Apps for Education, and later renamed G Suite Enterprise for Education; it is a web-based service that includes student email accounts, calendars, document storage, and more).[6] The Google tools are used by more than 30 million students, teachers, and administrators.[7] Google uses benefiting rhetoric, hands-off rhetoric, and sidelining rhetoric to

[3] Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. REV. 1673, 1681-1685 (2019).

[4] 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/.

[5] Marie Bienkowski, Mingyu Feng & Barbara Means, U.S. Department of Education, Office of Educational Technology, *Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics: An Issue Brief ED-04-CO-0040* (October, 2012), https://files.eric.ed.gov/fulltext/ED611199.pdf.

[6] Shantanu Sinha, *More Options for Learning with Google Workspace for Education,* EDUCATION – GOOGLE WORKSPACE (Feb. 17, 2021), https://www.blog.google/outreach-initiatives/education/google-workspace-for-education.

[7] Fred Alim et al., *Spying on Students: School Issued-Devices and Student Privacy*, ELECTRONIC FRONTIER FOUNDATION, 1, 5 (April 13, 2017), https://www.eff.org/files/2017/04/13/student-privacy-report.pdf.

position themselves as a "non-profit org" or public service and downplay their business model to teachers and students.[8] In reality, Google makes about 90 percent of its money from selling ads.[9] The collection of student data from commercial companies like Google poses privacy risks to students because of the heavy concentration of data aggregation, a lack of transparency and communication around terms and conditions, unclear security protocols, and insufficient policies regarding data archiving.[10] There is growing concern that the current laws and regulations are inadequate and unable to keep up with the current pace of technology, and that student privacy is undervalued by education policymakers.[11]

In 2018, the Federal Bureau of Investigation warned that the rapid proliferation of education technologies in schools poses privacy and safety risks for children due to the collection of not only personally identifiable information (PII), web browsing histories, IP addresses, and geolocation data, but also biometric data, behavioral information, disciplinary information, medical information,

[8] Maria Lindh & Jan Nolin, *Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education*, 15 EUR. EDUC. RES. J. 644, 650 (2016).

[9] Kurshan, *supra* note 4.

[10] Lindh & Nolin, *supra* note 8, at 649-654.

[11] Rhoades, *supra* note 1; Fedders, *supra* note 3; Alice Haston, *Keeping it Off the Record: Student Social Media Monitoring and the Need for Updated Student Records Laws*, 22 VAN. J. ENT.& TECH. L. 155 (2019); Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS*, 8 DREXEL L. REV. 339 (2015); Joanna C. Zimmerle, *Safe, Sound, and Private: Promoting Data Protection for Students,* 38 COMPUTERS IN THE SCHOOLS, 1 (2021).

academic data, and classroom data.[12] A 2020 report revealed that 408 cybersecurity attacks were launched against public K-12 education agencies during calendar year 2020, many of which involved data breaches.[13] Malicious use of student data could result in cyberbullying, identity theft, and social engineering (e.g., the psychological manipulation of divulging personal information).[14] The educational market is the third-highest target for data hackers, with data breaches of education records putting student safety at risk.[15] Recent examples include Schoolzilla, where data for over one million students was exposed,[16] and a 2017 breach with educational technology company Edmodo.[17] There was also a recent incident in Brooklyn where high school students walked out of school to protest the school's disclosure of student personal information to the Summit Learning platform.[18] In another example, Inbloom, a non-profit organization focused on personalized learning in K-12 education, was forced to shut down due to significant profit losses resulting

[12] Crime Complaint Center, Federal Bureau of Investigation, *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students I-091318-PSA,* (September 13, 2018), https://www.ic3.gov/Media/Y2018/PSA180913.

[13] Douglas A. Levin, *The State of K-12 Cybersecurity: 2020 Year in Review*, EDTECH STRATEGIES, 1, 3 (March 10, 2021), https://k12cybersecure.com/year-in-review/.

[14] *Id*. at 3-6.

[15] Rhoades, *supra* note 1, at 446.

[16] Alexi Pfeffer-Gillett, *Peeling Back the Student Privacy Pledge*, 16 DUKE L. & TECH. REV., 100, 105 (2018).

[17] Meriem El-Khattabi, Note: *Mining for Success: Have Student Data Privacy and Educational Data Mining Created a Legislative War Zone?,* U. ILL. J.L. TECH & POL'Y, 511, 520 (2017).

[18] Rhoades, *supra* note 1, at 458.

from parent outcry over the company's lack of disclosure about what data they were using and why, and the amount of student information it planned to share with third parties.[19]

Data breaches cause financial hardships for schools and parents in the event of ransomware attacks.[20] Schools are often unprepared to address data protection when it is outsourced to third-party services, and they seldom restrict companies' use of student data for marketing purposes.[21] Further, many are not ready to support Family Educational Rights and Privacy Act of 1974 (FERPA) regulations[22] related to online operator contracts.[23] Despite the heavy use of EdTech products by school districts across the nation, they often do not have the time or legal expertise needed to decipher complex privacy policy statements to ensure third-party compliance with federal and state laws.[24] Also, the Education Department has never actually withheld federal funding from a school in violation of FERPA, so loss of funding is something of an empty threat.[25] A 2013 study found most school contracts with online operators failed to list the type of student information collected or did not stop vendors from selling personal student data such as names, contact

[19] Leo Doran, *Partnership Boosts Data Privacy*, EDUCATION WEEK, February 10, 2016, at 8.

[20] Leo Doran, *Ransomware Attacks Force School Districts to Shore Up--Or Pay Up*, EDUCATION WEEK (January 11, 2017), https://www.edweek.org/technology/ransomware-attacks-force-school-districts-to-shore-up-or-pay-up/2017/01.

[21] Rhoades, *supra* note 1, at 456.

[22] 20 U.S.C. § 1232g (1974).

[23] Rhoades, *supra* note 1, at 456.

[24] Zimmerle, *supra* note 11, at 7.

[25] Rhoades, s*upra* note 1, at 470.

information, or health status.[26] Furthermore, only 25% of districts informed parents of cloud services, despite the fact that current regulations (e.g., FERPA, Protection of Pupil Rights Amendment (PPRA), and Children's Online Privacy Protection Act (COPPA)) all contain requirements related to parental notice, consent, and access to student information.[27] School district cloud service agreements mostly did not cover data security, and many allowed vendors to retain student information in perpetuity.[28] Digital technology has the potential to leave a data trail that can be available long after a student leaves school, allowing private interests to mine this data for profit and non-educational purposes.[29]

Students and teachers need to understand what rules govern their digital experience in terms of data being collected from the systems and software they use. Students have a tendency to share personal information online, and are largely unconcerned about third-party access to their data.[30] Furthermore, they may feel pressured to waive privacy rights in order to participate in classroom activities requiring the use of educational technology tools.[31] The recent COVID-19 pandemic has further exacerbated this problem. In fact, The Future of Privacy Forum (FPF) and National Education Association (NEA) recently released new recommendations for the use of video conferencing platforms in online learning, asking schools and districts to reconsider mandatory video requirements that create unique privacy and equity

[26] Reidenberg, *supra* note 2, see executive summary.
[27] *Id*.
[28] *Id*.
[29] Fedders, *supra* note 3, at 1683.
[30] Rhoades, *supra* note 1, at 454.
[31] Doran, *supra* note 19.

risks for students.[32] Teachers need more professional development training to better understand student privacy issues; the Parent Coalition for Student Privacy and the Badass Teachers Association found in a national survey of teachers that 68 percent said they had received no training in how to use education apps in ways that protected their own and their students' data, and a majority felt pressured to download some apps without understanding what data they would collect.[33] The survey report went on to recommend teachers evaluate the data privacy protections of EdTech services thoroughly before adopting them.[34] This paper will explore student privacy in relation to educational technology and uncover the loopholes in federal and state regulations that allow commercial companies to mine children's data at the expense of their privacy. California was selected as a case study to analyze a small sample of state regulations because of its reputation as a role model state in student privacy. As a leading state in creating student privacy standards, California still allows for loopholes in its regulations.

I. PRIVACY OF PERSONAL DATA

The general "privacy of personal data" is the "claim that data about oneself should not be automatically available to other individuals and organizations, and

[32] Casey Waughn, *Rethinking Video Mandates in Online Classrooms: Privacy and Equity Considerations and Alternative Engagement Methods,* STUDENT PRIVACY COMPASS (December 2, 2020), https://studentprivacycompass.org/videomandates/.

[33] Lauraine Genota, *Data Privacy*, EDUCATION WEEK (October 31, 2018), https://www.edweek.org/technology/data-privacy/2018/10.

[34] *Id.*

that, even where data are possessed by another party, the individual must be able to exercise a substantial degree of control over those data and their use."[35] Michael Zimmer suggests there are 4 groups of online activities that threaten to violate privacy, the first of which is information collection (e.g., the recording of an individual's activities) through data surveillance on the internet.[36] This often comes in the form of web cookies and tracking bugs allowing for the tracking of student actions and engagement inside of a web application leading to geolocation data, IP address data, or browser data.[37] Often, this information saves to the cloud automatically by default, without student and parental awareness or consent.[38] Persistent identifiers such as a user's IP address can be used to recognize a user over time and across vendors.[39] The second online activity is information processing or "the way information is stored, manipulated, and used after collection."[40] This can include unwanted data aggregation of personal and sensitive data allowing for behavioral tagging by advertisers.[41] Persuasive behavioral advertising is dangerous and can be used for clickbait, fake news, and predatory advertising, and can influence user self-perception and behavior.[42] Even though the data that advertisers collect is not personally identifiable, the aggregation process allows for them to

[35] Michael Zimmer, *Privacy Law and Policy*, THE INTERNATIONAL ENCYCLOPEDIA OF DIGITAL COMMUNICATION AND SOCIETY (Feb. 11, 2015), https://onlinelibrary.wiley.com/doi/10.1002/9781118767771.wbiedcs151.

[36] *Id*. at 11-13.

[37] *Id.*

[38] Alim et al., *supra* note 7, at 5.

[39] Zimmerle, *supra* note 11, at 3.

[40] Zimmer, *supra* note 35, at 2.

[41] *Id*. at 13-14.

[42] Zimmerle, *supra* note 11, at 7.

link individual pieces of information together to particular individuals and form online profiles; this "inferred data" creates predictive models based on algorithms.[43] The third online activity is information dissemination or the spreading or transfer of personal data online, which can lead to breaches of confidentiality, disclosure, appropriation, or distortion.[44] Once information is disseminated online, it is nearly impossible to remove it, so data from the past could linger and impact students' future scholarships, loan applications, or medical coverage.[45] The fourth online activity is invasion, which involves digital intrusion such as Google's Street View cameras, Facebook's tracking of online purchases, or the US National Security Agency's metadata of phone records.[46] Schools are even using remote proctoring software such as Top Hat, Kryterion, and ExamSoft to capture students' suspicious movements to guard against cheating.[47] Schools are also installing safety management platforms (SMP) such as Gaggle, Bark for Schools, and Securly that alert them to bullying or suicide risks.[48]

[43] Rhoades, *supra* note 1, at 455.
[44] Zimmer, *supra* note 35, at 14-15.
[45] Zimmerle, *supra* note 11, at 7.
[46] Zimmer, *supra* note 35, at 15-16.
[47] Lindsey Barrett, *Rejecting Test Surveillance in Higher Education*, 1 Mich. St. L. Rev. (forthcoming 2023).
[48] Harold J. Krent, John Etchingham, Alec Kraus & Katharine Pancewicz, *AI Goes to School—Implications for School District Liability*, 67 BUFF. L. REV.1329, 1331 (2019).

REVIEW OF STUDENT PRIVACY REGULATIONS

A. Historical Overview of Key Regulations

Most other industrialized countries support more comprehensive privacy and data protection measures than the United States does.[49] This section gives a historical overview of the key federal and California regulations impacting student privacy in the digital age. For the complete list, see Table 1 and Table 2. Also, for the list of key Supreme Court Cases, see Table 3.

Table 1: Federal Regulations Related to Student Privacy

Law/Act/ Regulation	Year Took Effect	Key Points	Loophole/Weakness
Family Educational Rights and Privacy Act of 1974 (FERPA)	1974	Protects students and their families by ensuring the privacy of student educational records; educational records are agency or institution-maintained records containing personally identifiable student and educational data	Overly broad definition of "educational record;" 2011 amendments permitted schools to disclose data to third parties (as authorized educational partners) that exceeds the traditional school records FERPA was designed to protect; no penalty for commercial

[49] Zimmer, *supra* note 35, at 4.

			companies violating FERPA
Protection of Pupil Rights Amendment (PPRA)	1978	Applies to programs that get their funding from the United States Department of Education and protects students from having to reveal personal information in certain surveys without parental consent	Parental consent requirement only applies when the surveys request certain information, such as political affiliations, mental and psychological disorders, and sexual attitudes
Communications Decency Act of 1996	1996	Title V of the *Telecommunications Act of 1996* is an attempt to prevent minors from gaining access to sexually explicit materials on the Internet	Section 230 protects online platforms from legal liability for any content created by their users
Children's Online Privacy Protection Act (COPPA)	2000	Governs the online collection of personal information from children under the age of 13; parental consent is required	FTC issued exception for data disclosed by schools to online operators acting as authorized educational partners- puts the burden for this back on FERPA
Children's Internet Protection Act (CIPA)	2000, updated in 2011	K-12 schools and libraries filter minors' internet access and monitor their online activities to protect	By relying on filtering software, schools delegate some decisions to private companies about what is

		them from harmful online content like pornography	appropriate[50]
European Union General Data Protection Regulation of 2018 (GDPR)	2018	Replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy; stricter controls on privacy than any U.S. laws - includes special protections for children, such as requiring parental consent prior to processing childrens' data[51]	N/A

50 Martha M. McCarthy, Suzanne E. Eckes & Janet R. Decker, Legal Rights of School Leaders, Teachers, and Students 89 (8th ed. 2019).

51 Laura Hautala, *CCPA is Here: California's Privacy Law Gives You New Rights,* CNET (January 3, 2020), https://www.cnet.com/tech/services-and-software/ccpa-is-here-californias-privacy-law-gives-you-new-rights/.

B. Family Educational Rights and Privacy Act of 1974 (FERPA)

The first law protecting student privacy was the *Family Educational Rights and Privacy Act of 1974* (FERPA)[52] to regulate schools' practices of releasing student information and to mandate more parental oversight and transparency.[53] Educational records were defined as information directly related to a student and maintained by an educational agency or institution or by a person acting for such agency or institution.[54] FERPA was introduced by Senator James Buckley and signed into law by President Ford, but Congress has amended FERPA nine times since its enactment due to changing technologies.[55] This law is considered the birth of federal privacy rights for students, and FERPA is still the most widely used federal education law protecting student privacy in the United States.[56] However, the statute is not sufficiently protective of student information given today's technological advances, as it is unclear whether students' personally identifiable information (PII) via school surveillance technologies is considered part of the educational record.[57] In 2011, the Education Department issued amendments to FERPA defining "authorized representative" to include non-governmental actors as representatives of schools, widening the scope of who

[52] *Supra* note 22.

[53] Rhoades, *supra* note 1, at 449.

[54] *Supra* note 22, at section 4A.

[55] Katelyn Ringrose, *Data Collection in Schools: Privacy Implications for K-12 Students Under a Weakened FERPA*, 16 DARTMOUTH L. J., 130, 132 (2018).

[56] Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences,* 44 SETON HALL LEGIS. J., 515, 519 (2020).

[57] Rhoades, *supra* note 1, at 477.

could access student records.[58] FERPA's overly broad definition of "educational record," along with the 2011 amendment that permits schools to disclose data to third parties as educational partners (in essence characterizing EdTech companies as the same as "school officials"), creates a loophole for the EdTech industry.[59]

PII can be disclosed from education records without student or parental consent into integrated data systems that link data from multiple government agencies under two exceptions: the audit and evaluation exception of federal or state education programs, and the school official exception.[60] Under the "school official" exception created in 2008, schools may now disclose education records to a service provider without consent from the parent or eligible student if the service provider performs a service that would otherwise use school employees, is under the "direct control" of the institution for using and maintaining education records, and is contractually prohibited from using education records other than as specified.[61] *Gonzaga University v. Doe* (2002)[62] established that there is no private right to sue, so students are not able to file private claims of action for FERPA violations, but they may file a

[58] Ringrose, *supra* note 55, at 136.

[59] Fedders, *supra* note 3, 1683–84.

[60] PRIVACY TECH. ASSISTANCE CTR., U.S. DEP'T OF EDUC., INTEGRATED DATA SYSTEMS AND STUDENT PRIVACY 7 (2017), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/IDS-Final_0.pdf.

[61] Bart W. Huffman et al., *Protecting Student Data: Student Privacy Requirements and Guidelines for Post-Secondary Institutions*, REED SMITH (Oct. 12, 2017), https://www.reedsmith.com/en/perspectives/2017/10/protecting-student-data-student-privacy-requirements-and-guidelines

[62] 536 U.S. 273 (2002).

complaint with the Education Department.[63] Students can also sue under a relevant state law, but not all states have such laws.[64] In 2014, the Education Department released guidance on how to interpret and apply FERPA in the digital age.[65] One example from the new guidelines indicates that a provider may not use data about individual student preferences gleaned from scanning student content to target ads because this does not constitute a legitimate educational interest.[66] However, the EdTech companies are able to collect and store information that goes beyond the traditional "school records" that FERPA was designed to protect, including indirect and inferred data, without requiring parental consent before disclosure.[67] The ability of online applications to collect student engagement data unrelated to a student's education exceeds what FERPA was designed to protect and is not considered "directory information."[68] There are no repercussions or financial penalties for EdTech companies who violate FERPA, since penalties are limited to the withholding of federal funding to schools or educational institutions.[69]

In *Owasso Independent School District v. Falvo* (2002)[70], the U.S. Supreme Court ruled that peer grading does not qualify as educational records under FERPA because they were not "maintained," as the student graders only handled the items for a few

[63] Rhoades, *supra* note 1, at 451–52.
[64] Ringrose, *supra* note 55, at 142.
[65] *Department Releases New Guidance on Protecting Student Privacy While Using Online Educational Services,* U.S. DEP'T OF EDUC. (Feb. 25, 2014), https://www.ed.gov/news/press-releases/department-releases-new-guidance-protecting-student-privacy-while-using-online-e
[66] *Id.*
[67] Rhoades, *supra* note 1, at 455.
[68] *Id*. at 459.
[69] *Id*. at 467.
[70] 534 U.S. 426 (2002).

moments and schools must demonstrate a more permanent intent to retain the file.[71] This has implications for the type of student data being collected by third parties that is not directly related to student education because it lacks the intent of permanency and can be considered temporary (and thus outside of FERPA regulation).[72] Also, the finding that peer grades are not education records because school officials did not capture the data or create it with the intent of retaining it in a permanent file is important. Cloud servers offer unlimited storage, and data generated and shared between users instead of with schools (e.g., emails or chat) evades FERPA requirements because it did not originate inside of an educational context.[73] Similarly, in *S.A. v. Tulare County Office of Education* (2009)[74], the ruling was that school emails stored on individual teachers' hard drives were not education records because they were not centrally located. Since those emails had not been printed and placed in the student's file, the court held there was no FERPA violation.[75]

C. Protection of Pupil Rights Amendment (PPRA)

[71] Daniel R. Dinger, *Johnny Saw My Test Score, So I'm Suing My Teacher: Falvo v. Owasso Independent School District, Peer Grading, and a Student's Right to Privacy under the Family Education Rights and Privacy Act*, 30 J.L & EDUC. 575, 616, (2001).

[72] Rhoades, *supra* note 1, at 464.

[73] *Id*. at 464-465.

[74] S.A. v. Tulare County Office of Education, No. CV F 08-1215, 2009 WL 30298 (E.D. Cal. Sep. 24, 2009)

[75] Julie Underwood, *Under the Law: You Say 'Records,' and I Say 'Data'*, 98 PHI DELTA KAPPAN, 74, 74 (2017).

The Protection of Pupil Rights Amendment (PPRA),[76] which was passed in 1978 and amended in 2002 as part of the No Child Left Behind Act, regulates student participation in surveys or evaluations that reveal specific types of information.[77] It restricts a school's ability to disclose, use, or sell student information that falls under the statute for marketing purposes without first notifying the student's parents and presenting them with the opportunity to opt-out.[78] It applies to educational agencies that receive federal funding, and it does not contain a private right of action.[79] Exceptions to PPRA apply when "the collection, disclosure, or use of personal information collected from students [is] for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions."[80] The main distinction between PPRA and FERPA is that PPRA is involved only when a school collects certain types of personal information from a student, while FERPA protects a student's education records from disclosure.[81] PPRA was created to work in tandem with FERPA to provide parents and students additional protection.[82] The parental consent requirement, however, applies only when the surveys

[76] Pub. L. No. 95-561, 92 Stat. 2143 (1978) (codified as amended at 20 U.S.C § 1232h).

[77] Emily Gold Waldman, *Show and Tell?: Students' Personal Lives, Schools, and Parents*, 47 CONN. L. REV. 699, 704–705 (2015).

[78] Dylan Peterson, *EdTech and Student Privacy: California Law as a Model*, 31 BERKELEY TECH. L.J. 961, 983 (2016).

[79] *Id.*

[80] 20 U.S.C. § 1232h(c)(2)(C)(i).

[81] Peterson, *supra* note 78, at 983.

[82] Loree Varella, *When it Rains, it Pours: Protecting Student Data Stored in the Cloud*, 42 RUTGERS COMPUT. & TECH. L.J. 94, 103 (2016).

request certain information, such as political affiliations, sexual attitudes, family problems, and other personal matters.[83] Many schools use student information in undefined and unknown ways, which would therefore fall outside the PPRA parental consent regulation.[84] Due to the restricted subjects and the requirement that the material be obtained with Board of Education funding, PPRA's, and by extension, FERPA's, application to student information processed through cloud computing is limited.[85]

D. Children's Online Privacy Protection Act (COPPA)

In 2000, Congress enacted the Children's Online Privacy Protection Act (COPPA)[86] to regulate online operators' collection and use of children's personally identifiable information (PII) in response to FTC findings that most websites marketed to children collected personal information and did not post an adequate privacy policy.[87] COPPA required websites to provide notice and receive parental consent prior to collection from children under the age of thirteen.[88] The enforcement agency is the Federal Trade Commission (FTC), who amended COPPA regulations in 2012 to include persistent identifiers such as cookies or fingerprints, IP address and geolocation, and media

[83] Waldman, *supra* note 77, at 704–705.
[84] Varella, s*upra* note 82, at 103.
[85] *Id.*
[86] Children's Online Privacy Protection Act of 1998, Pub. L. no. 105-277, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501–6505).
[87] Tianna Gadbaw, *Legislative Update: Children's Online Privacy Protection Act of 1998,* 36 CHILD. LEGAL RTS. J. 228, 228 (2016)
[88] *Id.*

files such as photos and video recordings.[89] The statute requires operators of children's websites to post privacy policies outlining what information is collected from children by the operator, how the operator uses the information, and the operator's disclosure practices.[90] However, the FTC excludes schools from COPPA enforcement, claiming that FERPA regulates school data disclosure.[91] This acts as a loophole if companies contract directly with schools, and allows commercial companies to operate without FTC oversight.[92] An analysis of free children's mobile apps' compliance with COPPA in 2018 revealed that the majority violated COPPA, due to their use of third-party software development kits (SDK) that transmitted sensitive data.[93]

Recently, the Federal Trade Commission (FTC) announced changes to update its COPPA Frequently Asked Questions (FAQs) to include companies contracting with schools: they must not state in their "Terms of Service or anywhere else" that schools are responsible for complying with COPPA because it is the responsibility of the Operator.[94] Also, the FTC provided more detailed descriptions of operators' and schools' obligations under the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Protection

[89] Rhoades, *supra* note 1, at 452–453.
[90] Fedders, *supra* note 3, at 1684.
[91] *Id*.
[92] Rhoades, *supra* note 1, at 471.
[93] Primal Wijesekera et al., *Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, 3 PROC. PRIV. ENHANCING TECHS. 63 (2018).
[94] *The Federal Trade Commission Updates to the COPPA FAQ*, FUTURE OF PRIV. F. (Oct. 21, 2020), https://fpf.org/blog/ftc-updates-coppa-faqs/.

of Pupil Rights Amendment (PPRA).[95] Still, since there is no automated system in place to formally track vendors whose privacy policies are not in compliance with COPPA, the FTC largely fails to act fast enough to catch noncompliant vendors who sell student data.[96]

E. California Regulations

All fifty states have separate and different student privacy protection laws, so a thorough review of state regulations is outside the scope of this paper. California has "long been considered a leader in privacy law,"[97] but despite being recognized as a leader in setting K-12 school privacy standards, even California is not doing enough to protect student privacy. California was selected as a case study to analyze a small sample of state regulations because of its reputation as a role model state in student privacy. For a summary of the key California regulations, see Table 2. In 2015, the *Privacy Rights for California Minors in the Digital World* (2015)[98] was enacted, which restricts certain types of marketing to CA minors and allows those who are registered users of an operator's site or service to request removal of personal content posted to a website, social media profile, or online service while under the age of eighteen.[99] In 2016, the *Student Online Personal*

[95] *Id.*
[96] Zimmerle, *supra* note 11, at 4.
[97] Peterson, *supra* note 78, at 972.
[98] S.B. 568, 2013 Leg. (Cal. 2013).
[99] *New California Privacy Law for Minors Has Taken Effect as of January 1, 2015*, COOLEY LLP (Jan. 5, 2015), https://www.cooley.com/news/insight/2015/new-california-privacy-law-for-minors-has-taken-effect-as-of-january-1-2015

Information Protection Act (SOPIPA) took effect.[100] This California law prohibits operators such as educational websites, online services, and mobile applications from sharing student data for targeted advertising for non-educational purposes.101 It also prohibits online service providers from creating K-12 student profiles for commercial purposes and forbids companies from selling student information.102 Under SOPIPA, K-12 mobile and online service operators must establish security measures and delete student information at the request of a school or district.103 The law does permit K-12 mobile and online service operators to use deidentified student information to improve educational products.104 SOPIPA is silent as to the standard that operators will be held to in terms of the level of personal data deidentification it requires, so one concern is that SOPIPA allows companies too much latitude in their use of deidentified data.105 Unfortunately, general audience websites like Google are not bound by the law, since they don't target K-12 students specifically.106

California was the first state to ban operators of education websites and online services from targeted advertising to students, but this term was never clearly

[100] S.B.1177, 2014 Leg. (Cal. 2014).

[101] *California's Student Online Personal Information Protection Act is the First State Law to Comprehensively Address Student Privacy,* COOLEY LLP (October 9, 2014), https://www.cooley.com/news/insight/2014/californias-student-online-personal-information-protection-act-is-the-first-state-law-to-comprehensively-address-student-privacy.

[102] Jordan Clark, *What is SOPIPA?*, EDLINK (April 1, 2020), https://ed.link/community/what-is-sopipa/.

[103] *Id.*

[104] COOLEY LLP, supra note 101.

[105] Peterson, supra note 78, at 991–992.

[106] *Id.* at 964–965, 964 n.18.

defined, leaving both companies and students confused about what was not allowed.[107] Marco Crocetti argues that SOPIPA's advertising prohibitions raise serious First Amendment concerns because it is overly broad and more restrictive than necessary to advance California's alleged governmental objectives.[108] It closes off a potentially large revenue source that could be used towards improving education, and is an unconstitutional restriction on commercial speech. Suggested alternatives are consent exceptions, industry self-regulatory regimes (e.g., Student Privacy Pledge), and advertising filtering regimes.[109]

In 2020, the *California Consumer Privacy Act* (CCPA)[110] took effect to regulate data privacy in California. It was modeled after the European Union General Data Protection Regulation of 2018 (GDPR),[111] but is a more restrictive version.[112] The GDPR protects the privacy of European Union (EU) residents' data, including that of American students who are living in the EU. However, EU students who

[107] RACHAEL STRICKLAND & LEONIE HAIMSON, THE STATE STUDENT PRIVACY REPORT CARD: GRADING THE STATES ON PROTECTING STUDENT DATA PRIVACY 9 (Jan. 2019), https://www.studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf.

[108] Marco Crocetti, *Targeted Advertising and the First Amendment: Student Privacy vs. Protected Speech*, 25 CATHOLIC UNIV. J.L. & TECH. 23, 39 (2016).

[109] *Id.*at 50.

[110] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.192 (2018).

[111] 2016 O.J. (L 119) 1. [hereinafter GDPR].

[112] Noah Ramirez, *Comparing CCPA and GDPR: 8 Key Differences Between the Privacy Laws*, OSANO (Sep. 29, 2020), https://www.osano.com/articles/gdpr-vs-ccpa

move to the US to attend school are not protected.[113] The GDPR contains several rights that go beyond any current laws in the United States, such as the right of data subjects to have their data erased, the right of data subjects to receive their personal data in a commonly used format and have it transmitted to another data controller, and the right not to be subject to an adverse decision based solely on the application of artificial intelligence.[114] Also, it requires companies to receive consent to collect data or to have some other valid reason for collecting user information, and it requires companies to minimize the data collected.[115] The CCPA broadly defines personal information to include biometric data, geolocation, household purchase data, and sleep habits.[116] The CCPA offers the following privacy rights: (1) "to know what personal information is being collected about them;" (2) "to know whether their personal information is sold or disclosed and to whom;" (3) "the right…to say no to the sale of personal information;" (4) "to access their personal information;" and 5) "to equal service and price, even if they exercise their privacy rights."[117] CCPA expands requirements on companies collecting PII from children under 13 to also include 13- to 16-year-olds, but it only applies to the sale of (not the sharing of) data, which allows companies to still track user behavior and link it to other accounts without technically "selling" the

[113] *Does GDPR Apply to EU Citizens Living in the US?,* HIPPA JOURNAL (May 11, 2018), https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/.

[114] Mark A. Rothstein and Stacey A. Tovino, *California Takes the Lead on Data Privacy Law*, 49 HASTINGS CTR. REP., 4, 5 https://onlinelibrary.wiley.com/doi/epdf/10.1002/hast.1042.

[115] Hautala, *supra* note 51.

[116] Rothstein, *supra* note 114, at 4.

[117] CCPA § 1798.100.

data.[118] Also, data can still be sold if PII is removed, and there are no provisions to address if a parent or student asks a company to delete PII that schools are required to collect and maintain for federal/state reporting.[119]

Table 2: California Regulations Related to Student Privacy

Law/Act/ Regulation	Year Took Effect	Key Points	Loophole/Weakness
Privacy Rights for California Minors in the Digital World	2015	Restricts certain types of marketing to minors. It also allows minors who are registered users of an operator's site or service to request removal of personal content	N/A
Student Online Personal Information Protection Act (SOPIPA)	2016	CA act that prohibits operators (e.g., educational websites, online services, online applications, and mobile applications) from sharing student data and using that data for targeted advertising to students for a	Google Search (and other general audience websites/services) not bound by this law, since it doesn't target K-12 students; the term "targeted advertising" was never clearly defined

[118] Micah Castelo, *How the CCPA Affects California School Districts*. EDTECH: FOCUS ON K-12 (July 15, 2020), .

[119] *Id.*

		non-educational purpose	
California Consumer Privacy Act of 2018 (CCPA)	2020	Leading state statute for an express private right of action for data breaches resulting from a failure to implement reasonable data security measures; does not regulate non-profits. Broadly defines personal info to include biometric data, geolocation, household purchase data, sleep habits. Consumers can request the info collected, to delete personal info, or to opt out of the sale of their personal info	Extends requirements on companies collecting PII from children under 13 to include 13- to 16-year-olds, but only applies to the sale of data (not the sharing of), doesn't include deidentified data, and doesn't make provision to address if a parent or student asks a company to delete PII that schools are required to collect and maintain for federal/state reporting[120]

I. OVERVIEW OF KEY CASES

A. Supreme Court Cases

The U.S. Supreme Court has not yet explicitly addressed a school's ability to regulate student internet activity in the context of big data and educational data mining.[121] With technology changing how and where information is stored and accessed by schools, this

[120] *Id.*
[121] Haston, *supra* note 11, at 161.

needs to be addressed. A few constitutional amendments have been influential in interpreting privacy cases. The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures of their private effects, papers, homes, and bodies; and it has been extended somewhat to students through case law.[122] The "due process" clause in the Fourteenth Amendment of the United States Constitution indicates no person shall be deprived of life, liberty, or property without due process of law.[123] And, the First Amendment promises free speech, including the allowance of online platforms to curate their own content. Just as the First Amendment protects newspaper editors who cannot be compelled to publish a particular content item, the same concept applies to search engines, which cannot be compelled to include certain links.[i] This section gives a historical overview of the key Supreme Court cases directly or indirectly related to student privacy in the digital age, all with some implications for privacy rights or how student information is collected, processed, or disseminated via cloud computing. For the complete list, see Table 3.

Table 3: Key Supreme Court Cases Related to Student Privacy

Case	Year	Key Points
Katz v. United States	1967	4th Amendment protection against unreasonable searches and seizures requires police to obtain a search warrant in order to wiretap a public pay phone

[122] Joanna Tudor, *Legal Implications of Using Digital Technology in Public Schools: Effects on Privacy*, 44 J.L. & EDUC. 287, 335 (2015).

[123] McCarthy, *supra* note 50, at 9.

Tinker v. Des Moines Independent Community School District	1969	Students do not lose their 1st Amendment rights to freedom of speech when they step onto school property
Doe v. McMillan	1973	Invasion of privacy case against D.C. school system for the dissemination of a congressional report that included identification of students in derogatory contexts (e.g., copies of test papers, disciplinary reports, and evaluations with the students' names still on them)
Whalen v. Roe	1977	Ruled that the reporting and record-keeping requirements of the *New York State Controlled Substances Act* did not violate a constitutionally protected 'zone of privacy' through collecting patient's name, address, and age - but recognized the constitutional right to information privacy
New Jersey v. T.L.O.	1985	The search of T.L.O.'s purse for cigarettes was a reasonable warrantless search
Reno v. ACLU	1997	Certain provisions of the 1996 *Communications Decency Act* (intended to protect minors from unsuitable internet material) violate the First and Fifth Amendments
Owasso Independent School District v. Falvo	2002	The practice of peer grading does not violate FERPA because they were not maintained and student graders were not acting for an educational institution within FERPA

Gonzaga Univ. v. Doe	2002	Individuals and organizations cannot sue to enforce FERPA
United States v. American Library Association	2003	American Library Association unsuccessfully challenged the *Children's Internet Protection Act*, claiming that requiring public libraries to install internet filtering software on their computers in order to qualify for federal funding restricted the first Amendment rights of their patrons
Safford Unified School District v. Redding	2009	Strip search of 8th grader ruled as a violation of her 4th Amendment right to be free of unreasonable searches and seizures
Riley v. California	2014	Cell phone discovered through a search was found to violate 4th Amendment right to be free from unreasonable searches and seizures

One early case related to information collection practices is *Katz v. United States* (1967),[124] which made government wiretapping of communication subject to the Fourth Amendment's warrant requirements. In *Tinker v. Des Moines Independent Community School District* (1969),[ii] the Supreme Court ruled that a prohibition against the wearing of armbands to protest the Vietnam War in public school violated students' First Amendment rights to freedom of speech when they step onto school property. This is important because, later, the Supreme Court extended these rights to include Fourth Amendment protections.[125] In *Doe v.*

[124] Katz v. United States, 389 U.S. 347 (1967).
[125] Tudor, *supra* note 122, at 332.

McMillan (1973),[126] parents of District of Columbia (D.C.) school children were seeking damages and declaratory and injunctive relief for invasion of privacy that they claimed resulted from the dissemination of a congressional report, on the D.C. school system, that included identification of students in derogatory contexts. The information included copies of test papers, disciplinary reports, and evaluations with the students' names still on them; and it had Fourteenth Amendment implications because it set limits on the immunity of civil government officials.[127] In *Whalen v. Roe* (1977),[128] the Supreme Court ruled that the reporting and record-keeping requirements of the New York State Controlled Substances Act did not violate a constitutionally protected "zone of privacy" through collecting patient's name, address, and age; but recognized the constitutional right to information privacy. In *New Jersey v. T.L.O.* (1985),[129] a student was charged with drug offenses based on items she had in her purse. The search of her purse for cigarettes was instigated because she was caught smoking in the bathroom, and it was ruled a reasonable warrantless search that did not violate the Fourth Amendment. The case is important because it implied that Fourth Amendment protections still apply to students but are limited in scope.[130]

In *Reno v. ACLU* (1997),[131] the Supreme Court ruled that certain provisions of the 1996 Communications Decency Act[132] (intended to protect

[126] Doe v. McMillan, 412 U.S. 306 (1973).
[127] Vance, *supra* note 56, at 517–520.
[128] Whalen v. Roe, 429 U.S. 589 (1977).
[129] New Jersey v. T.L.O., 469 U.S. 325 (1985).
[130] Tudor, *supra* note 122, at 336.
[131] Reno v. ACLU, 521 U.S. 844 (1997).
[132] Communications Decency Act of 2016, 47 U.S.C.§ 230 (1996).

minors from unsuitable internet material) violate the First and Fifth Amendments by being overly broad and vague in their definitions of the types of internet communications which they criminalized. In *Owasso Independent School District v. Falvo* (2002),[133] as discussed previously, the U.S. Supreme Court ruled that peer grading does not qualify as educational records under FERPA because they were not "maintained," as the student graders only handled the items for a few moments and schools must demonstrate a more permanent intent to retain the file.[134] In *Gonzaga University v. Doe* (2002),[135] the Supreme Court ruled that individuals and organizations cannot sue to enforce FERPA. A student attempted to sue a private university for damages to enforce provisions of FERPA, but FERPA's confidentiality provisions did not have the clear and unambiguous terms that the creation of individual rights required. The decision effectively closed the courts to the students, parents, and newspapers harmed by FERPA errors. The result is that schools may question why they should comply with FERPA if there is no enforcement.[136] In *United States v. American Library Association* (2003),[137] the American Library Association unsuccessfully challenged the Children's Internet Protection Act,[138] claiming that requiring public libraries to install internet filtering software on their computers in order to qualify for federal funding restricted the First Amendment

[133] Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426 (2002).

[134] Dinger, *supra* note 71, at 581–582.

[135] Gonzaga Univ. v. Doe, 536 U.S. 273 (2002).

[136] Zach Greenberg, *Let FERPA be FERPA*, 64 CHRON. OF HIGHER EDUC., (Jan. 14, 2018).

[137] United States v. Am. Libr. Ass'n, 539 U.S. 194 (2003).

[138] Children's Internet Protection Act (CIPA), 20 U.S.C. § 9134(f) (2018).

rights of their patrons. In *Safford Unified School District v. Redding* (2009),[139] an eighth grader was strip-searched by school officials on the basis of a tip by another student that she might have ibuprofen on her person in violation of school policy. This was ruled as a violation of her Fourth Amendment right to be free of unreasonable searches and seizures. This case is important because it "extends a reasonable expectation of privacy to students regarding their personal belongings."[140] In *Riley v. California* (2014),[141] the evidence admitted at trial from a gang member's cell phone, discovered through a search, was found to violate his Fourth Amendment right to be free from unreasonable searches. This decision "stands for the conclusion that the information on a cell phone is entitled to more protection than other common items found in someone's pocket or purse."[142]

B. Other Cases

Several more recent cases continue to shed light on the current state of online student privacy protection (see Table 4 for the full list). In *S.A. v. Tulare County Office of Education* (2009),[143] it was ruled that emails stored on individual teachers' hard drives are not education records until the document is centrally located. This implies that data collected online that is not maintained by the school is not covered under FERPA.[144] In 2014, a consolidated, multi-district litigation involving seven

[139] Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364 (2009).

[140] Tudor, *supra* note 122, at 136.

[141] Riley v. California, 573 U.S. 373 (2014).

[142] Tudor, *supra* note 122, at 335.

[143] S.A. v. Tulare Cnty. Off. of Educ., NO. CV F 08-1215 LJO GSA, 2009 WL 30298 (E.D. Cal. Jan. 6, 2009).

[144] Rhoades, *supra* note 1, at 453.

individual class lawsuits against Google, Inc. was combined into the case *In re Google, Inc. Gmail Litig*.[145] The plaintiffs challenged Google's operation of Gmail under state and federal anti-wiretapping laws, and argued for a COPPA violation. Among the plaintiffs were two students who were required to use Gmail accounts through their institution's adoption of Google Apps for Education (GAFE). Google admitted to scanning email messages from student users of GAFE and treating them like regular Gmail consumers. The plaintiffs alleged they used the information to build user profiles for targeted advertising in not just GAFE but other Google products like Google Search and YouTube.[146] Some emails could contain sensitive information, such as a child's disability status or mental health, which may now be forever associated with them.[147] In 2014, *Electronic Privacy Information Center v. United States Department of Education*[148] involved a complaint filed with the FTC that Google was using information collected from GAFE users who go outside GAFE to use other Google services within the Chrome browser, in ways that violate the *Student Privacy Pledge* Google had signed.[149] The Pledge only covers information collected within an educational service.[150] The suit prompted U.S. MN Senator Al

[145] *In re* Google, Inc. Gmail Litig., 936 F. Supp. 2d 1381, (J.P.M.L. 2013).

[146] Benjamin Herold, *Google Under Fire for Data Analysis of Student Emails*, 33 EDUC. WEEK, (Mar. 26, 2014).

[147] *Id.*

[148] Elec. Priv. Info. Ctr. v. U.S. Dep't of Educ., 48 F.Supp.3d 1 (D.C.C. 2014).

[149] Benjamin Herold, *Google Acknowledges Data Mining Student Users Outside Apps for Education,* 35 EDUC. WEEK, 12, (Feb. 17, 2016), https://www.edweek.org/technology/google-acknowledges-data-mining-student-users-outside-apps-for-education/2016/02.

[150] *Id.*

Franken to write a letter asking for more details on the privacy settings and uses for data within the GAFE suite of tools and what PII was being collected on individual students.[iii] Google responded that it collects names, email addresses, telephone numbers, device information, and IP addresses.[151] Even though it has agreed to not use personal information from GAFE users to target ads, anything subsequently used outside of GAFE is not protected.[152]

Table 4: Other Recent Court Cases Related to Student Privacy in the Digital Age

Case	Year	Key Points
S.A. v. Tulare County Office of Education	2009	Emails stored on individual teachers' hard drives are not education records until the document is centrally located; implies that data collected online that is not maintained by the school is not covered under FERPA
In re Google Inc. Gmail Litig	2013	Google admitted to scanning email messages from student users of GAFE and treating them like regular Gmail consumers
Electronic Privacy Information Center v. United States Department of Education	2014	Google was using information collected from GAFE users who go outside GAFE to use other Google services within the Chrome browser in ways that violate the *Student Privacy Pledge* Google had signed
Google Inc. v. Hood	2016	Google's policies and practices for online tracking of student data

[151] Herold, *supra* note 151.
[152] *Id.*

		was unclear; Google tracks and stores student data for advertising purposes when students use outside services
FTC v. Musical.ly	2019	Musical.ly (now TikTok) app illegally collected personal information about children under 13, such as email addresses, names, and schools without parental consent in violation of COPPA
FTC; and People of the State of NY v. Google LLC and YouTube, LLC	2019	Google settled with the Federal Trade Commission and New York's attorney general, for violating COPPA, to pay $170 million and make changes to its YouTube procedures for child-directed content
Kylie S. v. Pearson PLC	2020	Pearson neglected to implement security measures that would have thwarted hackers who slipped past Pearson's defenses and gained access to the data hosted on AIMSweb
New Mexico ex rel. Balderas v. Google LLC	2020	Google has used GSFE to spy on New Mexico students' online activities for its own commercial purposes, without notice to parents and without attempting to obtain parental consent (COPPA violation)

In *Google, Inc. v. Hood* (2016),[153] the Mississippi Attorney General James M. Hood, III, filed a lawsuit claiming Google's policies and practices for online

[153] Google, Inc. v. Hood, 822 F.3d 212 (5th Cir. 2016).

tracking of student data was unclear.[154] Furthermore, Google tracks and stores student data for advertising purposes when students use outside services like Google Maps or YouTube, despite Google's contract stating otherwise.[155] Google alleged that Hood's investigation violates Google's immunity under the Communications Decency Act (CDA),[156] its Fourth Amendment rights, and the First Amendment rights of Google and its users.[157] In *FTC v. Musical.ly* (2019), the FTC reached a $5.76 million settlement with Musical.ly, a popular video social network now known as TikTok, over accusations that the company's app illegally collected personal information about children under 13, such as email addresses, names, and schools, without parental consent, in violation of COPPA.[158] When asked by some parents to delete videos and other data, the site refused.[159] Specifically, TikTok violated COPPA by "failing to post a privacy policy on its online service providing clear, understandable, and complete notice of its information practices; failing to provide direct notice of its information practices to parents; failing to obtain verifiable parental consent prior to collecting, using, and/or disclosing personal information from children; failing to delete personal information at the request of parents; and retaining personal information longer than reasonably necessary

[154] Benjamin Herold, *Miss. AG Sues Google Inc. Over Student-Data Privacy*. 36 EDUC. WEEK, 4 (Jan. 25, 2017).

[155] Hood, 822 F.3d 212.

[156] 47 U.S.C.§ 230.

[157] Hood, 822 F.3d 212.

[158] *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That It Violated Children's Privacy Law*, FED. TRADE COMM'N (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

[159] *Id.*

to fulfill the purpose for which the information was collected."[160] TikTok user accounts were previously public by default, and adults were able to contact users regardless of their age.[iv] The FTC alleged that TikTok had "actual knowledge" they were collecting personal information from kids.[161]

Also in 2019, in the case *FTC and State of New York vs. Google LLC and YouTube, LLC,* Google settled with the Federal Trade Commission and New York's attorney general, for violating COPPA, to pay $170 million and make changes to its YouTube procedures for child-directed content.[162] The YouTube video sharing service, owned by Google, illegally collected personal information from children without their parents' consent.[163] COPPA imposes obligations on online services that have actual knowledge that they are collecting, using, or disclosing personal information from children under 13,[164] and the case determined that YouTube did have this "actual knowledge." If a child-directed content provider directly communicates the child-directed nature of its content to the third-party operator, or a representative of the third-party operator's ad network recognizes the child-directed nature of the content, this is considered having actual

[160] Lesley Fair, *Largest FTC COPPA Settlement Requires Musical.ly to Change its Tune,* FED. TRADE COMM'N, at para 8 (Feb. 27, 2019, 12:57 PM), https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its.

[161] Fair, *supra* note 163.

[162] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[163] *Id.*

[164] Zimmerle, *supra* note 11, at 3.

knowledge.[165] YouTube met both criteria, since it actively marketed itself as a top destination for kids.[166] The case classified YouTube as collecting personal information from children on behalf of individual creators, and placed new requirements on YouTube and content creators to self-identify their child-directed content on the YouTube platform.[167] YouTube also had to notify channel owners that their child-directed content may be subject to the COPPA obligations, and provide annual training about complying with COPPA for employees.[168] The case is significant because it did not allow YouTube to slide under COPPA's "internal operations" exception, which permits operators to collect persistent identifiers from children without parental consent if the identifiers are only used for internal operations.[169]

In 2020, a group of Illinois and Colorado parents initiated the case *Kylie S. v. Pearson PLC,* 475 F. Supp. 3d 841 (2020).[170] They alleged that Pearson neglected to implement security measures that would have thwarted hackers from gaining access to the data hosted

[165] *See also* Natasha Singer & Kate Conger, *Google is Fined $170 Million for Violating Children's Privacy on YouTube*, THE NEW YORK TIMES (Sept. 4, 2019), https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html (describing the settlement between YouTube and the FTC).

[166] *See id.*

[167] *See id.*

[168] *Id.*

[169] Sara Collins, *FTC Reaches Landmark Settlement Regarding Kids' Privacy, Clarifies Platforms' and Video Creators' COPPA Obligations for Child-Directed Content, FUTURE OF PRIV. F.* (Sept. 9, 2019), https://fpf.org/blog/ftc-reaches-landmark-settlement-regarding-kids-privacy-clarifies-platforms-and-video-creators-coppa-obligations-for-child-directed-content/.

[170] Kylie S. v. Pearson PLC, 475 F. Supp. 3d 841 (2020).

on AIMSweb, in violation of *FERPA*.[171] Pearson is an educational testing platform that stores students' names, emails, and birthdays, among other information.[172] In *New Mexico ex rel. Balderas v. Google, LLC*, 489 F. Supp. 3d 1254 (D.N.M. 2020),[173] the state of New Mexico alleged that Google had used its G Suite for Education (GSFE) to spy on New Mexico students' online activities for its own commercial purposes, without notice to parents and without attempting to obtain parental consent.[174] This is a violation of COPPA, since Google failed to provide direct notice to, and obtain verifiable consent directly from, parents before collecting students' personal data from school-issued email accounts.[175] Specifically, Google was accused of tracking students' physical locations, web-browsing histories, and personal contact lists.[176] Google used, as its defense, FTC guidelines stating that schools can act as intermediaries between companies and parents to obtain parental consent.[177] The ruling was in favor of Google, saying that Google could rely on individual schools to obtain the required parental

[171] *Id.*
[172] *Id.*
[173] New Mexico ex rel. Balderas v. Google, LLC, 489 F. Supp. 3d 1254 (D.N.M. 2020).
[174] *Id.*
[175] Dave Embree, *Google escapes New Mexico AG's student privacy suit*, WESTLAW DATA PRIV. DAILY BRIEFING (Oct. 16, 2020) https://1.next.westlaw.com/Document/I5189ebee073011ebbea4f0dc9fb69570/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&OWSessionId=d45017fb0638473c9f85d7252bff7fe3&fromAnonymous=true&bhcp=1&CobaltRefresh=84834.
[176] *Id.*
[177] *Id.*

consent for data collection activities, rather than contacting parents directly.[178]

II. IMPLICATIONS

A. Implications for Policymakers

There are many loopholes in existing federal and state regulations that allow commercial companies to mine children's data at the expense of their privacy, as discussed throughout this paper (see Tables 1 and 2). Policymakers need to work to make sure future legislation has clearer and more explicit language, and that it contains fewer loopholes to hold third party commercial companies to greater legal accountability. FERPA guidelines can be amended by the Education Department to more narrowly tailor the disclosure of online student data (making it more equivalent to traditional directory information in the educational record) that is shared with commercial online operators, or at least require parental consent.[179] Third party operators should not be authorized as educational partners under PPRA, because PPRA allows them to use student PII commercially as long as parental consent was obtained.[180] Also, COPPA needs to be amended to remove the school exemption of third-party operators who are deemed educational partners, to make them liable to COPPA enforcement, which would allow the FTC to impose strict monetary fines and policy changes on commercial companies that are

[178] *Id.*

[179] Rhoades, *supra* note 1, at 472.

[180] Alexis M. Peddy, *Dangerous Classroom "App"-titude: Protecting Student Privacy from Third-Party Educational Service Providers*, 2017 BYU Educ. & L.J. 125, 138 (2017).

found to be violators.[181] COPPA could also be expanded to include students up to age eighteen. In California, SOPIPA could be amended to include companies not necessarily "targeting K-12 students," but who have services that K-12 students clearly use; and the definition of "targeted advertising" could be clearer.[182] The CCPA should apply to the sharing of data, not only the sale of data, and the default should be to opt out (rather than putting the burden on consumers to opt out).[183] Also, rules against the selling of "deidentified" information in all regulations needs to be stricter, since companies can still piece together disaggregated data and use it to create personal profiles.

Policymakers may set underlying legal protections for appropriate data collection and use by governments, businesses, organizations, and other entities that collect, process, and share young peoples' data.[184] Key considerations under debate include determining the appropriate age of digital consent, providing consent rights to the parent or the child, promoting a consent-based or rights-based framework, and relying on comprehensive or sector-based legislation.[185] A partnership between the American Civil Liberties Union and the Tenth Amendment Center is providing model legislation for states to adopt to strengthen data privacy protections for students.[186] In particular, the legislation aims to strengthen these four areas: 1) parental consent to release student data for

[181] Rhoades, *supra* note 1, at 471.
[182] *See* Crocetti, *supra* note 108, at 28-29.
[183] *See* Castelo, *supra* note 118.
[184] Jasmine Park & Amelia Vance, *Youth Privacy and Data Protection 101*, STUDENT PRIV. COMPASS (Apr. 1, 2021), https://studentprivacycompass.org/youth-privacy-and-data-protection-101/.
[185] *Id.*
[186] Doran, *supra* note 19.

noneducational purposes to third parties; 2) limits on information gleaned from laptop loaners; 3) protection from warrantless searches of student personal electronic devices on campus; and 4) restricting access to student postings behind social media privacy settings.[187] Unfortunately, softer solutions, such as encouraging companies to sign the Student Privacy Pledge, seem ineffective. The Pledge is a voluntary pledge to protect student privacy regarding the collection, maintenance, and use of student personal information.[188] The purpose is to encourage service providers to more clearly articulate their practices, and over 300 companies have signed on.[189] Among the high-profile signatories are Google, Microsoft, and Apple. However, conspicuously absent are Pearson, the largest education textbook publisher and a major distributor of online education services, and Facebook.[190] An analysis of the privacy policies and terms of service for eight companies who signed the Student Privacy Pledge revealed that most were not actually in compliance with the pledge.[191] Apple had the most potential violations, and most of the companies in the analysis had potential violations when it came to the collection, maintenance, and use of student information.[192]

Another key area for policymakers is to require and fund privacy literacy in K-12 schools. For example, in California, a state senator introduced an unfunded

[187] *Id.*

[188] Brenda Leong, *K-12 Student Privacy Pledge Announced,* FUTURE OF PRIV. FORUM (Oct. 7, 2014), https://fpf.org/press-releases/k-12-student-privacy-pledge-announced/.

[189] *Student Privacy Pledge 2020 Signatories,* FUTURE OF PRIV. FORUM (2020). https://studentprivacypledge.org/signatories/.

[190] *See id.*

[191] Pfeffer-Gillett, *supra* note 16, at 102.

[192] *Id.* at 113-16.

digital citizenship and media literacy bill to require the state superintendent of public instruction to convene a committee of educators, librarians, parents, students, and media experts to draw up guidelines on how best to recognize fake news.[193] Something similar could be done for privacy literacy. Privacy literacy has been operationalized as recognizing how personal data and metadata are collected, along with the potential implications; assessing how personal data is shared and making informed, intentional choices to safeguard privacy; identifying privacy issues facing our society; and describing the positive case for privacy as a human right fundamental to individual well-being.[194] Other researchers define privacy literacy as having six dimensions: 1) knowledge of the practices of online service providers, institutions, and organizations; 2) technical aspects of online privacy and data protection; 3) knowledge of potential privacy threats and risks; 4) knowledge of laws and legal aspects; 5) strategies for individual online privacy control; and 6) strategies for dealing with privacy threats.[195] These definitions could be a starting point for drawing up guidelines.

---

[193] Carolyn Jones, *Bill would help California schools teach about 'fake news,' media literacy*. EDSOURCE (May 24, 2017), https://edsource.org/2017/bill-would-help-california-schools-teach-about-fake-news-media-literacy/582363.

[194] Sarah Hartman-Caverly & Alexandria Chisholm, *Privacy Literacy Instruction Practices in Academic Libraries: Past, Present, and Possibilities*, 46 IFLA J*,* 305, 316 (2020).

[195] Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eichler, Mona Fischer, Alisa Hennhöfer, & Fabienne Lind, *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" in* Reforming European Data Protection Law, 347-51 (Serge Gutwirth, Ronald Leenes, & Paul de Hert, eds., 2015).

B. Implications for School Officials

Privacy protection should be a shared responsibility among school districts, educational technology companies, and state boards of education.[196] School officials need to insist that EdTech companies be more transparent, be held to greater accountability, and offer greater security for student data. All apps and websites should encrypt student data to protect them from "forces outside of the resource" as a starting point.[197] More uniform regulation of terms of service, including where and for how long data is used and stored, should occur; and data retention policies should be adjusted to address service provider contracts and the deletion of personal online data when no longer needed.[198] Having privacy specialists review contracts with educational technology providers so schools can publish a privacy notice explaining how information is collected and used would be ideal.[199]

Schools can put pressure on EdTech companies to embed privacy protections in the design, operation, and management of their products and services. One example is applying Ann Cavoukian's "7 Foundational Principles," which include: 1) being proactive and preventive rather than reactive and remedial; 2) protecting privacy by default; 3) fully integrating privacy into systems; 4) retaining full functionality of services; 5) ensuring end-to-end security; 6) maintaining visibility and transparency; and 7) keeping things user-centric.[200] The Future of Privacy Forum

[196] *See* El-Khattabi, *supra* note 17, at 535.
[197] Zimmerle, *supra* note 11, at 6.
[198] Huffman, *supra* note 61.
[199] *See generally, id.*
[200] Park, *supra* note 188.

(FPF) and 23 other organizations released *Education During a Pandemic: Principles for Student Data Privacy and Equity,* containing 10 recommendations for schools as they rely on new technologies and data.[201] A key recommendation was for all technology and subsequent data use to be evidence-based, evaluated for efficacy, in alignment with all applicable laws, only be deployed in consultation with experts and community stakeholders, and only allow the use of school or district-approved technologies in the classroom.[202] Other recommendations included suggestions to only collect necessary health data, create transparent data governance policies, and limit the sharing of personal information with authorities to a narrowly-tailored and documented purpose in accordance with applicable statutes and regulations.[203]

Districts can contract with chief privacy officers (CPOs) or certified information privacy professionals (CIPPs).[204] If schools lack funding for outside vetting, they can develop in-house vetting through free resources such as toolboxes with pre-vetted online products, searchable repositories of reviews, and iKeepSafe's list of resources that are compliant with key privacy laws.[205] Board participation on state privacy or data commissions should include establishing guidelines for the proper training of staff who handle personal student digital data.[206] More professional development is needed for teachers to better understand basic student data privacy

---

[201] *Education During a Pandemic: Principles for Student Data Privacy and Equity,* STUDENT PRIV. COMPASS, (Oct. 27, 2020), https://studentprivacycompass.org/pandemicprinciples/.

[202] *Id.*

[203] *Id.*

[204] Zimmerle, *supra* note 11, at 10.

[205] *Id*. at 7-9.

[206] El-Khattabi, *supra* note 17, at 535.

concepts.[207] Some organizations that offer helpful privacy educational resources include Our Data Bodies, Electronic Frontier Foundation, and Library Freedom Project.[208] Also, the Teaching Privacy project is a set of educational tools to help teachers demonstrate privacy, and Common Sense Media offers a digital citizenship curriculum aimed at K-12 that includes privacy modules.[209]

National or regional associations, state boards of education, and state education departments can work to create stronger standards that incorporate privacy literacy. The International Society for Technology in Education (ISTE) currently has "ISTE Standards for Students," which include a digital citizen component stating "students manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online."[210] A conceptual framework for K-12 for the closely related subfield "artificial intelligence literacy" was recently published, and competency number 16, on ethics, includes user privacy.[211] Similarly, the "AI for K12" working group published a draft set of standards for K-12 classrooms around artificial intelligence

[207] Doran, *supra* note 19.

[208] *See Data Justice and Human Rights*, OUR DATA BODIES, https://www.odbproject.org; *see* ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/; *see* LIBRARY FREEDOM, https://libraryfreedom.org/.

[209] *See* TEACHING PRIVACY, https://teachingprivacy.org/; *See* Digital Citizenship Curriculum, COMMON SENSE EDUC., https://www.commonsense.org/education/digital-citizenship/curriculum.

[210] *ISTE Standards for Students*, ISTE (June 2016), https://www.iste.org/standards/iste-standards-for-students.

[211] Duri Long & Brian Magerko, *What Is AI Literacy? Competencies and Design Considerations*, (Apr. 21, 2020) *in* Proc. of the 2020 CHI Conf. on Hum. Factors in Computing Sys., at 7 https://doi.org/10.1145/3313831.3376727.

literacy that encompasses five big ideas, the last of which is the societal impact of artificial intelligence, including the value tradeoff for giving away one's data.[212] These can serve as a starting point for infusing privacy literacy more formally into the curriculum.

C. Implications for Students and Parents

Both students and parents need to develop greater awareness of data surveillance and the fact that personal information is collected online about people, often without their permission. Children and their parents should be informed, in an accessible manner, about how their data will be used, and what rights they have through digital literacy lessons, such as in bite-sized explanations, just-in-time notices, cartoons, videos, or gamified content. 213 Children also need to develop greater awareness of the impact of behavioral ads, so they are not prone to fraudulent information and propaganda. Researchers found that students in public and private schools struggled in their ability to effectively evaluate and verify social and political information online.214 Successful privacy protection behaviors were identified as such things as frequently changing settings, so that content is only visible to

[212] David S. Touretzky, Christina Gardner-McCune, Fred Martin, & Deborah Seehorn, K-12 Guidelines for Artificial Intelligence: What Students Should Know (June 23-26, 2019), *in* Proc. of the ISTE Conf. at 32 (June 23-26, 2019), https://uocsweb03.uocslive.com/ISTE/ISTE2019/PROGRAM_SESSION_MODEL/HANDOUTS/112142285/ISTE2019Presentation_final.pdf.

[213] Park, *supra* note 188.

[214] Sarah McGrew, Joel Breakstone, Teresa Ortega, Mark Smith & Sam Wineburg, *Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning,* 46 THEORY & RSCH. IN SOC. EDUC. 165, 183 (2018).

specific people; using fake information online, such as a fake name; blocking, deleting, or deactivating cookies; and monitoring which information is available about oneself online.[215] These are behaviors that parents and students can be encouraged to adapt.

It is worth noting that richer school districts can afford to employ people to deal with privacy and cybersecurity compliance, in order to choose digital products that protect student privacy, whereas poorer school districts may not have the resources to do so, making student privacy a social justice issue.[216] Low-income students are more likely to need school-issued computers for homework, and are, thus, more likely to bear the brunt of surveillance policies that allow a school to extend their reach into a student's home.[217] Furthermore, IP addresses are often matched with real estate data by online platforms to customize advertising,[218] meaning that students in less affluent neighborhoods receive different, and often predatory, advertisements. School resource officers who rely on educational and surveillance technologies should be aware of these inherent biases.

---

[215] Moritz Büchi, Natascha Just & Michael Latzer, *Caring is Not Enough: The Importance of Internet Skills for Online Privacy Protection*, 20 INFO., COMMC'N & SOC'Y 1261, 1267 (2016).

[216] Ashley Gold, *Online Learning's Toll on Kids' Privacy*, AXIOS (Sept. 16, 2020). https://www.axios.com/childrens-privacy-suffers-as-school-goes-online-321b010a-1319-4028-b456-46a0a47f8920.html.

[217] Fedders, *supra* note 3, at 1716.

[218] See Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* 144 (2016).

CONCLUSION

The purpose of this paper was to explore student privacy in the context of big data and educational data mining, especially the mining of student data by third party commercial companies. There is growing concern that current student privacy regulations are inadequate, given the changing technology landscape. This paper gave a historical overview of key regulations and case law related to student privacy and discussed the extent to which student data is still largely unprotected from third parties. It concluded with implications for policymakers, school officials, and parents who want to be more attentive in protecting children from this form of exploitation for commercial gain by EdTech companies.

---

[i] Sofia Grafanaki, *Platforms, the First Amendment and Online Speech: Regulating the Filters*, 39 PACE L. REV. 111, 139 (2018).
[ii] Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969).
[iii] *Senator Al Franken Censures Google on Student Data Privacy Practices*, EDSURGE NEWS, (Jan. 19, 2016), https://www.edsurge.com/news/2016-01-19-senator-al-franken-censures-google-on-student-data-privacy-practices.
[iv] Cecilia Kang, *F.T.C. Hits Musical.ly with Record Fine for Child Privacy Violation*. NEW YORK TIMES (Feb. 27, 2019), https://www.nytimes.com/2019/02/27/technology/ftc-tiktok-child-privacy-fine.html.