

# Children's Privacy: An Evaluation of EdTech Privacy Policies

**Tobi West**  
Coastline College  
Fountain Valley, CA USA

## Abstract

Due to social distancing requirements at the onset of the pandemic many schools suddenly transitioned to online learning platforms. Additionally, minors create a significant amount of digital assets, often without regard for privacy or future use. Without ill intent, adults may encourage children to create digital assets containing private information, potentially leading to future embarrassment. During the child's younger years, they have the autonomy to create digital assets, yet they do not have the legal right to determine the use or deletion of those assets.

Children's Online Privacy Protection Act (COPPA) is meant to protect children's privacy and as early adopters of new education technology, eager teachers are deciding which tools to use that may circumvent their school or district's approval processes. As features of their products, Education technology (EdTech) companies may share the data collected from children with third-party service providers to perform data analysis. Those service providers may not share the same compliance level in their privacy policy, putting the privacy and security of consumer data at further risk.

This study reviews the privacy policies of three EdTech tools for COPPA compliance based on the Federal Trade Commission's tips for consumers. The report includes information about the privacy implications of third-party data processing, the legal consequences of privacy violations after the collection of minors' digital assets, and an explanation of the privacy policy evaluation reports of EdTech tools provided by Common Sense Media with suggestions for parents, teachers, and school administrators.

**Keywords:** data privacy, privacy risk, compliance, EdTech tools, cybersecurity, student data

## 1. INTRODUCTION

Today's schoolteachers compete for student attention against online games and other web and mobile applications such as TikTok, Snapchat, and similar social apps. Even prior to social distancing requirements of the pandemic and the massive transition to online learning platforms for K-12 schools, teachers were looking for solutions that would be interesting and capture student attention to help them learn the concepts of the discipline (Chaiyo & Nokham, 2017). Many of these education technology (EdTech) tools provide supplemental instructional support through online engagement with students whilst capturing the data of minors which could infringe on the child's privacy rights (Chen, 2016). Websites such as Nearpod, Quizizz, Quizlet, Kahoot! collect students' personal information

and their responses to quiz questions or any other types of questions developed by teachers that can result in personal information being shared to the online platform.

EdTech tool sites reportedly have millions of students logging in on a regular basis. Children's Online Privacy Protection Act (COPPA) is intended to protect personal data and privacy for children under 13 and provides parents with the ability to control what information websites collect about their children and to have that data deleted upon request (FTC, 2020). Personal information collected about children under 13 is to be deleted after its intended purpose has passed. This can be interpreted by the companies to hold on to the data if no requests for deletion from parents, teachers, or schools are received. Some of the top-ranking sites include Edmodo with 87 million

users, SplashLearn with 30 million users, and Kahoot! with 50 million users (Chauhan, 2018) (Tutorful, 2020). Plunkett (2020) suggests that this type of data collection and sharing could lead to violations of the minor's privacy and may lead to embarrassing moments now or in the future because the data does not have an exact usage expiration.

During a 2019 student camp meeting, a teacher described how EdTech tools were used to help with online engagement for their Computer Science course. The teacher described the fun activities that students complete on the EdTech site, including a video scavenger hunt for items in the student's house, posting results to the online whiteboard, and other activities that asked questions about personal interests. From a data collection and student privacy perspective this is intriguing because the platform already collects personal information such as full name, age, and school and teacher affiliation which can lead to physical location and whereabouts during school hours. The teacher said she downloads the student response data in spreadsheet format from the site to evaluate for learning gaps and input grades to the classroom platform.

To better understand the issues, a review was conducted to evaluate the features, policies, and consent types that are publicly noted by three of the top ranked EdTech sites. This study compares the privacy compliance reports of these instructional support websites, services provided by third-party providers, forms of parental consent, and evaluates the privacy policies for compliance with COPPA based on Federal Trade Commission (FTC) tips (FTC, 2020).

## 2. BACKGROUND

Secondary schoolteachers may promote EdTech tools to engage with students in the online classroom and students are required to use them regardless of whether those applications are being introduced without direct consent from the parents (Peterson, 2016). Parents may expect that the EdTech websites are safe or that they have already been vetted by the teachers or school administrators when perhaps the tools have not been vetted to check for privacy measures to ensure that the students are safe and that the tool is compliant with COPPA requirements and other privacy regulations (Barrett, 2018). Additionally, teachers may require students to use the tools without a clear understanding of how the companies will use and share the data being collected. There is a lack of enforcement which may lead to further

compromise of student data privacy (Potaszniak, 2020).

The student data collected by the EdTech companies may be used in unexpected ways in the future, just as we have seen with the data brokering from social media platforms, such as Facebook, LinkedIn, and others. Currently there is a possibility that the data could also be shared with third-party providers that do not have the same levels of COPPA compliance, maybe the data are not shared in an aggregated form, or there could be other issues that may come up with third-party data sharing. The intent of this research is to inform secondary school teachers, EdTech tool developers, third-party companies, parents, and other privacy researchers of these possibilities and to show whether or not these EdTech platforms appear to be acting in compliance with regulations.

Another concern, teachers may download and save the student responses from the EdTech sites in spreadsheet format. While many teachers may have the best intentions with the data, such as using it for grading or analyzing for learning gaps, this miscellaneous storage opens many possibilities for data security and privacy risks. These digital assets, specifically the personal photos, videos, and private information that students may post during an online learning session, are at risk. Under existing law, Banta (2019) states that minors have no rights over their own digital assets such as email, social networking, documents, photos, text messages, and other forms of digital media.

### EdTech Tools

Broadly defined, EdTech tools are the technology devices and applications used by students, educators, and individuals in the course of learning (Peterson, 2016). This paper focuses on the web applications used by educators to assign tasks to students in their courses, to augment the capabilities of the school's curriculum and standard learning platform. Prior to the pandemic, in addition to use by online schools and individuals outside of the classroom, many teachers were already using EdTech applications in the physical classroom to provide alternative learning mechanisms.

EdTech tool providers range from small startups to well-established companies, and large tech giants like Apple and Microsoft. Many of the applications collect student interaction data to enhance the offerings and analyze the data to provide students with customized learning paths. That data is sometimes processed in conjunction

with students' private data for comparison to develop the custom learning path based on age, gender, geographic location, and other lessons completed.

The COVID-19 pandemic caused a sudden transition to online learning and a push for more EdTech tools due to the school campus closures, quarantine, and social distancing requirements (Dhawan, 2020). Not only were students thrust into using technology to complete their assignments, but they were also often required to use web-conferencing technology as well to interact with the teacher and their classmates (Sonnemaker, 2020). With so many privacy concerns to contend with, it is understandable that educators would turn to education technology to provide the ongoing education that students need.

Edmodo headquarters located in San Mateo, California offers an online education community environment for teachers, students, and parents to help students learn new skills. The organization states that it values enriching the lives of the community through improving education. Its goal is to help learners reach their full potential by connecting them to the people and resources they need (Edmodo, 2020). Edmodo offers some free services on the social learning platform and students can access additional services and functionality with a paid subscription (Cleverism, 2020).

SplashLearn intends to transform K-12 education through fun and personalization of the learning experience. Under the parent name of StudyPad, the company has locations in India and San Francisco, California (SplashLearn, 2020). SplashLearn focuses on K-5 math games and has options for classrooms and homeschoolers with breakouts for Common Core curriculum and online math mastery at each grade level. The website also includes a trust seal provided by kidSAFE Seal to show that the platform is COPPA Certified.

Kahoot! is an online platform that makes it easy for people of all ages to create, share, and play learning games (Kahoot, 2020). Kahoot! quizzes have reached far beyond the classroom and in May 2020, Kahoot! partnered with Microsoft to integrate the quiz platform into the Teams video conferencing application broadening the reach to more than 75 million users (Yahoo! Finance, 2020). Kahoot! was created in Oslo, Norway and has additional offices throughout the world in London, Paris, Austin, and Palo Alto, California.

### Digital Assets Created By Children

It is yet unclear whether social media and other digital assets are part of a deceased person's estate, according to Elliott this poses a risk to the ownership of those digital assets upon a person's death (Elliott, 2015). Similarly, minors cannot provide a clear plan for their own digital assets if they were to die before the legal age of consent, Banta (Potaszniak, 2020). Children are making a significant amount of digital assets daily through their online activities and the privacy, security, and future use of that data is at risk.

Third-party organizations may be contracted by the EdTech companies to assist with processing and analyzing personally identifiable information leading to data sharing and multiple copies of the data being stored in different locations. This additional transmission, sharing, and storage of the data poses increased risk to exposure and data breaches. Over the years, the number of third-party data breaches has continued to rise. Third-party breaches can result in millions of consumer records being exposed or malevolently placed on the dark web for sale to other cybercriminals (Winder, 2020).

### Privacy Laws

In addition to the handful of U.S. privacy laws that provide protections for citizens, the General Data Protection Regulation (GDPR) provides data privacy protection for citizens of the European Union (EU) and other countries that do business with EU citizens. For U.S. and California residents, there is the Children's Online Privacy Protection Act (COPPA), California Online Privacy Protection Act (CalOPPA), Family Educational Rights and Privacy Act (FERPA), and Student Online Personal Information Protection Act (SOPIPA).

Acronym	Full Title	Privacy Coverage	Penalty for Violation
COPPA	Children's Online Privacy Protection Act	Federal; children under 13	Allows for civil penalties of up to \$42,530 per violation
CalOPPA	California Online Privacy Protection Act	California; consumers of all ages	Fines of up to \$2,500 for each violation against an individual
CCPA	California Consumer Privacy Act	California; consumers of all ages	Fines of up to \$2,500 for each violation against an individual
CPRA	California Privacy Rights Act	California; separate rules for ages 0-13, 14-16, and 16+	Fines of up to \$7,500 for each violation against an individual
FERPA	Family Educational Rights and Privacy Act	Federal; students of all ages	Intentional violation can lead to school losing financial aid support
SOPIPA	Student Online Personal Information Protection Act	California; K-12 students	No specific provisions. Enforcement under Unfair Competition Law which could mean fines of up to \$2,500 for each violation against an individual
GDPR	General Data Protection Regulation	European Union; consumers of all ages	For severe infringements fines up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher

**Table 1: Privacy Regulations**

As of November 2020, California consumers have a new law, California Privacy Rights Act (CPRA) that will amend and supersede California Consumer Privacy Act (CCPA), beginning to go into effect in January 2023 (Bahar, Sand, & Wilson-Bilik, 2020). Privacy evaluators such as Common Sense Media tend to focus on compliance with the regulations of COPPA, CalOPPA, FERPA, SOPIPA, and GDPR due to the reach of the world wide web.

Many of the regulations describe what should be included in the privacy policy and how the data is collected, shared, stored, and the right to request deletion. COPPA compliance is required for websites or applications that target children under 13 and collect personal information or partner with third party companies to collect personal information, or a site that knowingly collects data from children under 13 while targeting a general audience or uses a third party to collect data from children under 13 through plug-ins or ad networks. To be compliant with COPPA for content targeted towards kids under 13, the operator must post a privacy policy that includes a list of all third-party operators that are collecting personal information, provides descriptions of the personal information in the user profile that is collected from kids under 13, describe how that information is collected and used, and describe the rights of the user's parents including a section that the operator will only collect what is reasonably necessary from users under 13 (Belding, 2018).

CalOPPA applies to websites that collect personally identifiable information (PII) from California consumers. It complements the COPPA requirements for privacy policies that protect children under 13 having first gone into effect in 2004 and then later amended in 2013. To be compliant with CalOPPA, a commercial website must prominently display a privacy policy that lists the PII that the website operator collects, provide a list of the categories of third-party service providers that the collected data may be shared with, a description of the process to notify users of changes to the privacy policy, and finally the effective date of the policy (Education Foundation, 2015).

CPRA was passed in November 2020 and is an amendment and expansion to CCPA which went into effect in January 2023. This includes the establishment of a new enforcement agency, California Privacy Protection Agency, responsible for implementation of consumer privacy laws (Hunton Andrews Kurth, 2020). CPRA may cause EdTech businesses to scramble for compliance

because they will be prohibited from sharing or selling personal data of California consumers younger than 16 (Rasch & Wilber, 2020).

FERPA is a federal law established in 1974 to protect student privacy for education records. This governs how others can access a student's education records, including employers, publicly funded educational institutions, and foreign governments. Parents have the legal right to view education records for kids under 18 and individuals over 18 have the right to view their own records. The Privacy Technical Assistance Center (PTAC) of the U.S. Department of Education (Privacy Technical Assistance Center, 2016) provides a Model Terms of Service to help EdTech companies understand how to be compliant with FERPA, which includes adding the following items to terms of service and privacy policies, a definition of data, de-identification of data, data may not be used for advertising or marketing to students or parents, must provide advance notice of changes to the policy or terms, collect only appropriate data, use data only for the purposes outlined in the policy, prohibit unauthorized data mining, prohibit sharing data with unauthorized parties, rights to data, provider's data will be shared with school/district upon request, and to employ adequate security controls.

Effective in 2016, SOPIPA was the first state law to comprehensively address student privacy. To be compliant with SOPIPA, educational websites, online services, or mobile application operators should not disclose student data that may be collected directly from the student, the school, or the school district, protect the collected information from unauthorized access, destruction, use, or modification through the implementation and maintenance of security procedures, and to delete data provided by a school or district as requested by that school or district. Some may say there are no penalties for non-compliance, yet others argue that enforcement under the Unfair Competition Law could result in fines up to \$2,500 per violation (Leong, Attai, Vance, & Rubin, 2016) (InfoLawGroup, 2016).

GDPR went into effect in 2018 for the European Union (EU) and has been impactful on other countries that wish to do business with the EU because these organizations must have privacy regulations in place in order to do so. To be compliant with the portion of GDPR specifically for minors under 16, organizations, including website and mobile application operators, must receive parental consent which may be in the form of

passport/ID copy by email, letter of authorization by email, processing transaction on parent’s credit card, via telephone (Minors and the GDPR, 2020).

**Assessing Privacy Compliance**

The FTC provided a list of questions that the school or districts should ask of EdTech providers to help assess the level of compliance with COPPA and the types of data that will be collected from students using the EdTech tool (FTC, 2020). The questions are not exhaustive, and the schools need to consider how the site or app would be used by teachers and students. The FTC’s questions have been paraphrased below.

- Types of personal information to be collected from students
- Uses for this personal information
- Use or share data for commercial purposes not related to the online services requested by the school? (e.g., online behavioral advertising, or building user profiles for commercial purposes.) If so, the school cannot consent on behalf of the parent.
- Must enable the school to review and request deletion of the student’s personal information. If not, the school cannot consent on behalf of the parent.
- Measures taken to protect the security, confidentiality, and integrity of the data
- Data retention and deletion policies for children’s personal information

**Terms of Service**

According to Rubin, the EdTech sites are marketing directly to teachers, circumventing the school’s and district’s processes for approval and as teachers seek new tools to engage with their students the enticements from new tools become very tempting. Additionally, teachers may not realize the future legal implications of their decision to accept the terms of service from the EdTech tool sites (Rubin, 2019). Teachers may not have the detailed knowledge of privacy laws such as COPPA and SOPIPA to make the determination as to whether the EdTech tools are compliant with the requirements for data storage, parental approval, and data deletion requests (Potaszniak, 2020).

**Consent**

When a site is considered purely educational, the FTC allows schools to obtain verifiable parental consent for the EdTech companies to collect children’s personal information. Consent can be given by the school, the district, the teacher, or the parent. This means that the school district,

school, or teacher may have access to request that children’s personal information be deleted.

For purely educational sites to accept consent from the school or teacher, they cannot share data collected from children under 13 for commercial purposes, the school must be able to review the child’s information collected, and the school must also be able to request deletion of information collected. Many schools will use a blanket policy regarding education technology tools and do not collect parent’s signatures for each tool being used or when new tools are introduced. Unless a scrutinizing parent objects to the use of a particular EdTech tool, students will use the sites they are told to submit data, or other files they are directed to create for assignments.

COPPA requires that a privacy policy state how consent is obtained. Through research and other studies, it has been shown that teachers and school districts have given consent on behalf of the student’s parents. The following table lists the consent types noted in the Privacy Policy for each of the education technology tools in this study.

EdTech Tool	Consent Type(s)
Edmodo	Must have parent’s or guardian’s consent; also suggests that teacher or school’s consent is acceptable in some cases.
SplashLearn	Verifiable parental consent. Does not mention alternative teacher or school consent.
Kahoot!	Does not knowingly request information from children under 13 and will delete upon parent’s request.

**Table 2: Forms of Consent**

The sites often do not explicitly describe how the consent is obtained or verified from parents or teachers. Many parents feel obligated to use the EdTech tools provided by teachers due to the sudden transition to the online learning environment at the start of the pandemic.

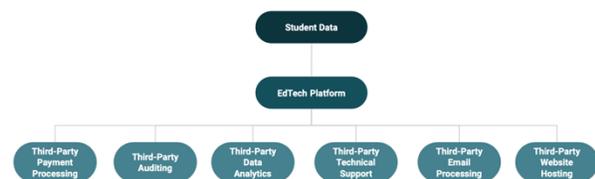
A comprehensive three-year analysis of 150 privacy policies from education technology applications was conducted by Common Sense Media, resulting in the 2019 State of EdTech Privacy Report (Kelly, Graham, Bronfman, & Garton, 2019). As noted in the report, most of the EdTech applications evaluated do not adequately define within their policies how privacy is preserved for student data. The authors explain that better-informed decisions can be made by

parents and schools using the information in the comprehensive report.

### Third-Party Data Processing

Third-party service providers are used to help process information collected by EdTech companies. These providers may send email on behalf of the company, process payments, perform data analysis for behavioral trends, or assist with technical support on the application or website. These processes require data from the original EdTech platform which may be in aggregate form or may be individualized as in the case of payment processing and technical support. Third-party data processors may not be required to maintain the same level of privacy protection as the primary company.

Third-party data processing often requires data transmission outside of the original organization and additional copies of the data to be stored in locations that may be outside of the original legal jurisdiction where the privacy protections can be different. This could lead to the data being used in ways other than the original intent, where it can be shared, sold, or rented to other parties. Another concern is fourth-party usage of data where the original privacy protections are not in place. This should be of great concern to parents, schools, and school administrators because students may upload videos, audio, narrative, or other private and sensitive information that is no longer protected when it is shared beyond the original EdTech platform.



**Figure 1: Data from EdTech Tools to Third-Party Providers**

### Third-Party Data Breaches

According to Data Leaks, at least 68 data breaches occurred in 2020 that led to millions of records being exposed for banks, healthcare providers, insurance carriers, telecom service providers, and other organizations. Specifically, WildWorks that has online safety experts on staff, had a third-party server expose 32 million usernames associated with parent accounts, encrypted passwords, and players’ birthdays and gender in November 2020 (Black Kite, 2020). WildWorks is an interactive game website for kids and families founded in 2003 (WildWorks, 2016).

Breaches of this volume demonstrate the need for EdTech companies to take measures to continuously remain in compliance with privacy regulations and share data responsibly to avoid privacy violations. When providing data to online companies, customers expect their data to be stored in a secure manner without having to understand the complexities of third-party data processing and cybersecurity. For this reason, organizations have a corporate social responsibility to secure and preserve the privacy of their customers’ data (West, 2020).

2020 Third-Party Breach Impact



**Figure 2: Third-party data breaches 2020**

## 3. METHODOLOGY

To evaluate these EdTech tools and compare them to COPPA, an analysis was conducted on each of the privacy policies compared to the FTC’s COPPA compliance tips. The evaluation rating by Common Sense Media for each of the tools is also provided as a reference. A review of the EdTech tool websites was conducted to document the notable features within the privacy policies relative to data protection for children and adults. Followed by a comparison as to how well each of the tools complies with the COPPA requirements.

To determine which EdTech tools to evaluate, a search was conducted for top EdTech tools for 2020 and articles were selected from those written or updated after the start of the pandemic in March 2020. From the top ten rated tools that claimed to have more than 30 million users according to Tutorful (2020) and Chauhan (2018). To evaluate the Privacy Policies, the contents were extracted from the site into a Microsoft Word document to highlight phrases and locate items that are relevant to COPPA compliance.

A search for COPPA compliance checklists revealed many articles that referenced the work of Common Sense Media, a company created by The Bill and Melinda Gates Foundation to help provide evaluation reports for children’s EdTech tools. These privacy evaluation reports were used for comparison in this study. Common Sense Media’s reports were detailed but not all the same, likely due to the timing of when each report

was written (Kelly, Graham, Bronfman, & Garton, 2019).

#### 4. DATA COLLECTION

The following information about Edmodo, SplashLearn, and Kahoot! was collected from their respective privacy policies and from the Common Sense Media privacy evaluation reports for analysis.

##### Intended Purpose and Volume of Users

Millions of users are engaged in these online learning platforms, many being K-12 students, around the world. Edmodo is similar to a social media type platform for teachers to communicate with students, colleagues, and parents. SplashLearn focuses on early-learning math concepts. Kahoot! thrives on user created quizzes to build their game-based platform. Table 4 details the purpose of this study’s EdTech tools, the year each company was founded, and the number of users.

EdTech Tool	Founded	Users
<b>Edmodo</b> K-12 learning management system	2008	87 million
<b>SplashLearn</b> preK-5 math	2010	30 million
<b>Kahoot!</b> Game-based quizzes	2012	50 million (75 million on MS Teams)

**Table 3: Number of Registered Users**

Each of the sites has a different purpose and say that they are focused on different target age ranges. Founded in 2008, Edmodo is a learning management system focused on collaboration, communication, and coaching where teachers can share content with students, distribute quizzes, and manage communications with education stakeholders including students, colleagues, and parents of students.

Founded in 2010, SplashLearn is a research-based immersive platform that targets pre-Kindergarten to 5th grade students with math lessons. SplashLearn uses a personalization engine to individually customize their math lessons. With the highest number of users of the three EdTech tools, Kahoot! relies on user-generated content to grow the quiz library on the site. Users may create private quizzes available to share from their own account or they may create publicly available quizzes for other platform users. Kahoot! opened as beta in 2013 and by 2016 announced 10 million public quizzes (The K!rew, 2016).

##### Types of Data Collected from Children

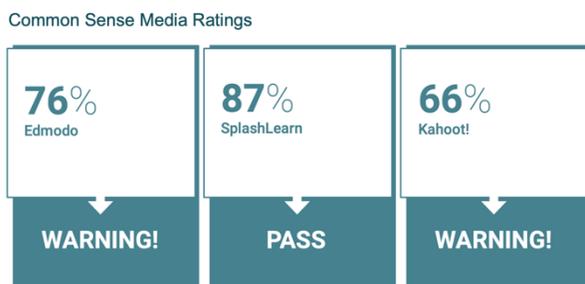
Table 4 lists the types of personally identifiable information collected from children by the EdTech sites according to their respective privacy policy (Edmodo, 2020) (SplashLearn, 2020) (Kahoot!, 2020). The column called *User’s Personal Info* describes the basic information collected when users create an account on the site. Additional data collection occurs with paid use of the site or when additional information is provided by the user upon further engagement.

EdTech Tool	User’s Personal Info	Additional Info Collected
Edmodo	Name, email address, and birth year.	Username, phone number, profile picture, school affiliation and location, billing and payment information, and other information in the course of providing Platform features or Edmodo Products. Info through third-party sign-on such as Google or Office 365.
SplashLearn	Screen name and gender.	Name or other identifier, student name, teacher email address, login dates, and times.
Kahoot!	None for unpaid users, only the player identifier.	Name, email address, username, and password. Geo-location is city-wide precision. Info through third-party sign-on such as Google or Office 365.

**Table 4: EdTech Data**

##### Privacy Evaluation Reports

Common Sense Media provides privacy evaluation reports about EdTech tools using a scored framework based on a variety of concerns and statutes including CalOPPA, COPPA, CCPA, FERPA, SOPIPA, and GDPR. The privacy concerns include data collection, data sharing, data security, data rights, data sold, data safety, ads & tracking, parental consent, and school purpose. Each concern is evaluated in detail by Common Sense Media with notes for each concern about what was included in the criteria. The figure below shows the ratings for the EdTech tools being reviewed and compared in this study.



**Figure 3: Common Sense Media Privacy Ratings**

### Third-Party Services of EdTech Companies

The following table outlines the third-party services used by each of the education technology tools in this study. Both Edmodo and Kahoot! clearly state they do not require their third-party services to have the same level of privacy protection as they themselves have in place.

EdTech Tool	Services Provided by Outside Vendors
Edmodo	Mobile analytics software, third-party ads with parental consent for under 13, third-party ads for individuals over 13, sending emails, analyzing data, processing payments, or other services needed to support our Platform and Products. Holds service providers to contractual obligations to protect information provided on a need-to-know basis. Does not control third-party websites.
SplashLearn	Shares aggregated data. Examples of shared data include sending billing receipts and weekly progress reports and providing user services. Amazon Web Services (AWS) hosting. Expects third-party services to protect the shared data at the same level.
Kahoot!	Website hosting, data analysis, information technology and related infrastructure provision, customer service, email delivery, auditing, payment processing and other services. Sweepstakes sponsors. Not responsible for the information collection, use, disclosure or security policies or practices of other organizations.

**Table 5: Third-Party Services**

### Privacy Violations

In 2017, Edmodo confirmed that hackers stole 77 million Edmodo user accounts which included usernames, email addresses, and hashed passwords (4iQ, 2017). At that time, this was the largest known breach of children’s data for sale on the deep and dark web. Although this research did not locate any data breaches or privacy violations in the news for SplashLearn or Kahoot!, the Government Accountability Office (GAO) reported data of thousands of students was compromised in 99 school data breaches from July 2016 to May 2020 (Barshav, 2020).

Kahoot! users can take advantage of the hacking resources on the web to be the Kahoot! winner or to fill the game with bot users that have funny or offensive names. Additional options to manipulate the Kahoot! include modifying the number of points earned per question, crashing the game, flooding the game with users, and adding random users (AK, 2020). While this does not necessarily pose a privacy risk, it is disruptive in the classroom and demonstrates that the site is vulnerable to external exploits.

### 5. EDTECH PRIVACY POLICY REVIEW

Based on the FTC’s COPPA compliance tips, Table 6 includes a review of the privacy policies from the EdTech companies in this study. Items were tagged as CLEAR, VAGUE, AND UNCLEAR depending on the level of detail provided in the privacy policy compared to the description in the FTC compliance tips. Most of the items reviewed were noted as CLEAR because the details in the policy sufficiently met the FTC compliance criteria.

In the review of Edmodo’s privacy policy, two items were noted as VAGUE, the third-party providers were unnamed and there was not a clear description of how verifiable parental consent was provided for the collection of data from children under 13. In the review of SplashLearn’s privacy policy, one item was noted as VAGUE, the policy did not provide a clear description of how verifiable parental consent was provided for the collection of data from children under 13. In the review of Kahoot’s privacy policy, one item was noted as VAGUE and one was noted as UNCLEAR. A portion of Kahoot’s policy was VAGUE because it did not include the names of their third-party providers, and another was unclear on how verifiable parental consent is obtained and the procedure to do so.

FTC Tip	Edmodo	SplashLearn	Kahoot!
1	VAGUE	CLEAR	VAGUE
2	CLEAR	CLEAR	CLEAR
3	CLEAR	CLEAR	CLEAR
4	CLEAR	CLEAR	CLEAR
5	VAGUE	VAGUE	UNCLEAR
6	CLEAR	CLEAR	CLEAR
7	CLEAR	CLEAR	CLEAR

**Table 6: Privacy Policy Review (expanded in Appendix A)**

### 6. OPPORTUNITIES

Due to the risks and necessity to preserve the privacy of minors, it is recommended that EdTech companies view this obligation as their corporate

social responsibility to manage third-party data processing and contract only with secure, reputable third-party service providers. Limiting the data collected and shared, and the number of contracted third-party service providers may reduce the footprint of data stored in multiple locations.

Parents, teachers, and school administrators should learn more about how EdTech companies use student data. They should leverage the privacy evaluation reports provided by independent organizations such as Common Sense Media to help with the selection of EdTech tools, not use them solely based on price or features offered. Laws should be properly enforced to ensure compliance and they should be updated to align with the modern use of technology to ensure consumers are provided with proper data privacy rights.

## 7. LIMITATIONS

This study was limited to a review of the privacy policies for three EdTech company's websites as of October 2020. This was not intended to be a compliance audit and the evaluation did not include logging into the websites or paying for subscription accounts to review business practices. Although there are many privacy regulations in different states and countries that may have been applicable, a limited number were included in the study.

## 8. CONCLUDING REMARKS

Common Sense Media works closely with schools and districts to provide a privacy evaluation of EdTech tools that address stakeholder concerns. These reports are made publicly available allowing the emphasized companies to make appropriate changes that go beyond regulatory compliance to provide consumers with the expected data privacy and security protections. These evaluation reports also provide individual teachers and parents with the information they need to make the best choices for the kids that they have powerful influence over, to help protect the data privacy of children of all ages rather than simply focusing only on the requirements of COPPA for children under 13.

Standards for online safety and privacy for minors must be improved and modernized to align with the digital assets that children are creating, and companies are collecting for profit. Understanding the types of data being collected from minors by EdTech organizations can help in the review of current regulations and determine where those

regulations need to be improved. Further assessment and comparison can help the EdTech organizations recognize if there are any missteps in the collection, use, or sharing of data collected from minors.

## 9. REFERENCES

- AK. (2020). *Kahoot Hack*. Retrieved from Google Chrome Store: <https://chrome.google.com/webstore/detail/kahoot-hack/efdcmgmfnfcikihmcmfdbbbhpembnimfk>
- Bahar, M., Sand, A., & Wilson-Bilik, M. J. (2020, November 10). *California's new privacy law, the CPRA, was approved: Now what?* Retrieved from Eversheds Sutherland LLP: <https://www.jdsupra.com/legalnews/california-a-s-new-privacy-law-the-cpra-93354/#:~:text=On%20November%20%2C%202020%2C%20California,effect%20on%20January%201%2C%202023.>
- Banta, N. M. (2019, May). Minors and digital asset succession. *Iowa Law Review*, 104(4), 1699-746.
- Barrett, L. (2018, March 1). *Best practices (and common pitfalls) of EdTech privacy policies. Commentary K-12*. Retrieved from Eduwire: <https://www.avnetwork.com/eduwire/reducing-transactional-distance-engaging-online-students-in-higher-education-edscoop>
- Barshav, J. (2020, November 9). *PROOF POINTS: What happens when private student information leaks*. Retrieved from The Hechinger Report: <https://hechingerreport.org/proof-points-what-happens-when-private-student-information-leaks/>
- Belding, G. (2018, August 2). *How to comply with COPPA — 7 steps*. Retrieved from INFOSEC: <https://resources.infosecinstitute.com/how-to-comply-with-coppa-7-steps/>
- Black Kite. (2020, December). *2020 Data Leaks*. Retrieved from Data breaches caused by third-parties: <https://normshield.com/data-breaches-caused-by-third-parties/>
- Chaiyo, Y., & Nokham, R. (2017). The effect of Kahoot, Quizizz and Google Forms on the student's perception in the classrooms response system. *International Conference on Digital Arts, Media and Technology (ICDAMT)*, 178-182.
- Chauhan, A. (2018, March 31). *11 Digital Education Tools For Teachers And Students*.

- Retrieved from eLearning Industry:  
<https://elearningindustry.com/digital-education-tools-teachers-students>
- Chen, H.-L. C.-H. (2016). Beyond identifying privacy issues in e-learning settings – Implications for instructional designers. *Computers & Education, 103*, 124-133.
- Cleverism. (2020). *Careers at Edmodo*. Retrieved from Cleverism: <https://www.cleverism.com/company/edmodo/>
- Dhawan, S. (2020, June 20). Online Learning: A Panacea in the Time of COVID-19 Crisis. *Journal of Educational Technology Systems, 49*(1), 5-22.
- Edmodo. (2020). *About*. Retrieved from Edmodo: <https://go.edmodo.com/about/>
- Edmodo. (2020). *Privacy policy*. Retrieved from Edmodo: <https://go.edmodo.com/privacy-policy/>
- Education Foundation. (2015, July 29). *California Online Privacy Protection Act (CalOPPA)*. Retrieved from Education Foundation Consumer Federation of California: <https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/>
- Elliott, A. (2015, Spring). Death And social media implications for the young and will-less. *Jurimetrics, 55*(3), 381-405.
- 4iQ. (2017). *Diving deep into the Edmodo data breach. Analyzing the largest breach of children’s data exposed so far*. Retrieved from 4iQ: [https://4iq.com/diving\\_deep\\_into\\_the\\_edmodo\\_data\\_breach/](https://4iq.com/diving_deep_into_the_edmodo_data_breach/)
- FTC. (2020). *Children’s Privacy. Privacy and Security*. Retrieved from Federal Trade Commission: <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy>
- FTC. (2020). *Complying With COPPA: Frequently asked questions. A guide for business and parents and small entity compliance guide*. Retrieved from Federal Trade Commission: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>
- Hunton Andrews Kurth. (2020, November 4). *California Voters Pass the CPRA*. Retrieved from Privacy and Information Security Law Blog: <https://www.huntonprivacyblog.com/2020/11/04/california-voters-pass-the-cpra/>
- InfoLawGroup. (2016, January 5). *Privacy and Ed-tech in 2016*. Retrieved from InfoLawGroup: <https://www.infolawgroup.com/insights/2016/01/articles/privacy-law/privacy-and-ed-tech-in-2016>
- Kahoot. (2020). *Kahoot!* Retrieved from About us: <https://kahoot.com/company/>
- Kahoot. (2020). *Make Learning Awesome. Kahoot! delivers engaging learning to billions*. Retrieved from Kahoot!: <https://kahoot.com/privacy-policy/#children-policy>
- Kahoot! (2020). *Kahoot! Privacy Policy*. Retrieved from Kahoot!: <https://kahoot.com/privacy-policy/>
- Kelly, G., Graham, J., Bronfman, J., & Garton, a. S. (2019). *2019 State of EdTech Privacy Report*. San Francisco: Common Sense Media.
- Leong, B., Attai, L., Vance, A., & Rubin, D. (2016, November 4). *FPF Guide to Protecting Student Data Under SOPIPA: For K-12 School Administrators and Ed Tech Vendors*. Retrieved from Future of Privacy Forum: [https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide\\_Nov-4-2016.pdf](https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf)
- Minors and the GDPR*. (2020). Retrieved from iubenda: <https://www.iubenda.com/en/help/11429-minors-and-the-gdpr>
- Nearpod. (2020). *You’ll Wonder How You Taught Without It*. Retrieved from Nearpod: <https://nearpod.com>
- Peterson, D. (2016). EdTech and student privacy: California law as a model. *Berkeley Technology Law Journal, 31*, 961-996. Retrieved from University of California, Berkeley, School of Law.
- Plunkett, L. (2020, July). To stop sharenting & other children’s privacy harms, start playing: a blueprint for a new Protecting The Private Lives Of Adolescents And Youth (PPLAY) Act. *Seton Hall Legislative Journal, 44*(3).
- Potasznik, A. (2020). *Spokespeople or Gatekeepers? A Case Study of Teacher Engagement with the Data Privacy Policy Environment in U.S. Public Schools*. Dissertation, University of Massachusetts, Boston.

- Privacy Technical Assistance Center. (2016, March). *U.S. Department of Education*. Retrieved from Protecting Student Privacy While Using Online Educational Services: Model Terms of Service: <https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service>
- Quizizz. (2020). *Free Quizzes for Every Student*. Retrieved from Quizizz, Inc.: <https://quizizz.com>
- Quizlet. (2020). *Learning tools & flashcards, for free*. Retrieved from Quizlet: <https://quizlet.com>
- Rasch, M. D., & Wilber, A. J. (2020, November 13). *Kohrman Jackson & Krantz LLP*. Retrieved from California votes to strengthen California Consumer Privacy Act With CPRA: <https://kjk.com/2020/11/13/california-votes-to-strengthen-california-consumer-privacy-act-with-cpra/>
- Rubin, D. B. (2019, March). *The Legalities of Classroom Apps*. Retrieved from The School Superintendents Association: <http://my.aasa.org/AASA/Resources/SAMag/2019/Mar19/Legal.aspx>
- Sonnemaker, T. (2020, October 13). *As Zoom classes take over during the pandemic, edtech companies provide a lifeline, but only for schools and parents willing to surrender their students' privacy*. Retrieved from Insider: <https://www.businessinsider.com/virtual-learning-privacy-tech-teachers-parents-schools-student-data-2020-10>
- SplashLearn. (2020). *About us*. Retrieved from SplashLearn: <https://www.splashlearn.com/about>
- SplashLearn. (2020). *Privacy policy. The complete K-5 math learning program built for your child*. Retrieved from SplashLearn: <https://www.splashlearn.com/privacy>
- The K!rew. (2016, September 28). *We've Reached 10 Million Public Kahoots!*. Retrieved from Kahoot!: <https://kahoot.com/blog/2016/09/28/10-million-public-kahoots/>
- Tutorful. (2020). *The 101 hottest EdTech tools according to education experts (updated for 2020)*. Retrieved from Tutorful: <https://tutorful.co.uk/blog/the-82-hottest-edtech-tools-of-2017-according-to-education-experts>
- West, T. (2020, December). *Weak Password Policies: A Lack of Corporate Social Responsibility*. *Colloquium for Information Systems Security Education*, 8(1).
- WildWorks. (2016). *Fun with substance*. Retrieved from WildWorks: <http://www.wildworks.com/#about>
- Winder, D. (2020, July 8). *Forbes*. Retrieved from New Dark Web Audit Reveals 15 Billion Stolen Logins From 100,000 Breaches: <https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=2dd1da26180f>
- Yahoo! Finance. (2020). *New Kahoot! integration with Microsoft teams brings engagement to distance learning and video conferencing*. Retrieved from Yahoo! Finance: <https://finance.yahoo.com/news/kahoot-integration-microsoft-teams-brings-131500923.html>

**Appendix A  
 COPPA Compliance Privacy Policy Review**

<b>FTC Compliance Tip</b>	<b>Edmodo</b>	<b>SplashLearn</b>	<b>Kahoot!</b>
<b>1 Third Parties Named</b> Names of all operators collecting personal information	<i>VAGUE</i> Although the information is not being collected by third parties, Edmodo shares information with unnamed third-party service providers.	<i>CLEAR</i> Provides a link that lists all third-party service provider names, URLs, and intended purpose.	<i>VAGUE</i> Although the information is not being collected by third parties, Kahoot! shares information with unnamed third-party service providers.
<b>2 Personal Information</b> Description of personal information collected and how it is used	<i>CLEAR</i> Describes types of information collected and the intended purpose.	<i>CLEAR</i> Describes types of information collected and the intended purpose.	<i>CLEAR</i> Describes types of information collected and the intended purpose.
<b>3 Parental Rights</b> Description of parental rights	<i>CLEAR</i> Parental rights, including how child's information is collected and intended purpose for disclosure to third parties are described.	<i>CLEAR</i> Parental rights, including how child's information is collected and intended purpose for disclosure to third parties are described.	<i>CLEAR</i> Parental rights, including how child's information is collected and intended purpose for disclosure to third parties are described.
<b>4 Notice To Parents</b> Direct notice to parents is clearly written	<i>CLEAR</i> Parental rights, including how to update and request deletion of child's data, are described.	<i>CLEAR</i> Parental rights, including how to update and request deletion of child's data, are described.	<i>CLEAR</i> Parental rights, including how to update and request deletion of child's data, are described.
<b>5 Parental Consent</b> Obtain verifiable parental consent before collecting child's personal information	<i>VAGUE</i> Requires parent's, guardian's, or teacher's consent. Additional parental consent when request is initiated by school district or administrator. Does not explain how consent is given.	<i>VAGUE</i> Requires explicit parental consent but does not explain how consent is given.	<i>UNCLEAR</i> Could not find any details on parental consent procedures.
<b>6 Child's Data</b> Allow parents to review data, revoke permission, and request data to be deleted	<i>CLEAR</i> Describes right to access data for review, deletion, and provides choices about child's data. Retention policy is slightly vague.	<i>CLEAR</i> Describes right to review and update data, request deletion, and right to object to data being used for marketing. Retention policy is slightly vague.	<i>CLEAR</i> Describes right to review and update data, request deletion, and right to object to data being used for marketing. Retention policy is slightly vague.
<b>7 Security Measures</b> Reasonable security measures to protect data	<i>CLEAR</i> Includes reference to password protected account, secure coding practices, and numerous other technical, administrative, and physical security mechanisms.	<i>CLEAR</i> Includes reference to periodic review of policies; application security testing; penetration testing; conducts risk assessments; and monitors compliance with security policies.	<i>CLEAR</i> Includes reference to organizational, technical, and administrative measures to protect Personal Information.