Brigham Young University Education and Law Journal

Volume 2017 | Number 1 Article 5

Spring 4-1-2017

Dangerous Classroom "App"-titude: Protecting Student Privacy from Third-Party Educational Service Providers

Alexis M. Peddy

DANGEROUS CLASSROOM "APP"-TITUDE: PROTECTING STUDENT PRIVACY FROM THIRD-PARTY EDUCATIONAL SERVICE PROVIDERS

I. INTRODUCTION

Kate, an eleven-year-old middle school student, is told by her teachers to bring a mobile device to class[1] so she can engage in interactive teaching lessons during class through a free mobile application called "Take With Me Learning," which tracks students' progress throughout the semester.[2] The mobile application requires the student to create a profile consisting of personal information including school, teacher, age, name, and email address.[3] Once the student has access, he or she can

---

[1] This would be considered a type of "Bring Your Own Device" (BYOD) program, which allows students to bring their own laptops, tablets, cellphones, and other mobile devices in order to access certain activities, such as cloud-computing services and mobile applications, provided at school. *See Getting Started with BYOD*, K–12 BLUEPRINT (2014), https://www.k12blueprint.com/sites/default/files/Getting-Started-BYOD.pdf. Khan Academy is one common mobile application schools use to improve learning and gauge a student's progress. *See infra* note 8.

[2] *See Beyond the Fear Factor: Parental Support for Technology and Data Use in Schools*, FUTURE OF PRIVACY FORUM 4 (Sept. 2015), https://fpf.org/wp-content/uploads/Beyond-the-Fear-Factor_Sept2015.pdf [hereinafter *Beyond the Fear Factor*] (stating that online services may be used by schools "to manage grades, attendance, class assignments, bus routes, school lunch programs, special education services, counseling, standardized testing, and the myriad other functions they provide on a continuous basis."). The most common Internet practices include the use of cloud-computing programs, online textbooks, and mobile applications. Cloud computing, or storing data "in the cloud," provides a school with Internet-based email, word processing, and spreadsheet programs, allowing for anytime, anywhere access by the students, teachers, and administrators. Steve Mutkoski, *Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel,* 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 511, 512–15 (2014). Such platforms include Microsoft, Google, Edmodo, Amazon, and IBM. *Id.* at 515–16. Schools also use cloud-based services for language tools, online textbooks, and online tutoring. *Id.* at 516.

[3] According to a 2012 FTC study of mobile applications and children, 89.75% of applications were intended for children in elementary school and younger. FEDERAL TRADE COMMISSION, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 6 (Feb. 2012), https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf. In addition, "over 75% of the apps that specified an age range specified one ending at 12 years old or

watch tutorials, take quizzes, play educational games, participate in forums, and access online textbooks.[4] The teacher can monitor the students' progress as they take various quizzes and complete certain tasks. The teacher can also view the questions students post on the forum.

At the beginning of the school year, Kate's teacher sends consent forms home with the children. These forms ask parents to give consent for any online activity their child might engage in throughout the year. The forms state that the parents will allow their child to access websites and applications, such as "Take With Me Learning," for *any* educational purposes approved by the school. Kate's mother signs the form and returns it. Three months later, Kate's mother discovers from watching the news that the "Take With Me Learning" application Kate's class uses is the product of a company well-known for violating collection and privacy laws. The company has been illegally collecting students' information, selling it to advertisers, and making it accessible without limitation. Upset that Kate's information may be subject to identity theft, tracking, and targeted advertising, Kate's mother contacts the school and claims that the school failed to inform her of the "Take With Me Learning" producer's practices and reputation. She claims the school has violated not only Kate's privacy but also her own right as a parent to control access to her child's interactions.

In response, the school references the consent form and explains that under the Child Online Privacy Protection Act

younger . . . ." *Id.* at 7. Mobile applications have become a concern for parents because they contain advertisements, which fund the application to allow the user access for free or at a low cost. Joanna Tudor, *Legal Implications of Using Digital Technology in Public Schools: Effects on Privacy*, 44 J.L. & EDUC. 287, 311 (2015). The operators of these applications collect the user's data and sell it to marketing agencies, many times without the user's knowledge. *Id.* The data collected generally "includes phone and email contacts, call logs, Internet data, calendar data, data about the device's location, the device's unique IDs and information about how the user engages with the app itself." *Id.*

[4] Online textbooks contain hyperlinks to different websites, videos, and homework help sites that may not be covered by the online textbook website's own privacy disclosures and policies. *See* DIGITAL TEXTBOOKS IN K–12 SCHOOLS, OFFICE OF RESEARCH AND EDUCATION ACCOUNTABILITY, TENNESSEE COMPTROLLER OF THE TREASURY, JUSTIN P. WILSON (Oct. 2013), http://www.comptroller.tn.gov/Repository/RE/Digital%20Textbooks.pdf. Online textbooks do create risks, however, with the compromise of young children's data and personal information, and also for the loss of parents' ability to exercise control over their child's interactions. Tudor, *supra* note 3, at 327.

(COPPA) it is the responsibility of "Take With Me Learning," not the school, to obtain parental consent when dealing with children under thirteen. Kate's mother contacts the school board and asks why the school was allowed to circumvent her consent when dealing with a third-party operator like "Take With Me Learning." She wants to know 1) why the school did not inform her of the application producer's information-collection practices and obtain her consent before engaging with her child, and 2) why "Take With Me Learning" did not take measures to ensure that the consent the school provided was verifiable.

Contracting with third parties has become increasingly common in present-day elementary and middle schools.[5] Those who qualify as third-party operators under COPPA's regulations make up a considerably large group.[6] School districts enter into agreements with such operators, who may generally be categorized as website and application service providers, to deliver services such as Google Apps for Education[7] and Khan Academy[8] to schools. Even though such applications facilitate a more efficient organizational structure

---

[5] *See* Jules Polonetsky & Omer Tene, *Who is Reading Whom Now: Privacy in Education from Books to MOOCs*, 17 VAND. J. ENT. & TECH. L. 927, 929–31 (2015); *PBS NewsHour: Why Digital Education Could Be A Double-Edged Sword* (PBS television broadcast Apr. 5, 2016), http://www.pbs.org/newshour/videos/#176786 (discussing the privacy concerns in Miami, Florida classrooms as teachers begin to use more online applications and the harms that are present).

[6] COPPA defines an "operator" as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information . . . for commercial purposes." 15 U.S.C. §6501(2)(A) (1998).

[7] Google Apps for Education is a service provided by Google "in the cloud" to educational institutions. The service offers email, calendar, and chat, as well as interactive services like Google Drive, Classroom, Docs, Slides, Sites, Hangouts, etc. *See The Google Apps for Education Core Services,* GOOGLE, https://www.google.com/edu/products/productivity-tools (last visited Sept. 12, 2016); *Google Apps for Education: Common Questions*, GOOGLE, https://support.google.com/a/answer/139019?hl=en (last visited Feb. 12, 2016). Unlike a personal account with Google, Google Apps for Education prohibits advertising, offers 24/7 support, has enhanced security features, and provides full administration of all user accounts. *Id. See also Google for Education: Privacy & Security Information Tools Schools Can Trust*, GOOGLE, https://www.google.com/edu/trust/#does-google-own-school-or-student-data (last visited Feb. 12, 2016) (addressing privacy and privacy law compliance concerns, including a statement that Google Apps for Education contractually requires schools to get the parental consent required by COPPA).

[8] KHAN ACADEMY, https://www.khanacademy.org/about (last visited Feb. 12, 2016) ("Khan Academy offers practice exercises, instructional videos, and a personalized learning dashboard . . . . [Khan Academy's] math missions guide learners from kindergarten to calculus using state-of-the-art, adaptive technology that identifies strengths and learning gaps.").

for teachers and administrators and provide students with beneficial interactive learning, the practice of contracting with third-party operators raises privacy concerns and creates the possibility of substantial harm to the children who use these operators' products.[9]

Three substantial risks exist in online classroom interactions between young students and third-party operators: illegal data collection, susceptibility to criminal activity, and identity theft caused by hacking. Firstly and most notably, opening the door for operators in the classroom creates the risk of illegal data collection and dissemination from both advertisers and criminals.[10] In order to reach larger audiences, advertisers utilize multiple techniques to track a user's behavior and gain insight that will assist in advertisement placement on that user's browser.[11] Such techniques include tracking activity through a device's IP address, tracking search terms entered into a search engine, and using "cookies" to retain a user's information.[12] Tracking a student's activity in such a manner can be particularly dangerous when the operator can collect personal information such as name, address, or location—when a student either inputs that information to create an account for a service or uses a service to perform research.[13] While such collection by advertisers is a

[9] *See* Tudor, *supra* note 3, at 306–30 (2015); Lauren A. Matecki, *Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era,* 5 NW. J. L. & SOC. POL'Y. 369, 374 (2010); Stephanie Simon, *Data Mining Your Children*, POLITICO (Mar. 16, 2016), http://www.politico.com/story/2014/05/data-mining-your-children-106676_Page2.html (last visited Oct. 16, 2016).

[10] Tudor, *supra* note 3, at 306–30. Concern has grown in recent years as operators increase their use of passive collection methods. Matecki, *supra* note 9, at 388. Matecki also quotes that a serious concern for child privacy exists because of "'the vulnerability of children,' (2) 'the immediacy and ease with which information can be collected from them,' and (3) 'the ability of the online medium to circumvent the traditional gatekeeping role of the parent.'" *Id.* at 374 (quoting FTC, FILE NO. 954,4807, PRIVACY ONLINE: A REPORT TO CONGRESS 12 (1998), available at http://www.ftc.gov/reports/privacy3/toc.shtm).

[11] Tudor, *supra* note 3, at 306.

[12] *Id.* at 307–10.

[13] *Id.* at 311–12 (addressing the ways that applications used in schools collect personal information from students and the harms that this creates for the unsuspecting student). Collection of personal information may also include a student's daily interests—for example, a math program used in Miami's iPrep Academy creates customized lessons by gathering student interests (ranging from favorite foods to the names of their friends) to include in future math problems. *PBS NewsHour, supra* note 5, beginning at 1:13.

business practice, legislation exists that makes this collection illegal when the operator collects personal information from a child under the age of thirteen without parental consent.[14]

Secondly, the child's information could be compromised through criminal activity.[15] Criminal activity could include activities such as identity fraud, harassment, and stalking.[16] One recent example includes the 2014 case of *United States v. Rhim-Grant*, in which the defendants (food service managers in Miami-Dade County Public Schools) used their access to the school computer database to steal approximately four hundred student social security numbers, resulting in numerous fraudulent tax returns.[17] In this particular case, the information was stolen by individuals who were part of the school's network; however, as schools contract more frequently with third-party online service providers, schools and their students become more susceptible to such criminal activity.

A third major concern is that school databases can be hacked, which can lead to identity theft.[18] Hackers have targeted universities in search of students' names, birthdates, and social security numbers.[19] While K–12 school districts have not yet had major problems with this type of hacking, young students may be more susceptible as they participate in classroom educational applications, not only because these grades use applications from third-party operators with increasing frequency, but also because children lack full knowledge of the potential harm they invite by entering their

---

[14] 15 U.S.C. §6502(a) (1998) (prohibiting an operator of a website or online service directed to children or knowingly used by children to collect the child's personal information).

[15] *See* Tudor, *supra* note 3, at 325–330.

[16] *Id.* at 325.

[17] *PBS NewsHour*, *supra* note 5, beginning at 4:57; Press Release, FBI: Miami Division, *Twenty-Five Defendants Charged in Separate Schemes That Resulted in Thousands of Identities Stolen and Millions of Dollars in Identity Theft Tax Filings* (April 3, 2014), https://archives.fbi.gov/archives/miami/press-releases/2014/twenty-five-defendants-charged-in-separate-schemes-that-resulted-in-thousands-of-identities-stolen-and-millions-of-dollars-in-identity-theft-tax-filings. Frank Maderal, Assistant United States Attorney assigned to the Rhim-Grant case, stated that all the defendant had to do was "login, access the information, print it out." *PBS NewsHour*, *supra* note 5, beginning at 5:30.

[18] Tudor, *supra* note 3, at 327.

[19] *Id.* (citing an FTC report on child identity theft). *See also* Simon, *supra* note 9 (citing an incident at the University of Maryland where nearly three hundred thousand students, faculty, and staff had their personal information, including social security number, stolen).

personal information online.

In order to protect young students from these dangers and ensure compliance with COPPA at school, the law must ask *who* is responsible for ensuring that the students' personal information remains safe—the school or the third-party operator? Because COPPA does not apply directly to schools as entities,[20] the Federal Trade Commission (FTC) issued guidance in 2015, creating a "school exception."[21] This exception allows schools to give permission to third-party operators in place of parents, so long as it is given strictly for educational purposes.[22] However, it also becomes a question of whether federal action is adequate or whether state action is also required. Federal legislation like COPPA fails to adequately protect young students, and its language generates confusion about which third-party operators must follow regulations for online privacy and who is at risk for sanctions if they don't comply. States lacking protection should therefore create their own legislation targeting classroom interactions between students and third-party operators to ensure that student personal data is kept private and not subject to outside collection and dissemination.

This Comment addresses concerns and tensions between COPPA and the school system and proposes a more comprehensive solution at the state level. COPPA itself does not apply to a school as an entity; but as technology improves and infiltrates the classroom, young students will continue to need COPPA's protection. Due to the FTC's lack of COPPA enforcement, some states have begun to create their own school-specific legislation to increase protection for their students while interacting online. Allowing illegal collection of data without proper consent to go virtually unmonitored creates a high risk of harm to a child. Therefore, this Comment

---

[20] 15 U.S.C. § 6501(2) (1998) (defining operators as having commercial purposes). *See also* Lesley Fair, *Testing: A Review Session on COPPA and Schools,* FEDERAL TRADE COMMISSION (Jan. 23, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/01/testing-testing-review-session-coppa-schools ("Schools—which are usually part of the local government—don't fall within the legal definition of who's covered by COPPA because they aren't commercial 'operators.'").

[21] *A Guide for Business And Parents And Small Entity Compliance Guide*, Federal Trade Commission M1 (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools [hereinafter *2015 Guidance*].

[22] *Id.*

argues that *all* states should proactively create legislation governing classroom interactions between students and third-party operators.

Part II of this Comment examines COPPA's legislative history and its requirements, as well as how lack of enforcement has rendered COPPA's application to schools unclear and unworkable. Further, this section compares COPPA to current federal student-data legislation and recent federal attempts at classroom-oriented agency rules and legislation, concluding that reform at the state level is the most effective in ensuring that young students' privacy is not compromised through the illegal collection of personal information.

Part III explains and critiques the gap between COPPA's protection and the school system, focusing on the confusing and inefficient consent requirements that both schools and third-party operators can circumvent under FTC regulation as it stands. It argues that allowing a school to obtain blanket "verifiable parental consent" is dangerous because (a) it is difficult for the online operator to authenticate the consent given by the school, and (b) it is unclear who specifically within the school can give the consent in lieu of parents. Further, because states seek greater protection and transparency in online dealings for their students, Part III also provides examples of states, such as California, Washington, Utah, and Delaware, that have begun creating student-data legislation to address student and third-party-operator interactions in the classroom. It urges that the remaining states do the same—particularly by adopting a dual prohibitive/governance approach (an approach that encompasses both express prohibitions and methods of oversight for schools to ensure compliance).

Part IV offers both prohibitive- and governance-based provisions states should consider when writing new student-data legislation. Lastly, Part V concludes.

II. COPPA: BACKGROUND AND PROBLEMS CREATED

A. Legislative History and Reasons for Enactment

By 1998 the personal computer had become a basic tool not

only at work, but also in the home and at school.[23] According to the 1997 census, 74.4% of children ages three to seventeen had access to a computer, and 22.6% of these children had used the Internet.[24] With computer and Internet use on the rise among some of society's youngest members, Congress found that protecting such students' personal information became a priority. The FTC determined in 1998 that "children lack the developmental capacity and judgment to give meaningful consent to the release of personal information to a third party"[25]—a child may disclose such information in order to engage in online activity without fully understanding the consequences.[26] "Before 1998, no federal law restricted collection of personal information from children online."[27] In fact, according to a survey conducted by the FTC that year, 89% of websites directed at children collected personal information from them, with only 23% of websites requesting parental consent from parents for this collection.[28]

Such collection practices by website operators caused some people to be wary of Internet use for children.[29] Ninety-seven percent of parents expressed concerns about their children's personal information being shared with third parties.[30] Congress found that interactions presented to minors while on the Internet "frustrate parental . . . control," that protection of minors on the Internet "is a compelling government interest," and that offering defenses for minors is the "least restrictive means" of protecting their privacy on the Internet.[31] As a result, Congress adopted Senator Richard Bryan's COPPA bill to advance the following goals:

(1) [T]o enhance parental involvement in a child's online

---

[23] U.S. CENSUS BUREAU, COMPUTER USE IN THE UNITED STATES: POPULATION CHARACTERISTICS 1 (1997), http://www.census.gov/prod/99pubs/p20-522.pdf (stating that "36.6% [of American households] had computers," which was "up substantially from 22.8% in 1993, 15.0% in 1989, and 8.2% in 1984.").

[24] *Id.* at 3.

[25] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 5 (1998) [hereinafter 1998 FTC REPORT].

[26] *See* Matecki, *supra* note 9, at 374.

[27] David R. Hostetler & Seiko F. Okada, *Children's Privacy in Virtual K-12 Education: Virtual Solutions of the Amended Children's Online Privacy Protection Act (COPPA) Rule,* 14 N.C. J.L. & TECH. ON. 167, 176 (2013).

[28] 1998 FTC REPORT, *supra* note 25, at iii.

[29] *Id.* at 3.

[30] *Id.* at 37.

[31] Pub. L. No. 105-277, 112 Stat. 2681, Part III (1998).

> activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent. The legislation accomplishes these goals in a manner that preserves the interactivity of children's experience on the Internet and preserves children's access to information in this rich and valuable medium.[32]

Congress enacted COPPA[33] to regulate the online collection, use, and disclosure of personal information of children under the age of thirteen.[34]

B. COPPA Standards and Requirements

In its latest form (FTC rule passed in 2013), COPPA protects a range of personal information: name, address, Social Security number, photograph, video, and geolocation information.[35] COPPA applies to two parties: (a) operators of commercial websites and online services directed at children and (b) operators of general audience websites and online services who have actual knowledge that they are collecting personal information from children.[36] Before an operator may undertake such activities, it must provide notice to parents and receive verifiable parental consent.[37]

However, the statute recognizes that situations exist in which less parental consent is necessary; thus it adopts a

---

[32] 144 Cong. Rec. S11657 (Oct. 7, 1998) (statement of Sen. Bryan).

[33] The Child Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998) (effective in 2000).

[34] *Id.*

[35] *See* 16 C.F.R. §312.2 (2013).

[36] 15 U.S.C. §6502(a)(1).

[37] 15 U.S.C. § 6502(b)(1)(A). "Verifiable parental consent" is defined as:

> [A]ny reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

15 U.S.C. § 6501(9).

"sliding scale"[38] when determining requirements for parental consent. COPPA does not require verifiable parental consent when the online contact is on a "one-time basis," for the sole purpose of providing notice to a parent and receiving consent, for protection of the child's safety, or as required by law.[39] For example, a third-party operator does not need to provide notice or obtain verifiable parental consent when responding to a one-time email request from a child where the child's email is promptly deleted after issuing a response.[40] However, an operator must provide *notice* to parents and an opportunity to opt out when allowing a child to subscribe to periodic interactions such as email newsletters and must obtain *full parental consent* in situations where children can post or share personal information publicly.[41] Any personal information that has been collected for these one-time interactions may be kept only for as long as necessary to fulfill the operator's purpose.[42] Afterward, the operator must delete the child's information using reasonable measures.[43] Because the law allows for situations where parental consent is not required, the key to ensuring compliance is enforcement.[44]

The FTC is the governing body that regulates and enforces COPPA.[45] It has the full authority to treat violations in the same manner as other rules defining unfair and deceptive acts or practices under the Federal Trade Commission Act.[46] An operator who violates COPPA may face civil penalties up to

[38] Matecki, *supra* note 9, at 377–78; *see also* 15 U.S.C. § 6502(b); *COPPA +1: Issues and Impacts For Children's Privacy,* KELLER AND HECKMAN LLP (Sept. 11, 2014).

[39] 15 U.S.C. § 6502(b)(2).

[40] *2015 Guidance*, *supra* note 21, at (H)(2); *COPPA +1: Issues and Impacts For Children's Privacy, supra* note 38.

[41] *COPPA +1: Issues and Impacts For Children's Privacy, supra* note 38.

[42] 16 C.F.R. § 312.10.

[43] *Id.*

[44] *See* Hostetler & Okada, *supra* note 27, at 188–89.

[45] 15 U.S.C. § 6505(a) (stating that this title is to be enforced by the commission under the Federal Trade Commission Act). The FTC must create regulations to ensure parents receive proper notice and opportunity to give parental consent; to provide parents with the opportunity to review the child's information and the opportunity to prevent further use of the child's personal information; to limit a website's collection of the child's personal information; and to establish procedures to protect the confidentiality and security of the child's information. 2 Fed. Trade Comm'n. § 20:15 (2015); 15 U.S.C. § 6502(b)(1) (listing the requirements for the regulations to be imposed by the FTC).

[46] 15 U.S.C. § 57(a)(1)(B); 15 U.S.C. § 6504(a)(1).

$16,000 per violation.[47] In determining the amount of civil penalties, courts consider the "egregiousness of the violations, whether the operator has previously violated the Rule, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company."[48] In addition, any state attorney general may bring a civil action on behalf of its residents.[49]

However, even with such measures established by law, the FTC has not effectively enforced them.[50] As of January 1, 2015, only twenty-four COPPA actions had been filed.[51] In addition, only three states—New Jersey, Texas, and Maryland—had successfully brought enforcement actions.[52]

C. Problems with COPPA Enforcement

Since its enactment, COPPA has faced criticism for both its ineffectiveness and its improper enforcement.[53] Even though COPPA initially seemed to work after its first FTC review in 2002, with more than 90% of *children's* websites meeting the necessary disclosure requirement, it has not generated resounding success with websites not specifically directed at children under the age of thirteen.[54] The statute's vague language has rendered it difficult for website operators to avoid violations.[55] One of the main criticisms directed at COPPA involves the ability of a child to falsify his or her age, tricking the operator into believing it is in compliance with COPPA

---

[47] *2015 Guidance*, *supra* note 21, at (B)(2).

[48] *Id.*

[49] 15 U.S.C. § 6504(a)(1).

[50] *See COPPA +1: Issues and Impacts For Children's Privacy, supra* note 38; Matecki, *supra* note 9.

[51] Richard A. Chapo, *List of COPPA FTC Enforcement Cases,* COPPA AND FERPA: COPPA AND FERPA LEGAL ADVICE (Feb. 3, 2015).

[52] *Id.*; *see also* Maryland Attorney General, *Attorney General Gansler Secures Settlement from Snapchat, Inc.* (June 12, 2014); New Jersey Attorney General, *New Jersey Attorney General and Division of Consumer Affairs File Federal Suit Against App Developer Accused of Collecting, Transmitting Children's Personal Information Without Parental Notification or Consent* (June 6, 2012); Texas Attorney General, *Attorney General Abbott Takes Action Against Web Sites That Illegally Collect Personal Information from Minors* (Dec. 5, 2007).

[53] *See* Matecki, *supra* note 9, at 379–87; Hostetler & Okada, *supra* note 27, at 181–84.

[54] FTC, STAFF REPORT, *Protecting Children's Privacy Under COPPA: A Survey On Compliance* (Apr. 1st, 2002), www.ftc.gov/os/2002/04/coppasurvey.pdf.

[55] Matecki, *supra* note 9, at 379.

when in fact it is in violation and thus subject to fine.[56] Only fourteen federal actions were filed from 1999 to 2014, including actions against Lisa Frank, Inc. (2001); Hershey Food Corp. (2003); Xanga.com, Inc. (2006); Sony BMG Music Entertainment (2008); and Yelp, Inc. (2014).[57] With technology and online interaction capabilities continually on the rise, especially in the classroom, the likelihood of further COPPA violations is inevitable.

D. Application of COPPA in Schools and the "School Exception"

One of COPPA's perceived shortcomings is its inapplicability to schools. While COPPA protection applies to the privacy of children under the age of thirteen, it does not directly apply to schools as entities.[58] Thus, a gap exists between the protection of a child's privacy at home and a child's privacy while at school.

Unlike other federal legislation, COPPA deals strictly with interactions between children under thirteen and online operators. Its purpose is to protect children regardless of the setting. In application, COPPA requires that before a third-party operator authorizes a child under thirteen to use its website and services, it must provide notice and obtain verifiable parental consent.[59] However, operators contracted within the school setting must provide such notice directly to the school, not to the parent.[60] Additionally, but *only upon request* from the school, the operator must provide a description of the types of information collected, an opportunity to prevent further use or collection of the child's personal information, and the opportunity to review the child's personal information submitted and/or have it deleted.[61] Thus, notice provided to schools allows the schools to decide whether to

[56] *Id.* at 382–83. COPPA requires that an operator have "actual knowledge" that it is collecting personal information from a child in order to be in violation. 15 U.S.C. § 6502(a)(1).

[57] Chapo, *supra* note 51.

[58] 15 U.S.C. § 6501(2).

[59] 15 U.S.C. § 6502(b)(1)(A).

[60] *2015 Guidance*, *supra* note 21, at (M)(1) (stating that the operator must provide the school with all the notices required under COPPA). However, the FTC also recommends that the schools consider making the notice available to parents as best practice. *Id.*

[61] *Id.*

contract with each specific operator for educational services.

The FTC draws a distinction for when an operator may rely on the school's consent in lieu of parental consent. If the operator collects the child's data *solely for the use and benefit of the school*, consent given by the school is sufficient.[62] This school exception is based on the policy rationale that "school officials already act on behalf of the students' best interests and well-being when arranging and delivering their education in non-virtual context."[63] However, if the operator collects and uses the child's information for commercial purposes, then parental consent must be obtained.[64] The FTC states, "[a]s long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent."[65] It further advises, "Where an operator gets consent from the school rather than the parent, the operator's method must be reasonably calculated, in light of available technology, to ensure that a school is actually providing consent, and not a child pretending to be a teacher, for example."[66] While other federal protections do exist to protect a student's data *at school*, they do not offer the same protections as COPPA, leaving children under the age of thirteen vulnerable while engaging with third-party operators at school.

1. The inadequacy of current federal student data legislation

The most widely known federal student data privacy law is the Family Educational Rights and Privacy Act (FERPA).[67] FERPA covers elementary, secondary, and post-secondary school students.[68] However, FERPA is narrow—limited to the

[62] *Id.* at (M)(2) ("Where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, and for no other commercial purpose, the operator is not required to obtain consent directly from parents . . . .").

[63] Hostetler & Okada, *supra* note 27, at 198.

[64] *2015 Guidance*, *supra* note 21, at (M)(2). For the collection of a child's information for commercial purposes, some methods of obtaining "verifiable parental consent" include signed consent forms sent via mail, fax, or scan; credit/debit card transactions; toll-free phone calls; and checking the parent's government-issued identification against a database of such information. *Id.* at (H)(4).

[65] *Id.* at (M)(1).

[66] *Id.* at (M)(2).

[67] 20 U.S.C. § 1232.

[68] 20 U.S.C. § 1232(a)(3) (2013).

prohibition of the release of students' personal information from a school's *educational records*.[69] Like COPPA, FERPA creates scenarios in which parental consent may be circumvented.[70] Since FERPA strictly governs educational records, it does not extend to the online classroom interactions that have become so prevalent in today's society.

Another federal statute that addresses online privacy is the Protection of Pupil Rights Amendment of 1978 (PPRA),[71] which protects students in grades K–12.[72] Like COPPA, PPRA applies when personal information is collected through online interaction, and even provides a similar "school official exception."[73] PPRA allows the third-party operator to use the student's personal information commercially, so long as the proper parental consent has been obtained.[74] Because PPRA carries the same consent exceptions as COPPA, it has the same inherent flaw—failure to provide the necessary checks to ensure parental consent for children, especially since the statute gives schools the ability to circumvent parental consent for educational purposes. Neither FERPA nor PPRA is adequate nor strict enough to address the current parental consent gap between schools, parents, and third-party providers to ensure a child's protection. Therefore, change must be made at the state level.

---

[69] *Id.* at (b)(1). An "educational record" includes "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." *Id.* at (a)(4). Under FERPA, parents retain the right to review and amend their child's education records until the child reaches eighteen years old or reaches a post-secondary institution. 20 U.S.C. § 1232(d). FERPA requires parental consent be given before any personal information or information found within the educational record is shared. *Id.* at (b)(1).

[70] Under the "school official exception," the school may disclose information without prior consent to other school officials or vendors who perform a function for the school that would otherwise be performed by a school employee. 34 C.F.R. § 99.31(a)(1)(i)(A)–(B) (2011). The vendor must have a legitimate educational interest in the data, and the school must be in direct control of the vendor's use and maintenance of the data. *Id.* at (a)(1)(ii).

[71] 20 U.S.C. § 1232(h).

[72] 20 U.S.C. § 1232h(c)(6)(F) (2012).

[73] The exception allows the school to circumvent parental consent when the personal information collection is for the "exclusive purpose of developing, evaluating, or providing educational products or services . . . ." *Id.* at (c)(4)(A).

[74] PPRA requires that schools notify parents, obtain consent, and offer an opt-out opportunity before allowing the child to engage in any online "collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information." *Id.* at (c)(2) and (c)(1)(E) (2012).

2. Recent COPPA concerns and changes: The 2013 FTC rule and federal legislative attempts

In the fifteen years COPPA has been in effect, it has faced numerous reform attempts at the federal level via legislation and agency action. In 2013 the FTC successfully promulgated a rule that provides children with greater privacy as well as clearer guidelines for third parties obtaining parental consent.[75] While the FTC's new changes do expand a child's privacy and provide the parent with more control, they do so in a manner that does not improve its application in schools. This is especially concerning as technology continues to infiltrate every aspect of life and the lines of COPPA compliance become blurred.

As a result, legislators in Congress have taken steps toward expanding COPPA to the classroom.[76] Generally, recent legislative attempts have focused on expanding the age group to cover a larger group of minors, expanding the definition of "personal information," and expanding the group of

[75] 16 C.F.R. § 312 (2013). A child's "personal information" includes additional persistent identifiers, such as IP address; photo, audio, or video of the child; and geolocation. *Id.* at § 312.2; *see also COPPA +1: Issues and Impacts For Children's Privacy*, *supra* note 38. Additionally, the FTC addresses specific ways for operators to obtain verifiable parental consent, including the new methods of approval by checking a government-issued ID against a database, video conferences with parents, and asking knowledge-based questions to which only a parent would have the answer. 16 C.F.R. § 312.5(b); *see also COPPA +1: Issues and Impacts For Children's Privacy*, *supra* note 38. These explicitly-stated methods will hopefully direct operators toward a "reasonably calculated" method and make the process more tangible and efficient. 16 C.F.R. § 312.5; *see also* 15 U.S.C. §§ 6501(9) (defining "verifiable parental consent" as "any reasonable effort . . . to ensure that a parent of a child receives notice of the operator's personal collection, use, and disclosure practices, and authorizes [such uses]."). The FTC also reigned in their "notice to parents" standard, requiring many additional administrative and operational compliance steps to ensure correct notice is provided. 16 C.F.R. §312.4. Notice given to parents "must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials." *Id.* at § 312.4(b). Such compliance steps include both direct notice to parents (i.e., through the use of hyperlinks) and notice given through the website or online service (i.e., third party operators "must post a prominent and clearly labeled link to an online notice of its information practices . . . ."). *Id.* at §312.4(c)–(d).

[76] Congress considers student privacy to be an important issue to many of its constituents, evidenced by its hundreds of attempts to pass legislation over the years. *See* Tanya Roscorla, *The Lowdown on Federal Student Data Privacy Legislation of 2015*, CENTER FOR DIGITAL EDUCATION (July 28, 2015), [hereinafter *Lowdown on Federal Legislation 2015*], http://www.centerdigitaled.com/k-12/The-Lowdown-on-Federal-Student-Data-Privacy-Legislation-of-2015.html ("Over the last few years, state legislatures have considered hundreds of student data privacy bills, and that's shown federal policymakers that this issue is important to their constituents.").

"operators."[77] Some of the most recent legislative attempts include the Do Not Track Kids Act of 2015,[78] the Student Digital Privacy and Parental Rights Act of 2015,[79] and the Every Student Succeeds Act.[80] The Do Not Track Kids Act of 2015 would expand COPPA coverage to *minors* between the ages of twelve and sixteen[81] and make it unlawful for operators (including operators of websites, online services, and mobile applications explicitly) to engage in targeted marketing without verifiable parental consent for children or the consent of the minor.[82] It would also provide an "eraser button" for

[77] *See Comparison of 2015 Federal Education Data Privacy Bills*, NATIONAL ASSOCIATION OF STATE BOARDS OF EDUCATION (July 22, 2015), http://www.nasbe.org/wp-content/uploads/2015-Federal-Education-Data-Privacy-Bills-Comparison-2015.07.22-Public.pdf, [hereinafter *Federal Legislation Chart*] (comparing eight different pieces of legislation introduced or passed in 2015 to FERPA and COPPA, which demonstrates that protecting education privacy is a relevant and important issue to Congress).

[78] H.R. 2734, 114th Cong. (2015). The Do Not Track Kids Act of 2015 is most pertinent to the collection of personal information from young children by third party contractors in school. It was introduced by Senator Edward Markey and Representative Joe Barton to the House on June 11, 2015, and seeks to amend COPPA and expand its coverage. *See Summary H.R. 2734*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2734; Ronald London, John D. Seiver & Bryan Thompson, *Significant Amendments to COPPA Proposed in Do Not Track Kids Act*, DAVIS WRIGHT TREMAINE LLP (June 22, 2015), http://www.privsecblog.com/2015/06/articles/marketing-and-consumer-privacy/significant-amendments-to-coppa-proposed-in-do-not-track-kids-act/. Earlier versions of this legislation were proposed in 2011 and 2013, but both died in committee. *See H.R. 3481 (113th): Do Not Track Kids Act of 2013*, https://www.govtrack.us/congress/bills/113/hr3481; *Summary H.R. 1895, 112th Congress* (2011–2012), https://www.congress.gov/bill/112th-congress/house-bill/1895.

[79] H.R. 2092, 114th Cong. (2015). Representatives Luke Messer and Jared Polis introduced The Student Digital Privacy and Parental Rights Act on April 29, 2015. *Id. See also* Press Release, *Congressman Jared Polis, Messer, Polis Introduce Landmark Bill to Protect Student Data Privacy: Measure Represents the Most Significant Federal Attempt to Protect Student Data in Decades* (Apr. 29, 2015), http://polis.house.gov/news/documentsingle.aspx?DocumentID=397810. The Act focuses on regulating the online providers in the K–12 classrooms, not on amending COPPA. *See Federal Legislation Chart*, *supra* note 77, at "The Student Digital Privacy and Parental Rights Act of 2015" column. The Act prohibits operators from collecting and selling a student's information to a third party for a non-school related purpose. H.R. 2092, at §3(a).

[80] Every Student Succeeds Act, 114 P.L. 95, 129 Stat. 1802 (enacted Dec. 10, 2015).

[81] H.R. 2734, at § 9(a)(1) (defining "minor" as "an individual over the age of 12 and under the age of 16). This amendment distinguishes between a "child" and a "minor," with a "child" being an individual under the age of 13, as defined by the parent statute COPPA (15 U.S.C. § 6501(1)).

[82] H.R. 2734, at § 3(a) (stating that a parent must give verifiable parental consent before an operator may collect a *child's* personal information, and a minor must give consent before the operator may collect the minor's personal information).

parents and children to eliminate personal information that has been made available,[83] and set forth enforcement provisions for other agencies and states in addition to those promulgated by the FTC.[84] The Student Digital Privacy and Parental Rights Act would prohibit operators from collecting and selling a student's information to a third party for a non-school related purpose[85] and give parents more control over their child's information.[86] Most notably, this legislation would require operators to publicly list what type of data they collect, how it is used, and whether it is shared in a clear and easy-to-understand manner.[87] While these two attempts seem promising, their track records and stagnant positions in Congress seem to suggest that federal legislation may not be the most efficient or welcome approach to protecting our children from the threat of private-information collection and use by third-party operators in the classroom.[88]

Congress successfully enacted a student-data privacy law in 2015, The Every Student Succeeds Act,[89] but eliminated the

[83] *Id.* at § 6(b)(1) (stating that no later than one year after the enactment of the Act, the commission must promulgate a rule "to implement mechanisms that permit a user . . . to erase or otherwise eliminate content or information submitted . . . that is publicly available . . . and contains or displays personal information of children or minors."). Additionally, the operator must make users aware of the mechanism. *Id.*

[84] *Id.* at § 7(b)–(c) (listing five other federal acts under which this Act may be enforced and explaining the steps a state attorney general must take to enforce).

[85] H.R. 2092, at §3(a).

[86] *Id.* at § 3(c)(1) (stating that parents have the ability to directly authorize the student's information for non-educational purposes). Also, parents may request the deletion of their child's information that is not required by the school to be maintained. *Id.* at § 3(b)(2).

[87] *Id.* at § 3(b)(3).

[88] The Do Not Track Kids Act of 2015 has not moved since its introduction and assignment to committee. *See Summary H.R. 2734*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2734 (showing that the last action took place on June 12, 2015). Additionally, the failed attempts in 2011 and 2013 provide little hope for this amendment's enactment. *See H.R. 3481 (113th): Do Not Track Kids Act of 2013*, https://www.govtrack.us/congress/bills/113/hr3481; *Summary H.R. 1895, 112th Congress* (2011–2012), https://www.congress.gov/bill/112th-congress/house-bill/1895?q=%7B%22search%22%3A%5B%22%5C%22hr1895%5C%22%22%5D%7D&resultIndex=3. The Student Digital Privacy and Parental Rights Act of 2015 has also not moved since being assigned to committee on May 1, 2015. *See Summary: H.R. 2092, 114th Congress* (2015–2016), CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2092/all-actions-without-amendments?q=%7B%22search%22%3A%5B%22%5C%22hr2092%5C%22%22%5D%7D&resultIndex=1.

[89] Every Student Succeeds Act, 114 P.L. 95, 129 Stat. 1802 (enacted Dec. 10, 2015). The Act was enacted on December 10, 2015 to amend the Elementary and

language directed at protecting interactions between students and third-party operators.[90] The bill originally seemed promising in bringing improvements to student privacy at the federal level through the creation of an enforcement committee.[91] Such a committee would have been the first major step in enforcing the protections that laws like COPPA have let slip through the cracks—such as ensuring proper parental consent has been obtained. Because these extra classroom privacy protections failed to make it into the final version of the law, it seems that Congress is unwilling to address this issue anytime soon. Failing to realize that technology will not wait for the law to catch up will bring more harm and privacy violations to those who deserve the most protection. Therefore, in an effort to keep up with the technological advancements and ensure a safer school environment, states should create legislation specifically directed to online student interaction at school.

III. THE STRUGGLE BETWEEN SCHOOLS AND COPPA

The applicability of COPPA to the school setting has been unclear since its inception. Although the FTC seemed to

Secondary Education Act of 1965, 20 U.S.C. § 6311. *Id.*

[90] *See* Benjamin Herold, *Student Data Privacy Mostly Missing in ESEA Reauthorization*, EDUCATION WEEK (Dec. 1, 2015, 12:23 PM). In its enacted form, the Every Student Succeeds Act focuses more on a school's accountability in ensuring academic achievement. *See* Every Student Succeeds Act, 114 P.L. 95, 129 Stat. 1802 (2015); EXECUTIVE OFFICE OF THE PRESIDENT, EVERY STUDENT SUCCEEDS ACT: A PROGRESS REPORT ON ELEMENTARY AND SECONDARY EDUCATION (Dec. 2015). The Every Student Succeeds Act does the following: ensures that states set high standards, maintains accountability, empowers states and local decision-makers to develop their own educational improvement systems, preserves annual assessments and reduces the burden of erroneous and ineffective testing, provides more children access to high-quality preschool, and establishes new resources to test teaching strategies and their success. *Id.* at 1–2. Congress only addresses student privacy vaguely within the text, with broad findings such as, "Students' personally identifiable information is important to protect;" "Students' information should not be shared with individuals other than school officials in charge of educating those students without clear notice to parents;" and "With the use of more technology, and more research about student learning, the responsibility to protect students' personally identifiable information is more important than ever." Every Student Succeeds Act, at §§ 8545(a)(1)–(3).

[91] *See Lowdown on Federal Legislation 2015*, *supra* note 76. Originally, the legislation was to include the creation of a Student Privacy Committee for enforcement and for clarifying unclear definitions, such as "third party" and "personal identifiable information." *Federal Legislation Chart*, *supra* note 77, at "ESEA Amendment" column. The committee was to ensure that identifiable data could not be used for targeted advertising or marketing and that a student's data could be deleted upon request. *Id.*

recognize the need for COPPA protection within schools, it stated in its response to notice and comment and within its Statement of Basis and Purpose that since "many schools already seek parental consent for in-school Internet access . . . the operator can presume that the school's authorization is based on the school's having obtained the parent's consent."[92] This creates an extra barrier for third-party operators in gaining verifiable parental consent, and further begs the question of whether the contractor must "double-check" the school's consent policies. Such a burden creates the uncertainty of consistent COPPA enforcement. The burden should not be on the operators alone—schools should have some of the responsibility of ensuring the protection of their students' privacy rights. With technology more prevalent than ever in the classroom, measures should be taken to ensure both protection of our most vulnerable citizens while in school and protection of a parent's right to give consent.

A. The FTC's Unsettling Guidance to Schools: The Problem with Allowing Schools to Give "Verifiable Parental Consent"

In March 2015 the FTC released FAQs that specifically address how schools can seek compliance with COPPA. Schools must confirm that the services they use comply with federal law, including COPPA for schools that teach children under thirteen.[93] Under COPPA, the FTC said that schools may act as a *parent's agent* in giving consent when the services are solely for an educational purpose to benefit the school,[94] and that the operators of the educational online services may *presume* that the school has reasonably obtained proper parental consent so long as the student's personal information is not used for commercial purposes.[95] While such guidance could be considered reasonable, presuming that a school always provides notice to parents and gains verifiable parental consent before contracting with a new third party is unrealistic.

This is the main flaw with the FTC's compliance guidance for schools. Not only does it take control out of the hands of the

[92] 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999).

[93] Mutkoski, *supra* note 2, at 519.

[94] *2015 Guidance*, *supra* note 21, at (M)(1).

[95] *Id.* at (M)(2).

parents, but it also places an extra burden on third party contractors. The contractors must ensure that the consent methods used by schools are "reasonably calculated" when relying on the school as a proxy for parental consent.[96] This seems to take away responsibility from schools in protecting the privacy of their students under the age of thirteen. Without responsibility on the schools to uphold COPPA, collecting a young child's data while at school becomes easier, especially when there is no careful oversight or parental involvement required. Therefore, allowing schools to give "verifiable parental consent" opens the door for many possible COPPA violations.

Allowing a school to provide "verifiable parental consent" to an online operator on behalf of a parent seems to be the most efficient and least burdensome method to educate students in the technological era. Having to inform every single parent of a child under thirteen of all the collection and privacy disclosures of every single application or website the child uses could waste a great amount of time, energy, and resources. In addition, it is likely that some parents will deny their child's involvement, arguably placing the child at an educational disadvantage. Advocates for schools acting *in loco parentis*—"in the place of a parent"—believe that "[requiring] one more administrative step . . . saddles already overburdened educators and schools with one more level of effort and is likely to further hinder the delivery of effective online education."[97] However, exposing young children's personal information and surrendering their parents' ability to protect them can produce an even greater harm.[98] A desire for efficiency and a virtual classroom does not outweigh the privacy rights of society's youngest members and the parental right of control.[99]

---

[96] *Id.* However, if the operator intends to use the student's data for other commercial purposes, the operator must obtain actual parental consent. *Id.*

[97] Hostetler & Okada, *supra* note 27, at 199.

[98] *See supra* Part I.

[99] According to a survey conducted from March 26, 2015 through April 2, 2015, while the majority of parents are comfortable if their child's data is collected solely for the purpose of educational benefit, they generally disagree with the use of their child's personal data for commercial purposes. *Beyond the Fear Factor, supra* note 2, at 8. Appropriate educational purposes that parents believe are okay to collect include grades, attendance records, special needs status, standardized test scores, and disciplinary records. *Id.* Most parents are comfortable with the child's principal, teachers, and schools using the information. *Id.* at 8–9 (showing that 89% of parents are comfortable with their child's principal and teachers having access to their child's

There are two major problems with a school giving "verifiable parental consent" on behalf of the child's parents. First, it is difficult for the online operator to authenticate the consent given by the school.[100] Under COPPA, an online operator must make sure that the school offering the parental consent has used "reasonably calculated" methods to obtain consent.[101] The operator must ensure that the school is providing authentic consent, not falsified consent such as a child pretending to be a teacher.[102] The second problem is determining which school officials may provide the consent.[103] The FTC recommends that the school district or individual school be responsible for making the decision to use the operator's services and forming the contract.[104] However, in many cases it is the individual teachers who make such decisions.[105] From technological and legal standpoints, this may not always be the best method.[106]

Without proper training and understanding, both school districts and teachers may lack the expertise and knowledge of the law required to make a completely informed decision, and may enter into contracts with operators that are in violation of COPPA.[107] These decision makers may not know of the required privacy and collection disclosures that operators must provide, and may in turn fail to discover the operator's true collection purposes or fail to get additional parental consent if so required.[108] This is especially the case with free applications

---

information). However, most parents are not comfortable with companies that create educational software, websites, and applications having access to their child's data. *Id.* (providing the statistic that only 42% of parents feel comfortable with companies that create educational software, websites, and apps having access to their child's information).

100 Kelsey Finch, *COPPA in the Classroom*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (May 7, 2014), https://iapp.org/news/a/coppa-in-the-classroom/.

101 *2015 Guidance*, *supra* note 21, at (M)(2).

102 *Id.*

103 *See* Finch, *supra* note 100.

104 *2015 Guidance*, *supra* note 21, at (M)(3).

105 *See* Finch, *supra* note 100.

106 A recent survey conducted among 4,300 teachers found that 49% of teachers believed that parents should have the smallest role in deciding what technology to use in the classroom. Dian Schaffhauser, *Teachers: We Want More Control over Ed Tech Decisions*, THE JOURNAL (Dec. 16, 2015), https://thejournal.com/articles/2015/12/16/teachers-we-want-more-control-over-ed-tech-decisions.aspx.

107 *See* Finch, *supra* note 100*; PBS NewsHour*, *supra* note 5, beginning at 3:47.

108 A Fordham Law study published in 2013 found that "as a governance matter,

since they are funded mostly through targeted marketing and the collection of the user's information.[109] Additionally, the operators' presumption of "verifiable parental consent" when contracting for educational purposes requires that they either simply trust that the school acted accordingly with COPPA or investigate the school's methods, which seems highly inconvenient and unlikely to occur.

If the school does indeed fail to comply with COPPA, it is not the school that is most harmed or punished. It is the children and parents who face harm to their rights, and the operators that risk federal fines and punishment. Schools lack any incentive to ensure compliance with COPPA. Without uniform procedures laid out for schools to ensure enforcement, the guessing game of whether actual "verifiable parental consent" has been obtained will continue, as will the loss of privacy rights for society's most vulnerable members. With failure on the federal level to ensure that "verifiable parental consent" has been obtained, the best way to achieve a uniform system of enforcement is through state law.

B. Examples of How States Are Responding

Since COPPA's application to the school setting is still unclear and fails to be adequately addressed at the federal level, many states have begun enacting their own legislation to fix the gaps between child privacy, parental consent, third-party operators, and the classroom. Because COPPA has a state law preemption clause[110] that prevents the states from rewriting their own versions of COPPA, legislators are tasked

approximately 20% of the responding districts had no policies addressing teacher use of information resources." Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, FORDHAM LAW SCHOOL CENTER ON LAW AND INFORMATION POLICY, 24 (Dec. 13, 2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip (finding that 95% of districts rely on cloud services for a variety of functions). In such cases, the school administration has no oversight of the transfer of student information. *Id.* The study provides the following example: "[I]f a school principal or teacher decided to use a service such as Dropbox for students to share family photos, the central administration would not have the opportunity to vet the terms and conditions of the service and would not have the ability to ensure COPPA compliance." *Id.*

[109] Tudor, *supra* note 3, at 311.

[110] 15 U.S.C. § 6502(d) (1998) (stating that "No State or local government may impose any liability for commercial activities or actions by operators . . . in commerce in connection with an activity or action described in this title that is inconsistent with the treatment of those activities or actions under this section.").

with creating very narrow, school-specific, privacy legislation to ensure that there is no conflict with the COPPA scheme.[111] Some common approaches to state legislation include creating unambiguous, school-specific language, increasing the level of transparency between the third-party contractor and the parent, and forming privacy task enforcement committees or appointing officers to oversee compliance.

1. Unambiguous school-specific legislation

The most successful and strict piece of privacy legislation, the Student Online Personal Information Protection Act (SOPIPA),[112] comes from California and has served as a model for many other states.[113] It focuses specifically on the interactions of K–12 schools and online operators[114] and eliminates confusion over parental consent by providing specific, all-inclusive prohibitions.[115] Unlike federal legislation, SOPIPA does not allow an operator to use the students' information for *any* commercial purpose, so a convoluted parental consent provision is not necessary.[116] SOPIPA prohibits targeted marketing, the creation of student profiles for commercial purposes, and the sale of a student's information.[117] It also requires that an operator "implement and maintain reasonable security procedures and practices" and "delete a student's covered information if the school or district requests deletion of data under the control of the school or district."[118] California's new law is the first of its kind and has inspired other strict state legislation protecting the privacy rights of young students, especially in states like Washington, Utah, and Delaware.[119]

---

111 *See COPPA +1: Issues and Impacts For Children's Privacy*, *supra* note 38.

112 CAL. BUS. & PROF. CODE § 22584 (2014).

113 *See* Tanya Roscorla, *More States Pass Laws to Protect Student Data*, CENTER FOR DIGITAL EDUCATION (Aug. 27, 2015), http://www.centerdigitaled.com/k-12/What-States-Did-with-Student-Data-Privacy-Legislation-in-2015.html?utm_source=related.

114 CAL. BUS. & PROF. CODE § 22584(a).

115 See *id.*, at (b).

116 *See Id.*

117 CAL. BUS. & PROF. CODE § 22584 (b)(1)–(3).

118 *Id.* at (d).

119 *See* Roscorla, *supra* note 113.

2. Increased transparency between third-party operators and parents

Washington's most recent student privacy law, The Student User Privacy in Education Rights Act (SUPER Act),[120] promotes a greater amount of transparency between the online service providers and the schools. Specifically, the law requires that the operators provide a clear and easy-to-understand explanation about the types of information they collect, give notice before making material changes to their privacy policies for school services, and facilitate access to and correction of a student's personal information if so requested by the student, parent, school, or teacher.[121] Like COPPA, the SUPER Act only allows the school to give consent on behalf of the parent for educational purposes.[122] Similar to SOPIPA, this law only applies to student-oriented services, not to services that are designed and marketed for individuals or entities generally.[123] While the language found in COPPA creates confusion with regard to "verifiable parental consent" and carries unclear application to the school setting, the SUPER Act provides specific school scenario-based guidance, leaving little room for inconsistent application by the school and misunderstandings of consent and notice responsibilities.[124] With more transparency and little room left for interpretation, a law like this would likely be much easier to enforce. Having such thorough requirements for transparency should be necessary to ensure that all parties involved—schools, third-party operators, parents, and even students—are aware of their responsibilities and protections in such a new, emerging classroom interaction.

3. Privacy task enforcement officers/committees

Other states, like Utah, have taken a slightly different,

---

[120] WASH. REV. CODE §§ 28A.604.010–.903 (2015).

[121] *Id.* at § 28A.604.020(1)–(3).

[122] *Id.* at § 28A.604.030(1). Parents retain full control when the operator desires to use the student's personal information for commercial purposes. *Id.*

[123] *Id.* at § 28A.604.010 (1)(a)*; see* CAL. BUS. & PROF. CODE § 22584(a) (2014).

[124] For example, Section 3 discusses the "Obligations of School Service Providers—Transparency," Section 4 discusses "Obligations of School Service Providers—Choice and Control," and Section 5 discusses "Obligations of School Service Providers—Safeguards." S.B. 5419, 64th Leg., Reg. Sess. §§ 3–5. In addition, Section 6 discusses how the prohibitions apply to adaptive learning and customized education. *Id*. at § 6.

more enforcement-based approach.[125] Until it was recently repealed in May 2016, Utah's law explicitly designated the considerations of maintaining, securing, and safeguarding student data to the state board of education. The state board of education also provided disclosures to parents and students on how the students' data would be collected and used and managed contracts with third-party service providers.[126] This scheme filled the inconsistent enforcement gap created by COPPA and lessened the uncertainty of *who* is responsible for ensuring the child's privacy security while at school. Additionally, the law created a "chief privacy officer," who was required to "oversee the administration of student privacy laws" and "work with the board to develop funding proposals and recommendations . . . ."[127] Designating such enforcement responsibilities to an entity whose sole job is privacy oversight is likely the best method of improving the level of enforcement and guaranteeing that a student's personal information is not collected and used inappropriately. In order to avoid the loss of a child's privacy rights due to lack of clear administrative guidance, such privacy officers should be appointed on a wider scale.

C. How States Should Respond: Prohibitive and Governance Approaches

Even though statues like California's SOPIPA, Washington's SUPER Act, and Utah's "chief privacy officer" law are being enacted, not all fifty states have adopted such student-data privacy legislation to govern online interactions in the classroom.[128] Since 2013, safeguarding student privacy has emerged as top priority in nearly every state's legislative

---

[125] UTAH CODE ANN. § 53A-1-711 (2015) (repealed by Laws 2016, c. 221, § 18, eff. May 10, 2016 (H.B. 358), http://le.utah.gov/~2016/bills/static/HB0358.html). To access the language of the repealed statute, see UTAH STATE LEGISLATURE, http://le.utah.gov/xcode/Title53A/Chapter1/C53A-1-S711_2015051220150512.pdf.

[126] UTAH STATE LEGISLATURE , UTAH CODE ANN. §§ 53A-1-711(2)–(3) (2015), http://le.utah.gov/xcode/Title53A/Chapter1/C53A-1-S711_2015051220150512.pdf.

[127] *Id.* at § (4)(b).

[128] *Student Data Privacy Legislation: What Happened in 2015, and What is Next?*, DATA QUALITY CAMPAIGN, 1 (Sept. 2015), http://2pido73em67o3eytaq1cp8au.wpengine.netdna-cdn.com/wp-content/uploads/2016/03/DQC-Student-Data-Laws-2015-Sept23.pdf, (stating that twenty-one states passed student-data privacy laws in 2014 and fifteen states passed student-data privacy laws in 2015).

agenda.[129] However, legislative proposals have differed greatly among the states—particularly between prohibitive approaches and governance approaches.[130] A prohibitive approach "seeks to ensure student privacy by preventing or halting the collection of a certain type of data . . . or a certain data use . . . ."[131] A governance approach "seeks to amend or establish the procedures (e.g., security audits, public lists of data collected), roles and responsibilities (e.g., establishment of a chief privacy officer, description of school board and legislature roles), and supports (e.g., state leadership) needed to ensure that data are used appropriately."[132] While each approach has proven to be successful on its own, there is a higher chance (based on 2015 data) that a combined approach is more successful at reaching enactment.[133] One piece of legislation that seems to have successfully combined these approaches is Delaware's Student Data Privacy Protection Act.[134] For example, under the prohibitive approach, the Act prohibits online service providers that offer services for K–12 from selling student data, using student data for target advertising, amassing a profile for non-educational purposes, and disclosing student data in a manner not permitted by the Act.[135] Under its governance approach, the Act creates a "Student Data Privacy Task Force," similar to Utah's, with an extremely detailed composition of members.[136]

---

[129] *Id.* at 2. Common questions among legislators in 2015 included the following:

> (a) how can schools use education technology, applications, and websites in support of student learning while still safeguarding student privacy?; (b) how can states best address the differences in the users and uses of data collected by the district and data collected through the use of online services?; (c) how can states best implement privacy laws and support their districts' privacy policies and activities?; and (d) how can states best develop privacy and data use policies that address immediate questions and concerns and allow for responsive governance decisions in the future?

Id.

[130] *Id.* at 3 (stating that 125/182 proposed bills in 2015 were prohibitive in nature (with 79/110 in 2014) and that 122/182 proposed bills in 2015 were governance based in nature (with 52/110 in 2014)).

[131] *Id.*

[132] *Id.*

[133] *Id.* at 8 (showing that in 2015, while 15/125 prohibitive approach proposals were signed into law and 24/122 governance approach proposals were signed into law, 11/73 proposals that combined the prohibitive and governance approaches became law).

[134] Student Data Privacy Protection Act, S.B. 79, 148th Gen. Assemb., Reg. Sess. (Del. 2015) (amending 14 DEL. CODE ANN. §§ 8101A–8106A). With this law, the legislature sought to balance a student's educational opportunities without compromising the privacy and security of the student's information. *Id.* at "Synopsis."

[135] *Id.* at § 1 (amending 14 DEL. CODE ANN. §§ 8105A(1)–(4)).

[136] *Id.* at § 3. The statute states:

Like California, Delaware adopted legislation that creates all-inclusive prohibitions, thereby removing the confusion created by a commercial collection parental consent requirement. States that lack sufficient student data privacy laws should follow the combined approach taken by Delaware to ensure both that harmful actions by third-party operators are prohibited and that efficient measures are in place at schools to monitor compliance.

For example, one such state that is in need of adequate student-data privacy laws is Tennessee.[137] The current law in Tennessee, enacted in 2014, only expands protection for information within a school educational record, failing to address the classroom interactions between schools and third-party operators.[138] Failure to have a uniform law across the state leads to a patchwork of inconsistent district policies, which in turn leads to different protections for students based on district. For example, the Williamson County School District implemented the BYOT initiative, or "Bring Your Own Technology" initiative during the 2012–2013 school year.[139]

> The Task Force is composed of the Attorney General, the Secretary of Education, the President of the State Board of Education, the Secretary of the Department of Technology and Information, the Chief of the State School Officers Association, the President of the Delaware School Boards Association, the President of the Delaware Charter Schools Network, the President of the Delaware State Education Association, and the President of the Delaware Congress of Parents & Teachers, Inc., or their respective designees, and two representatives from companies, trade associations, or groups which operate in the area of student data privacy or online educational technology services, appointed by the Chairs of the Education Committees of the Senate and House of Representatives.

Id.

[137] Based on a 2012 survey conducted on seventy public Tennessee schools whose students used personal devices in the classroom, 43% of the participating schools used PC laptops, 22% used Apple iPads, 17% used netbooks, 12% used Apple Mac laptops, and about 6% used some other form of electronic device in the classroom. Doug Wright, *Digital Textbooks in K-12 Schools*, OFFICE OF RESEARCH AND EDUCATION ACCOUNTABILITY, TENNESSEE COMPTROLLER OF THE TREASURY, JUSTIN P. WILSON, at 3–4 n. F (Oct. 2013), http://www.comptroller.tn.gov/Repository/RE/Digital%20Textbooks.pdf (citing a survey conducted by the Technology in Education Survey System at the Center for Research in Education Policy at the University of Memphis, http://www.crepsurveys.net/TESS/StateUserHomepage.jsp?public=1 (accessed Sept. 25, 2013)). While Tennessee recently enacted an education law in 2014, it does not address the interactions between schools and third-party operators. *See* H.B. 1549, 108th Gen. Assemb. (Tenn. 2013).

[138] *See* T.C.A. § 49-1-703 (2014).

[139] *See* WILLIAMSON COUNTY SCHOOLS, INSTRUCTIONAL TECHNOLOGY: BYOT QUESTIONS AND ANSWERS (Mar. 8, 2012) [hereinafter BYOT Q&A], http://www.wcs.edu/wp-content/pdf/InstructionalTechnology/BYOTQA.pdf. This program allows students in grades 3–12 to either bring a portable electronic device

Under this program, each student is assigned a Gmail email account and uses Google Docs[140]—a type of cloud computing that requires interaction with online service providers. Such a program is exactly the type that requires the protection of laws like COPPA, SOPIPA, the SUPER Act, or Delaware's Student Data Privacy Protection Act. Since the state of Tennessee has not passed any legislation guiding the school districts in such a manner, the Williamson County school district itself created its own policies to govern the BYOT initiative.[141] While these policies are strict and require great levels of school monitoring, they differ from other school districts—like Shelby County School District. The Shelby County policies provide a more exhaustive list of the actions that can and cannot be taken by students and other users generally.[142] Williamson County is more governance based while Shelby County is more prohibition based. On its face, it seems that the Shelby County School District offers more protections for students than the Williamson County School District. If states in similar situations want to provide uniform protection for *all* school children and avoid a patchwork of inconsistent district policies,

with full Internet capabilities or check out a device owned by the school in order to enhance classroom learning—including smartphones, iPads and tablets, iPods, laptops, netbooks, and eReaders. *Id.; see also* WILLIAMSON COUNTY BOARD OF EDUCATION, ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET SAFETY PROCEDURES, at 6 [hereinafter WILLIAMSON INTERNET SAFETY PROCEDURES], http://www.wcs.edu/wp-content/pdf/BoardPolicies/4406p.pdf.

[140] BYOT Q&A, *supra* note 139.

[141] According to the district's "Acceptable Use, Media Release, and Internet Safety Procedures," students must remain connected to the Williamson County School's guest network at all times in order to be monitored by teachers for safety reasons. WILLIAMSON INTERNET SAFETY PROCEDURES, *supra* note 139, at 2. As long as the child is connected to the district's network, the district is able to restrict and filter the information that the student is allowed to access. *Id.* Additionally, the district reserves the right to collect and examine a student's device if there is a reasonable suspicion that the student is violating school policy or the law. *Id.*

[142] See *Student Access Release and Authorization Form*, SHELBY COUNTY BOARD OF EDUCATION, http://www.scsk12.org/schools/whitestation.ms/site/documents/StudentInternetAgreement.pdf. For example, the policy states, "Students shall not transmit personally identifiable or personal contact information about themselves or others, except the student's e-mail address, without prior consent by the parent and the teacher. Personally identifiable or personal contact information shall include name, address, telephone number, photograph, social security number, school name, and classroom." *Id.* at 4. Additionally, the policy states, "The [Memphis City Schools (MCS)] network may be used only for educational and professional purposes consistent with the MCS's goals. Commercial use (advertisements, business logos, etc.) of the MCS network is prohibited, unless specifically permitted in writing by the Department of Communications." *Id.* at 5.

then they should adopt legislation that both expressly prohibits potentially harmful actions by third-party operators and provides rules of governance, which school districts must follow in order to ensure that each student is protected. Since federal attempts have failed to provide adequate protection for students in these situations, a combined prohibition-governance approach is likely the best method of ensuring data privacy protections at the state level.

IV. PROPOSED STATUTORY APPROACH FOR STATES

The best approach for a state in constructing new legislation is to implement unambiguous guidelines, clear prohibitions, and a workable governance plan.[143] The ultimate goal, as executed in Washington,[144] should be not only to ensure a student's privacy protection while interacting online in the classroom, but also to create a level of transparency for all parties—students, schools, third-party operators, and parents.[145] All parties should be aware of the rights afforded to students, the prohibited behaviors of a third-party operator, and the enforcement responsibilities of the school. Therefore, in order to avoid a COPPA-like situation where it is unclear when consent is needed, who may give consent, and who is responsible for double-checking that consent has been properly obtained, the following proposals will provide strict guidelines, leaving no room for such questioning. A state statute following this prohibitive-governance approach will likely create uniformity in states with a patchwork of varying district policies.

---

[143] *See Student Data Privacy Legislation: What Happened in 2015, and What is Next?*, *supra* note 128, at 3; *see also* Mutkoski, *supra* note 2, at 530–32 (discussing the best practices that should be implemented in educational institutions for cloud computing practices).

[144] *See* S.B. 5419, 64th Leg., Reg. Sess. §§ 3–5 (Wash. 2015). For example, Washington's SUPER Act states, "School service providers shall provide clear and easy to understand information about the types of student personal information they collect and about how they use and share the student personal information," and "School service providers must obtain consent before using student personal information in a manner that is materially inconsistent with the school service provider's privacy policy or school contract for the applicable school service in effect at the time of collection." *Id.* at §§ 3(1), 4(5).

[145] Most parents do not know what the student data privacy laws entail, therefore, creating transparency is critical. *See Beyond the Fear Factor*, *supra* note 2, at 14 (finding that 54% of parents "do not know anything about federal laws that restrict what public schools can do with their child's information.").

A. Prohibitive Proposals

One way to eliminate ambiguous interpretation is through clearly-worded guidelines and prohibitions. Because this proposal deals exclusively with the interactions between students and third-party operators, creating complete prohibitions allows for easy enforceability. Such unambiguous language will not only make the restrictions understandable, but it will also create transparency so all parties involved know what to expect for a legal, online classroom interaction to occur. The following provisions should be included in a state's legislative proposal or amendment in order to ensure that a child receives complete protection from illegal collection of personal information, sale of personal information, or identity theft while using classroom applications in school.

1. "In a K–12 institution,[146] no operator shall knowingly engage in targeted advertising, sell a student's information, or use a student's personal information[147] for any purpose other than the educational purpose for which the operator was contracted, unless disclosure is made for reasons required by law or court order."

Prohibitions should be straightforward and should not provide opportunities for evasion.[148] This provision does not allow an operator to engage in *any* commercial purposes while providing services to students within a school, offering absolute protection for students. This absolute prohibition also eliminates any of the previous confusion caused by the need to obtain "verifiable parental consent" so that the operator may engage in commercial activities.[149] A list of exceptions would

---

[146] Instead of imitating COPPA, state legislators should make the law applicable to all students in elementary through high school. This age range promotes not only equal protections for all minor students, but also uniformity with other existing education privacy laws, thus eliminating any kind of confusion.

[147] The definition of "personal information" should mirror that found in Delaware's law, including not only a list of physical information—such as residential address—but also the different ways in which "personal information" is created, such as through an online profile created by the student while using the operator's service. *See* Student Data Privacy Protection Act, S.B. 79, 148th Gen. Assemb., Reg. Sess. at § 8102(A)(16) (Del. 2015).

[148] *See* CAL. BUS. & PROF. CODE § 22584 (2014). SOPIPA does not include an extensive list of exceptions, as seen in COPPA (15 U.S.C. § 6502(b)(2)), thus making clarity and enforceability difficult.

[149] *See supra* Part III(A).

leave states with the same problems that already exist under federal law. Forming such a strict and specific law will prevent both inconsistent interpretation and potential violations of student privacy.

2. No operator shall refuse to delete a student's information if the student or the student's parent requests the removal of such information from the operator's control.

Borrowing from the proposed Do Not Track Kids Act of 2015, this proposed provision creates an "eraser button" to allow a student's personal information to be deleted upon request.[150] Such an option gives not only the student control over his or her information, but also allows parents to exercise their right of parental control over their minor child's interactions. Having an "eraser button" requirement ensures that only operators with non-commercial intentions that are willing to leave control in the hands of the students and their parents are allowed to contract with schools for interactive classroom purposes.

3. Any third-party operator that wishes to contract with a school for educational purposes must disclose all collection policies. School districts must approve the operator's collection policies before the operator may engage with the students.

This provision draws from The Student Digital Privacy and Parental Rights Act of 2015, which requires operators to publicly list what type of data they collect, how it is used, and whether it is shared in a clear and easy-to-understand manner.[151] Making such policies available to schools before any contract agreement is entered into is the best way for the school to prevent the possibility of any privacy violations. In addition, it provides the greatest amount of transparency, not only between the school and the third-party operator, but also between the third-party operator and parents since the school must also relay the operator's collection policies to the

[150] *See* H.R. 2734, 114th Congress, at § 6(b)(1) (2015–2016) (stating that no later than one year after the enactment of the Act, the commission must promulgate a rule "to implement mechanisms that permit a user . . . to erase or otherwise eliminate content or information submitted . . . that is publicly available . . . and contains or displays personal information of children or minors."). Additionally, the operator must make users aware of the mechanism. *Id.*

[151] H.R. 2092, 114th Cong. at § 3(b)(3) (2015).

parents.[152] Having clear-cut guidelines and prohibitions is likely the most effective way to eliminate ambiguous interpretations.

B. Governance proposals

Governance and enforcement procedures are also crucial in ensuring that the protective measures in place remain effective. Since the students' interactions with the operators take place within the classroom, it is logical that the majority of enforcement responsibilities should fall on the school. Unlike COPPA, which makes it the responsibility of a third-party operator to ensure that proper consent is obtained, this proposal requires that the school take extra preventative measures to ensure that violations are avoided. Involving schools heavily in governance is the best way to create transparency and keep operators in check. Because parents already entrust schools with their child's physical safety, trusting schools with children's online safety is not an unrealistic expectation. States should consider the following provisions to improve their enforcement methods and keep their new restrictions effective.

1. The Board of Education shall establish a Student Data Privacy Task Force to research and make recommendations regarding the development and execution of current student data privacy laws and policies.

Creation of an enforcement task force is another way in which schools can ensure that their students are receiving adequate protection. Like Delaware and Utah, states should create a privacy task force specifically designated to oversee school district compliance with state law and the school's specific privacy policies.[153] The purpose of the task force is "to study and make findings and recommendations regarding the development and implementation of a comprehensive framework to govern the privacy, protection, accessibility, and use of student data within and as part of the State's public

[152] *See infra* Part IV(B)(2)(3).

[153] *See* Student Data Privacy Protection Act , S.B. 79, 148th Gen. Assemb., Reg. Sess. § 3 (Del. 2015); UTAH CODE ANN. § 53A-1-711 (2015) (repealed by Laws 2016, c. 221, § 18, eff. May 10, 2016 (H.B. 358), http://le.utah.gov/xcode/Title53A/Chapter1/C53A-1-S711_2015051220150512.pdf).

education system."[154] Creating a task force removes the enforcement burden from teachers and school administrators who have other administrative duties to uphold. Each member of the task force must be properly educated and trained in technology and privacy law before holding a position. Legislators should look to Delaware's Student Data Privacy Protection Act to determine what individuals may best suit the position.[155] With a designated enforcement task system in place, schools can seek to ensure that their students are better protected.

2. Any teacher or school administrator who intends to allow students to access an online service for educational purposes while at school must participate in a certified student-data privacy course at least once a year.

Without proper training and understanding, both school districts and teachers may lack the expertise and knowledge of the law required to make a completely informed decision, and may enter into contracts with operators that are in violation of relevant student-data privacy law.[156] Since it is usually individual teachers who make the initial decision to use an operator's services,[157] it would be highly irresponsible if the decision-maker selected a service without ensuring the proper protections are in place. Therefore, any legislative effort presented by states should require teachers to participate in a mandatory student privacy course at least once a year.

3. Any teacher or school administrator who intends to allow students to access an online service for educational purposes while at school must provide parents with the operator's collection policies and receive consent prior to the introduction of the online service to the students in the classroom for its use.

This provision stems from the basic notion that parents should maintain control over their child's interactions. If a parent thinks that a particular activity may be harmful to his or her child's privacy, that parent should have the ability to

---

[154] Student Data Privacy Protection Act, S.B. 79, 148th Gen. Assemb., Reg. Sess. § 3 (Del. 2015).

[155] *See Id.*

[156] *See* Finch, *supra* note 100.

[157] *See id.*

disallow the child's participation.[158] Creating a provision that keeps parents abreast of an operator's collection policies is one of the most obvious ways of promoting transparency.

4. Each teacher or school administrator who engages students in online classroom interactions must keep a current log—that includes all services a student interacts with and the third-party operator's collection policies—in the event a parent or other authorized school administrator requests review of a student's interactions.

This provision seeks to create complete transparency between third-party operators, schools, and parents. Allowing for a quick reference is extremely helpful in both keeping track of the risks a student may face and for an inspection by an enforcement task force. Maintaining a log of all the services students use enhances the school's ability to closely govern the interactions between operators and students. By following these suggested guidelines, individual states will be able to fill the gaps left in the relationship between third-party contractors, students, parents, and schools. Such legislation will ensure that a child receives better protection from the illegal actions by third-party operators while using classroom applications in school.

V. CONCLUSION

Students must be protected from unwanted and illegal collection of their personal information. Although using technology is a great way for teachers to track student progress and to prepare students for their future technology-driven lives, it produces both risk for potential harm and places a greater level of responsibility on a school to protect its students. Current federal legislation (including COPPA) and recent federal legislative attempts have failed to adequately provide clear guidance for interactions between third-party providers and students in the classroom. Unfortunately, such federal laws are extremely confusing, difficult to apply, and are not strictly enforced, which has led to a heightened risk of

[158] *See generally* Every Student Succeeds Act, 114 P.L. 95, 129 Stat. 1802 § (e)(2) (2015) (providing that parents may opt their child out of testing). This new federal law demonstrates that parents should still have control over their child's education.

student privacy violations in the classroom. All states—particularly ones without laws governing classroom interactions—should adopt prohibitive and governance provisions to promote 1) an absolute, unambiguous protection of student privacy, 2) greater responsibility on schools for enforcement, and 3) transparency amongst third-party operators, schools, students, and parents. With the guidance and enforcement policies in the hands of the states, the risk of illegal collection and use of students' personal information will become more manageable.

*Alexis M. Peddy**

*J.D. Candidate, May 2017, The University of Memphis, Cecil C. Humphreys School of Law; B.A., Political Science, The University of Mississippi, 2014. I would like to thank Professor Andrew J. McClurg and Jacob Strawn for their dedicated help in the preparation of this work. I would also like to thank my family and friends for their love and support.