Spring 2020

National Science Foundation Grant Report: Initial Phase

Principal Investigator:

Dr. Kristen Walker

Project Manager:

Paola Moreno

Research Assistants:

Beenish Niazi

Debbie Rodriguez

Frank Zapata

Mark Rostom

Parit Kasemsri

Pedro Rodriguez

Ziad Chehadeh

Table of Contents

Table of Figures

Key Takeaways

OUTREACH TO SCHOOL DISTRICTS

Challenges with Contacting EdTech Procurement Personnel
Identifying the correct administrator to speak with has been a difficult task. We found that the decision-making is not centralized in one department head or the position cannot be identified by other employees of a given district.

COVID-19
After deferring recruitment for a few weeks we began conducting our interviews using video conferencing technology. We quickly noticed a shift toward centralization in leadership of the educational technology spaces.

EXAMINE KEY ASPECTS OF K-12 TECH/MARTECH

Policies
Policies regarding education and Educational Technology are being created after a problem regarding the issue arises, rather than being implemented to prevent the issue. Most of the time, when a company or individual is caught breaching one of these policies, a fine is is all they receive. No real action is taken so that companies won't do it again, it is the equivalent of a slap on the wrist. Older policies have not accounted for technological advancements of today, these policies do not get amended so new ones are made to cover up what the old ones missed. When states see a problem that has not been addressed at the federal level, they will take it upon themselves to make an alternative.

People
There exist conflicting views on EdTech policy needs among key stakeholders. Educators, advertising companies, and others find themselves at odds with each other regarding the vulnerabilities of children under protection laws. The lack of awareness on security and privacy issues among gatekeepers—parents, administrators, etc.--only exacerbate the problem.

Programs
Education and Marketing technology are two related industries with alarmingly unclear connections and networks. As technology advances, more and more of our lives are moving online. Schools have begun to rely on technology as an education tool for students as young as kindergarten. This reliance on technology has uncovered a lack of privacy concerns when programs are developed which have caused some dangerous privacy issues for students in the education system. With the online learning transition amid the COVID-19 crisis, schools were forced to move all learning tools to online means and surrender student privacy into the hands of EdTech companies.

COVID-19 RESPONSE

The COVID-19 crisis gave us an unusual opportunity to study the true weaknesses of education technology like they have never been seen before. We have yet to see such a large-scale transition to online learning in such a small amount of time, and the downfalls of privacy and school readiness to accommodate to changing needs quickly reveled themselves. As schools scrambled to find the best online learning alternatives, programs simultaneously scrambled to update their software to accommodate larger numbers of students. In a time of quick and uncertain change, a plethora of privacy and usage concerns with education technology came to the forefront of discussion.

IRB & HIRING/RECRUITING K-12 PRIVACY TEAM

IRB Approval Process

After the NSF grant was awarded by NSF SaTC in October 2019 and the Principal Investigator, Dr. Walker, worked with research assistant, Beenish Niazi, to complete CSUN's Institutional Review Board (IRB) process on Cayuse. That process took several months with an IRB application for expedited review. After addressing the IRB comments and concerns, the grant project received final IRB approval on January 8, 2020.

Hiring/Recruiting K-12 Privacy Team

- In November and December 2019, the PI and research assistant created job announcements for the student positions included in the grant – two undergraduate Research Assistant positions and one graduate Research Associate position (see appendix X).
- At the end of the fall 2019 semester, one undergraduate Research Assistant, Beenish Niazi was formally hired by The University Corporation (TUC) and the position announcements were sent to undergraduates and the graduate position was shared with the Sociology and Psychology Departments on campus. A Graduate Research Associate, Paola Moreno (MS Sociology) was hired at the end of the fall semester. Interviews were conducted for two types of undergraduate positions: 1) the remaining Research Assistant position and 2) an undergraduate team who would earn course credit for working on the grant (syllabus in Appendix X). Nine undergraduates applied and six were chosen as follows:
    1) *Paid Research Assistant position:*
    Mark Rostom
    2) *Independent Study:*
    Ziad Chehadeh
    Parit Kasemsri
    Debbie Rodriguez
    Pedro Rodriguez
    Frank Zapata

RESEARCH TASKS

Key Literature and Secondary Data Sources

The spring 2020 term began with determining grant meetings (Mondays at 11am). Students were tasked with reviewing literature, performing an annotated bibliography, and researching details about the school districts for outreach and interview purposes. These tasks continued along with weekly discussions until the 4th week of the semester, when three primary themes were identified to focus on regarding K-12 educational technology and privacy:

1. Policies: The policies involved with K-12 educational technology at the federal and state level (i.e. FERPA, CIPA, COPPA, and SOPIPA)
2. People: Key stakeholders involved in the K-12 educational technology process
3. Programs: Exploring the K-12 educational technology industry and the connection to the Marketing Technology (MarTech) industry.

Outreach for School District Personnel for Interviews

In spring 2020 the team also began outreach to interview school district personnel.

OUTREACH TO SCHOOL DISTRICTS

Of the 977 school districts in California, we began by narrowing down the largest 25 school districts (ranked by size of enrollment) and the 25 smallest school districts. Using cluster sampling we ensured a wide diversity of students, households and institutions statewide. We targeted the educational technology adoption decision-makers at these sites, but that proved more difficult than previously considered.

Challenges

<u>No centralized position.</u>

By inquiring into the educational technology departments or divisions of these school districts, we confirmed that identifying the correct administrator to speak with would be a difficult task in itself. Scouring through webpages and district-wide education plans, we were able to compile an initial list of potential contacts for each of the fifty target districts. We called a representative at each district at least 5 times, on average, if no response was received. Most of our calls have been met with uncertain assistants and polite redirections to voicemail inboxes, if answered at all. Of the fifty districts contacted, we have received a positive response from eight. Of those eight, two require a preliminary application process for research within the district, six have confirmed the correct personnel or have redirected us to them, and only two have agreed to an interview. Beyond a lack of trust or lack of interest, we've identified a cause of this obstruction to be no definite position to be directed to. A trend we continuously encountered, the decision-making is not centralized in one department head or the position could not be identified by other employees of a given district.

<u>COVID-19 Emergence and reaction</u>

The outbreak of the coronavirus has been very hindering to our interview progress, to say the least. As the country shifted all non-essential work and services online, our outreach and interview processes moved to virtual spaces as well. Beyond the travel restrictions and mandated social distancing that stunted our interview progress, we had to accommodate the changing environment of the education sector. For the last couple of months, school districts have been scrambling to mitigate and adapt to the drastic changes required for a smooth and safe transition to remote learning. Our team deferred recruitment for a few weeks after learning of the challenges being faced by administrators, educators, and students across the state. After resuming, we haven't had much success in terms of interviews, but we have noticed a centralization in leadership of the educational technology spaces. Whereas before, no clear position could be identified, we are now receiving responses along the lines of, "this isn't a good time to connect." We have at least been able to identify the correct personnel to whom we could direct our questions.

Interviews

Despite the challenges, we have been able to conduct a couple of fruitful interviews that could serve to inform this initial phase of our study.

<u>Laguna Joint Elementary School District</u>

This is a rural, multi-grade classroom in Northern California. There are currently 10 students enrolled in the school/district. Two in 1st grade, two in 2nd grade, two in 3rd grade, two in 4th grade, and two in 5th grade; all in the same classroom. The students are 50% Hispanic, 6.3% Mixed race, and 43.7% "other." 87.5% of the students are English learners and 81.3% of families are socioeconomically disadvantaged. From the Local Control Funding Formula (LCFF), in 2015/2016, funding for Laguna Joint Elementary School District was about $16,477/student.

We spoke with the County-District-School (CDS) Coordinator. For this smaller, more rural school district, one person takes on the roles of teacher, principal, County liaison, and everything in between. Students here are children of dairy-farmers and likely live in trailers or mobile homes, so accessibility to technology has been a priority for the school/district. Students share four MacBooks, eleven Notebooks, and one Google Chromebook to access their grade-designated, Google Classroom-mediated lessons. The CDC Coordinator works directly with the Marin County Office of Education for most ed-tech inquiries but maintains autonomy in almost all decisions. Though agreement for technology use is required, no exhaustive digital training is offered to students or parents.

<u>Santa Ana Unified School District</u>

There are currently 51, 974 students enrolled in the district. The district is comprised of 55 schools: 36 elementary schools, eight intermediate schools, seven comprehensive high schools, three educational options secondary schools, and one child development center. The students are 96% Hispanic, 2% Asian, and 2% Other. 40% of students are English learners and 88% of families are socioeconomically disadvantaged. From the Local Control Funding Formula (LCFF), in 2015/2016, funding for Santa Ana Unified School District was about $9,564/student.

We spoke with the Curriculum Specialist in the district, who is the highest ranking employee with regard to ed-tech decisions in the district. There is no educational technology position in the administration—no Director, no Assistant Superintendent. Previous to COVID-19, the district was already 1:1 with Google Chromebooks. The movement happened when state testing went strictly online, and the deliberation process of selecting devices actually included the users (students). The district has its own data processing center and manages data security in-house. Noteworthy, the district does offer digital citizenship courses to not only students, but parents as well.

EXAMINE KEY ASPECTS OF K-12 TECH/MARTECH

Policies

Increasing use of technology requires regulations that promote an ethical and safe environment for its users. In the US there are regulations on the federal and state level that address different aspects of consumer protection. On the federal level, The Federal Trade Commission (FTC) prohibits companies from deceptive practices such as failing to follow a published privacy policy or not taking proper measures to secure customer data (FTC.gov). This section aims to examine some policies that address consumer rights, data protection and privacy laws.

CARU

Children's Advertising Review Unit (CARU) is a self-regulatory, investigative advertising review unit, curated in 1974 by "Advertising Self-Regulatory Council (ASRC) and operated by the Better Business Bureau National Program (BBB NP)" (About CARU), to help advertisers, agencies, and companies on how to properly promote ethical and responsible advertising directed to children 12 years and younger" (About CARU, para. 5).

CARU's responsibility is to "evaluate child-directed advertising and promotional material in all media to advance truthfulness, accuracy and consistency with CARU'S guidelines and relevant laws" (About CARU). A hypothetical example of CARU's enforcement is when a toy company implies that its new toy is 'life changing' when it is likely that children might not understand that its advertising and marketing is misleading and false. CARU is described as an offspring of the federal Children's Online Privacy Protection Act of 1998 (COPPA), by enforcing and replicating the same guidelines that COPPA has constructed, which "highlights issues, including children's privacy, that are unique to the Internet and online sites directed at children age 12 and under" (About CARU). CARU also offers services to advertisers, agencies, and companies with a blueprint on how to properly adhere to their guidelines when advertising to children 12 years and younger. CARU has the ability to track and reviews advertisements directed to children by receiving consumer complaints through the BBB National Programs' website. CARU proposes changes to companies, agencies, or advertisers on what is appropriate before any fines and violations are incurred.

Children's Advertisement Review Unit (CARU)

- Review board operated By Better Business Bureau (BBB)
- Makes sure advertisements directed to kids are honest and truthful
- CARU called in to make sure advertisements shown during COVID-19 are not misleading

Figure 1. Overview of CARU

COPPA

The Children's Online Privacy Protection Act (COPPA) enacted in 1998, protects children privacy through limiting the collection of children's personal data. Although COPPA was officially passed by congress in 1998, it was only enacted because of growing marketing practices targeting children throughout the 1990s and did not formally take effect until April 2000 (Rouse, 2010). The fact that this act took years to be presented to congress and another two years to be enforced after being approved, shows how slow changes in laws can be and raises concern to the reliability and relevance of policies. COPPA was written to protect children under thirteen and uses parental involvement through consent before collecting their child's information. COPPA focuses on regulating websites that target children and general websites that have a high volume of child users, operating under five requirements: notice, parental consent, parental review, security, and limiting the use of games & prizes. Websites must disclose what information is being collected on children visitors, how the information is used and whom the information is disclosed to. COPPA prioritizes data security requiring websites to establish external security and the regular Maintenance. Parental consent is generally required, unless it is for a one-time basis. This is stated specifically as "responding directly on a one-time basis to a specific request from the child" and "not used to re-contact the child."

Parental consent has to be verifiable, websites must get to "any reasonable effort" prior to the collection of any personal information from children. The parent of the child is also "one informed of the personal data processing practices by the online service provider and two authorizes those practices" (Van Der Hof, 2016). To be compliant with COPPA standards, a website must have firewalls, information deletion, limits on employee access, and screening of third parties to whom the information is disclosed to (Gadbaw, 2016). For parental review, a site must offer the parent the ability to review the information that has been collected and a way to contact the website from prohibiting further use or maintenance of the child's information (Gadbaw). Limiting games and prizes is used to avoid conditioning children into giving out personal information to seek a reward.

Children's Online Privacy & Protection Act (COPPA)

- Federal law
- Enforced by federal trade commission (FTC)
- Limits collection of personal identifiable information (PII) for children 12 & under
- If COPPA is violated: website will be liable for fines determined by FTC

"Grom Social"

- Has seen surge in use during COVID-19 Pandemic
- COPPA complicit
- Keeping kids safe and entertained

Figure 2. Overview of COPPA

Enforcing COPPA

As of 2016 The New York Attorney General found Viacom, Mattel, JumpStart, and Hasbro to be in violation of COPPA by allowing illegal Third-Party Tracking Technology on their websites (History of COPPA Violations). Mattel was fined $250,000 for using tracking technology by a third-party data broker (A.G. Schneiderman Announces Results Of "Operation Child Tracker," Ending Illegal Online Tracking Of Children At Some Of Nation's Most Popular Kids' Websites). Fines by the FTC are up to $42,530 per violation as of 2019(https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children). Viacom was fined $500,000 using target advertisement. Jumpstart an educational and entertainment software was fined $85,000 for targeting advertisement to children and failed to notify their partners they were targeted towards children. YouTube has also been fined $170 million for violating COPPA Feb. 27, 2019, December 1, 2018 OATH, an AOL Yahoo merger company, was fined $5 million for targeting ads to children. (A.G. Schneiderman Announces Results Of "Operation Child Tracker,").

In 2019 TikTok was fined $5,700,000 by the FTC for illegally collecting personal information from children (Alexander, 2019). In response to the fine, TikTok then initiated tools and changes to accommodate tools for parents and age appropriate content (Musical.ly's Agreement with FTC.). To be FTC compliant, TikTok has introduced a feature that splits content and filters appropriate content to users depending on age(Musical.ly's Agreement with FTC.). Younger users are no longer able to share personal information and users will be directed to age appropriate content (Musical.ly's Agreement with FTC.).

COVID-19 and COPPA:

In response to COVID-19 EdTech companies have been producing services and products that are marketed as COPPA compliant. Grom Social is an application marketed to kids to interact socially around the world with family remembers and other kids. The application allows kids to post video, watch exclusive kid-friendly content, and make friends online. Since the month of March Grom has seen a 24.5 percent increase in users (Grom social keeping kids safe online during COVID-19 pandemic). BulbEd has also offered its flagship education Digital Portfolio software for free in light of the crisis. The program is set to deploy and support teaching remotely and learning by scale according to need (Starting today, due to the COVID-19 pandemic).

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal program that protects student educational records (Family Educational Rights, 2018). FERPA grants the rights of educational records of the student, to their parents. This right transfers to the student once they enter a post-secondary institution after high-school or turn 18 years old, whichever comes first (Family Educational Rights, 2018). Students who have their rights transferred to them are then considered an “eligible student.” FERPA applies to all schools in the U.S. that receive funds from the United States Department of Education, as well any educational program funded by the United States Department of Education (Family Educational Rights).

FERPA grants the right for the parents or eligible students to be able to look and review their educational records that the school has on file (Family Educational Rights, 2018). Another right granted is to be able to “to request that a school correct records which they believe to be inaccurate or misleading” (Family Educational Rights, 2018). If the school does not comply with an amendment, the parents or eligible student have the right to a formal hearing (Family Educational Rights, 2018). Parents or an eligible student may also grant rights the rights of student information to other parties with written consent (Family Educational Rights, 2018). Although FERPA does protect student’s educational information from getting in the wrong hands, FERPA does allow for information to be transferred to other parties without prior consent. These parties include but are not limited to;

- School officials with legitimate educational interest;
- Schools to which a student is transferring to;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena; and
- Appropriate officials in cases of health and safety emergencies.

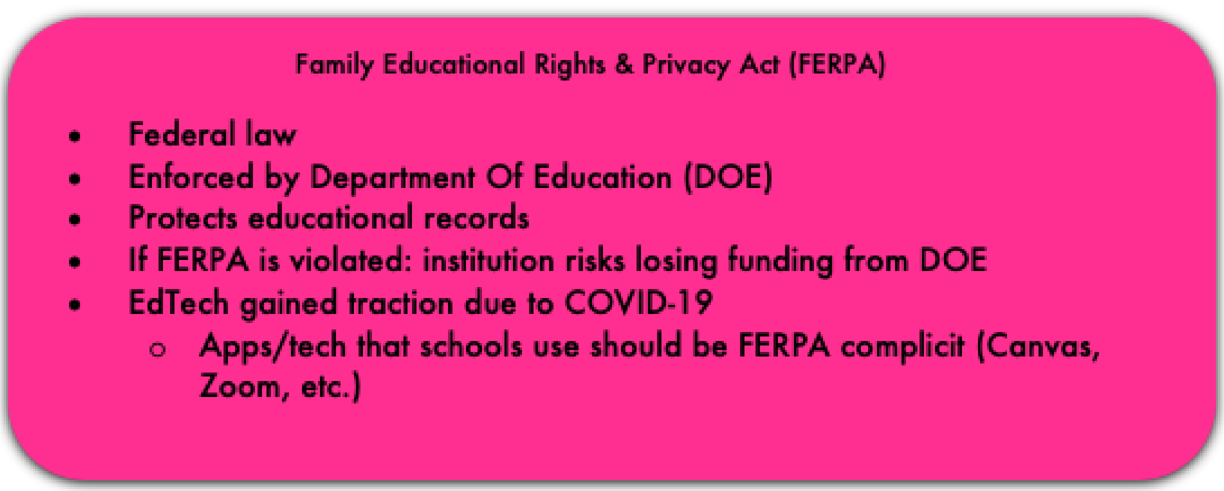

Figure 3. Overview of FERPA

Figure 4. Allowances of FERPA

FERPA Origins

FERPA ensures that student information is in the hands of only people who should have it. FERPA protects students "educational records" which was defined as in a 1974 amendment as "those records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational agency or institution or by a person acting for such agency or institution" (Legislative history of, 2004). Educational records may also include any grades, any disciplinary report, attendance records, or medical history related to the student's enrollment (Protecting the privacy, 1997). These records can be stored in a registrar office with physical paper copies, on computer hard drives, in cloud storage, or any other means to have information (Protecting the privacy, 1997). Before FERPA was enacted, parents and students did not really know what they could or could not see about their records. FERPA was sponsored by the principal supporter, Senator James Buckley of New York (Stone 2002). His motivations for FERPA were due to the school's lack of transparency with parents.

Educational Technology Policies and COVID-19

The coronavirus (COVID-19) pandemic is wreaking havoc in education and technology. Schools across the country have shut down in response to the coronavirus outbreak. Harvard-Westlake School, a private school in Los Angeles, California, announced it would be closed indefinitely to help slow the spread of the novel coronavirus (Fattal, 2020). Governor Gavin Newsom of California announced that all schools be shut down for the time being, and soon after announced that schools be closed for the remainder of the 2019-2020 school year (Kohli, 2020). As of April 2020, there is no information available on whether schools at any level will open 'as usual' for the 2020-2021 school year. With schools being closed, education has shifted to distance-learning. Many schools and teachers are still lecturing and teaching, but through video-conference programs and one example of an enormous increase in K-12 use is Zoom. Zoom existed before the pandemic, but mostly in a professional or college settings, such as meetings with colleagues, staff members etc. Zoom is now being used by schools and universities all over the country, with questionable safety and increasing privacy concerns O'Flaherty, 2020). Zoom founder and CEO, Eric Yuan, has heard the concerns from schools and parents and is acting on it by adding security features and by focusing on improving these features (O'Flaherty, 2020). After hearing that schools will be shut down for the rest of the year, Yuan, offered Zoom's premium service at no cost to K-12 schools in the U.S. starting on March 13, 2020 (Konrad, 2020). Zoom has faced many privacy concerns; many schools and school districts have had people showing up and either yelling profanity or showing inappropriate images (Chavez, 2020). Some educators and parents worry that Zoom violates FERPA and is not complicit due to the privacy concerns (St. Amour, 2020). Zoom is FERPA complicit, they do not sell student information, not monitor or track video meetings hosted under a school domain, and they also provide multiple levels of security that students and teachers can add (Zoom and FERPA, 2018). New York City Schools have been advised to move away from Zoom and switch to Microsoft Teams because it offers the same features but with an added level of security (Chavez, 2020).

The sudden and overwhelming switch to distance learning is an emerging and constantly changing problem. Research connecting COVID-19 and FERPA, is very difficult to find, likely due to timing and focus. Finding information on EdTech and FERPA is already a challenge in itself, the pandemic has not made it any easier.

SOPIPA

The Student Online Personal Information Protection Act (SOPIPA) is a law enacted by the California senate to protect student information through within education spaces. SOPIPA implements four steps to restrict the speech of operators that provide online services, websites or applications primarily target for K-12 schools (McGrath, 2016).

1. SOPIPA restricts operators from using student data to create profiles about K-12 students, expect in furthering K-12 school purposes.
2. Prohibits the selling of student information, covered information
3. Prohibits the disclosure of student information, covered information, unless under certain expectations.
4. Knowingly engaging in target advertising through the operator's service. (McGrath, 2016).

Arkansas, Georgia, Virginia and Delaware all have longstanding laws that address data protection (ROSCORLA). Virginia's HB 2350, Delaware's SB 79 and Georgia's SB 89 has a designated privacy offer and developed a model for student data privacy policies for its school boards (ROSCORLA). Arkansas's HB 1961 prevents operators from suggesting recommendation in search engines to students (ROSCORLA). Georgia's bill does not prevent educational institutions from recommending educational material and it does not prevent operators from marketing to parents (ROSCORLA).

Education technology (EdTech) is becoming increasingly popular among schools and educators due to the convenience and ease of use. EdTech also intends to offer a personalized learning on student level basis (Horn, 2016). SOPIPA prohibits operators of online websites, apps, or services that are primarily used by K-12 students from "knowingly using, disclosing, compiling, or allowing a 3rd party to use, disclose, or compile the personal information of a minor for the purpose of marketing or advertising specified types of products or services" (SB 1177). This law makes it so that EdTech companies are held to a certain degree of responsibility to put education before money.

SOPIPA was designed to address what FERPA and COPPA do not address (Varella 2016). FERPA grants rights to parents and students about a student's educational records, but does not have any protections against the student's information from being sold to EdTech companies. SOPIPA, makes sure that EdTech operators in California cannot "target advertising on any other site, service, or application when the targeting of the advertising is based upon any information…that the operator has acquired because of the use of that operator's site, service, or application" (SB 1177). This means that along with not targeting advertisements directly on their own individual website, they also may not give any information that they have collected, knowingly or unknowingly, to any third party that will engage in targeted advertising. This is a positive sign for privacy because educators and parents are reassured that their students will be digitally safe when they are using an EdTech service. SOPIPA also prohibits EdTech providers from using personal identifiable information (PII) to amass profiles on K-12 students (SB 1177).

Student Online Personal Information Protection Act (SOPIPA)

- California law
- Overseen by CA Attorney General
- Designed to address what FERPA fails to protect
- Protects student's information from third parties, even if it's covered

Figure 5. Overview of SOPIPA

Student Data in California

SOPIPA is intended to protect student information termed as "covered information." Covered information includes student information that has been provided by schools, school representatives, parents and the students legal guardians. Covered information includes personally identifiable information, but unlike many laws that clearly define personally identifiable information, SOPIPA does not. Currently this highlights the issue of how operators (school districts and EdTech companies) will be held accountable if they misuse covered information. Each operator must assess the data they are collecting on students, teachers, and parents and determine if it can be personably identifiable (FPF Guide to Protecting Student Data Under SOPIPA: For K-12 School Administrators and Ed Tech Vendors).

Covered information defined as personally identifiable information or materials regardless of media or format. Created or provided information by students, parents or legal guardian is identified as personally identifiable information. Information provided by employee or agents of K-12 schools, local education, agency or county offices also fall under personally identifiable information. Information that is gathered by an operator through operation site, service, or application and is descriptive of student information must also be SOPIPA compliant. A problem can also be seen in how third-party companies would determine what actual knowledge is (FPF Guide to Protecting Student Data Under SOPIPA: For K-12 School Administrators and Ed Tech Vendors).

Student Information as a Commodity

SOPIPA restricts operators from sharing information and marketing that information. If an operator challenges SOPIPA based on the first amendment the courts must decide what level of scrutiny is appropriate to make a decision. SOPIPA can be scrutinized in the law through various ways. In the court children data is often scrutinized under the first amendment. This states that the government do not have the right to restrict expression based on message, ideas, subject matter, or content. Courts may deem information as either noncommercial. Case law such as the 2011 Supreme Court case of Sorrell v. IMS Health Inc. shows how the First Amendment was applied to grant protections of informational data (McGrath, 2016). In Sorrell v. IMS Health Inc. the courts were in favor of protecting the prescriber-identifying information from pharmaceutical companies. Under SOPIPA student information must also be defined as either speech or commodity. SOPIPA advocates state that the Sorrell v. IMS Health Inc. case should require courts to first determine if laws restricting speech is first be content and speaker based, second, to consider whether “the restriction is consistent with the applicable level of First Amendment scrutiny” (McGrath, 2016).

CIPA

In 2000, congress passed the Children’s Internet Protection Act (CIPA), which was designed to be able to prevent children from seeing content that is deemed harmful or obscene, on school or library computers (Children’s Internet Protection, 2019). Schools and libraries often receive a significant discount, an education rate (E-rate), when purchasing electronic equipment, programs, internet connection, or any other educational service (The E-Rate Technology, 2020). If schools intend to use this discount, they must be compliant with CIPA and must filter out any pictures that are:

- Obscene:
- Child pornography;
- Harmful to minors (Children’s Internet Protection, 2019).

Schools that are subject to CIPA must also monitor internet behavior of any minors using the equipment and educate about the importance of online etiquette. “Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.” (Children’s Internet Protection, 2019, para. 4).

Children's Internet Protection Act (CIPA)

- Federal law
- Requires schools and libraries to filter out searches that are;
  - Harmful to minors;
  - Obscene; and
  - Child pornography
- Failure to do so results in loss of discount rate (E-Rate) on technology and software
- Students must be educated on online etiquette

Figure 6. Overview of CIPA

Challenges with Policy

Potential Risks

One of the biggest criticisms of these policies has been the violation of rights to freedom of speech and expression for children. For example, COPPA applies specifically to children under thirteen. To be COPPA compliant, websites heavily restrict key features for children; features that may be available to older users. Many websites have opted to ban children ages 12 and under altogether.

On the other hand, some believe these policies don't protect children enough. Another weakness of COPPA is that it does not protect children between the ages of 13 to 17 from targeted advertisements and informational profiling. Amendments from Representative Bobby Rush of Illinois introduced an update to the current COPPA ruling. This draft of a standalone bill will address issues that COPPA does not address with an emphasis on protecting young teens. Representative Kathy Castor of Florida is also introducing a bill H.R. 5703 that would change the enforcement of COPPA. The Castor bill specifically aims to protect consumers between the ages of 13 to 17, ban targeted advertisements to children, and require an opt-in consent. Castor's bill will include "constructive knowledge" to hold companies responsible for protecting young consumers from the websites they are using (Kern, 2020).

Experience Issues

Fines and breaches seem to be a slap on the wrist for EdTech companies. In 2018, the United States Department of Education released a statement on FERPA enforcement stating that most complaints they receive "involve isolated incidents of inadvertent or accidental disclosures of student education records or PII contained therein" (Improving the Effectiveness, 2018 p. 3). Even if a FERPA violation is accidental, something as small as a student seeing another students grade, it is considered a violation. Though, some may not be aware and that is the problem. If educators make accidental violations in the classroom and those go unreported, how will we know if bigger mistakes are made when using EdTech and no one is reporting or being held accountable for the violations. FERPA is national legislation, meaning every school in the U.S. receiving funds from Department of Education must follow it. There can be serious consequences for FERPA violations. The biggest consequence is that the institute that is receiving funding, may lose federal funds or have their funds reduced (§1232g). Although the biggest consequence is having funds revoked, "No campus has ever lost funding due to violating FERPA" (Couture, 2018, para. 16). In addition to federal FERPA legislation and rules, individual schools may have their own policies when it comes to FERPA violations, for example, University of the Southwest in New Mexico states, that any faculty that violates FERPA may have any of the following consequences

- Temporary suspension of access;
- Inability to perform one's work;
- Possible prosecution under criminal codes; or
- Dismissal/Termination

Control Issues

The main issue with these policies is that they were not well-equipped to handle the ever-changing landscape of consumer engagement with technology. These policies were first introduced in a time of less access and fewer users. Because of this limited knowledge of technological reach, protections under these policies are neither clear nor exhaustive. CARU falls short on many areas such as being clear and precise with what exactly is not acceptable and what constitutes good standing within their guidelines. Complaints from the Public Health Advocacy Institutes towards CARU are "CARU and its supporters advertise or otherwise promote awareness of CARU's activities... nor do they use public-service announcements or similar outlets to encourage consumers to file complaints (Kelley,2005, pg 7) and "CARU's reviews take place only after the fact – when triggered by staff monitoring or by complaints against messages already being disseminated" (Kelley,2005, pg 7).

CARU lacks national awareness, which will broaden its scope by having more consumers aware of deceptive advertisements in order to protect children 12 years along with parents, guardians, and the general public understand what the unit's mission and guidelines are. By doing so, CARU guidelines and definitions should be described and explained better. CARU does not have any outside third party, to review final decisions based on complaints but does submit follow-up actions for the Federal Trade Commission (FTC) to impose on non-compliant companies. To serve the advertising industry, CARU is designed to act unbiased with their decision making. Yet, how does the public rely on CARU's decisions to be fair and who can challenge them if needed? To serve in an unbiased manner, CARU should be funded by outside affiliates. Many speculate CARU is dog that won't bite the hand that feeds them. The potential conflict of interest exists because CARU was developed to help prevent untruthful and deceptive advertising towards children 12 years and younger, yet assumptions CARU is currently funded by advertising, industry affiliates.

SOPIPA's lack of definition of what personally identifiable information is can have broad implications for consumers. Companies can be held to higher standards with this as the FTC can define how certain companies are not compliant with SOPIPA. However, this could be used by the B2B sector to compete against each other. The lack of definition of personally identifiable could also be too broad for operators. Covered information can be used in the business or marketing sector to target specific information to children. Covered information is sourcing data from various locations and sometimes not from the child themselves. Operators can still target parents and source information about their children (McGrath, 2016). Protecting children's information should also encompass the information that is being produced by their guardians and the educators they work around (McGrath, 2016).

FERPA's involvement in EdTech is not well documented. Literature that does exist, simply redefines FERPA rather than discuss the impact on EdTech companies. One article on EdTech Magazines website discusses what schools should know about FERPA in the digital age, but does not discuss any specific instances of EdTech violations, but rather the possibility (Cunningham, 2019). When researching the privacy policy of popular EdTech company, Instructure (owner of Canvas), last updated in October of 2019, there was nothing in it regarding FERPA. Whether the Department of Education is enforcing FERPA in the EdTech space is not clear.

At the higher education level many university and school registrar offices have guides for faculty on how to be complicit with FERPA. The University of California, Los Angeles (UCLA) has a guide that includes tips on how to publish grades, how to take attendance on a roll sheet, and how to go about assigning homework on to a publicly available website. One recommendation they give is to "consider using the campus learning management system" (FERPA for Faculty, 2014). This guide is a little dated, so they are unable to account for all these technological advancements. Although this guide is from UCLA, it can be applied to other schools as well. By advising faculty to use the learning management system, it sounds as if that system is FERPA complicit. While it might be, it is not very clear.

These Parents and Educators especially those working or managing online education during the COVID-19 outbreak are also put in a vulnerable position as their children. These adults are now the gatekeepers of student information, educators are now asking students to create online based content that might not be covered under COPPA's protection. Parents and educators are now also in charge of data security for this information, some of whom are not fit or educated on such matters. From the EdTech companies at this time seem to be taking advantage of the shift to online. This shift to online creates a vast sea of knowledge and information for EdTech companies to be stored and harvested for personal use.

Access Issues

With changing times, technology in education is now used more than ever, with educators using EdTech multiple times a week in the classroom, and students using EdTech even outside of the classroom (Wan, 2019). When schools purchase EdTech products or licenses, they usually do so in bulk quantities so there can be enough products for multiple students to use at once, and enough program licenses for the entire school (The E-Rate Technology, 2020). Doing this, can get expensive so schools typically take advantage of the E-rate program and get a significant discount on EdTech (The E-Rate Technology, 2020).

People

EdTech and Digital Literacy

Technology has influenced multiple industries and changed our overall interactions with computers and programs. Education technology (EdTech) has been one of the biggest advancements in education systems thus far; expected to reach the high billions by 2025 (Marr, 2020). This growing industry has started to influence businesses as well as legislators, teachers, students, and parents/caretakers in one way or another; and has paved the way for digital literacy and digital citizenship. Edtech has helped schools by providing programs and platforms that have changed curriculum for teaching and learning in and out of classrooms. However, privacy issues and data breaches have impacted EdTech businesses and lawmakers.
Digital literacy can be defined as “the ability to find, evaluate, utilize, share, and create content using information technologies and the Internet” (Cornell University, 2020).

In a 2012 article Wan Ng, an associate professor from Sydney who is interested in the cognitive process of learning with technology, presented a framework that has three dimensions: technical, cognitive, and social-emotional (See Figure 7). These three dimensions address the technical and operational skills of technology, the critical thinking that takes place when searching online, and the responsibility of emotionally being able to have online etiquette when communicating online. With the rise of the EdTech industry, digital literacy plays a key role. Although definitions and models like Ng’s give a better understanding of digital literacy, many do not follow a linear interpretation because of diverse experiences, backgrounds and socioeconomic factors. This study will examine key stakeholders and explain the additional influences throughout the way- specifically addressing challenges and benefits of EdTech and digital literacy. It will also address issues related to the COVID-19 crisis which resulted in a shift to virtual learning highlighting the role of Edtech companies in the educational environment.

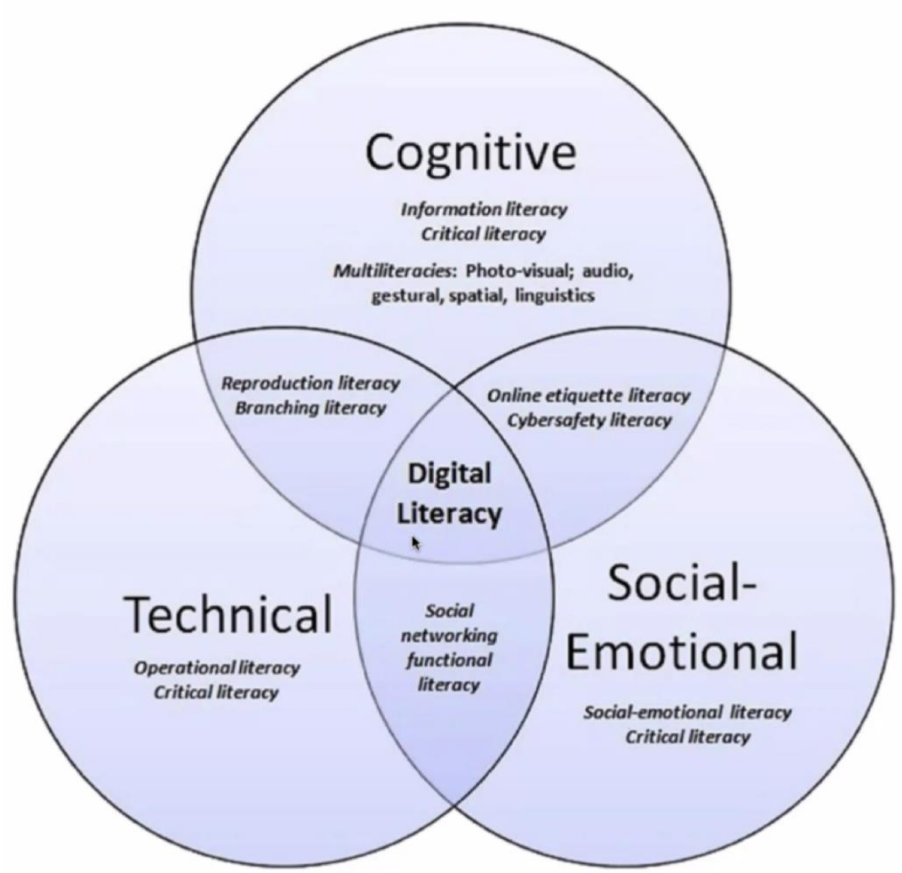

Figure 7. Digital Literacy Model Ng. 2012

Ng, W. (2012). Can we teach digital natives digital literacy?. Computers & Education, 59(3), 1065-1078

<u>Benefits and Challenges of Stakeholders in EdTech</u>

Students in K-12 are considered to be digital natives. Digital natives are those born in the technological era and naturally possess a familiarity with technology. In other words, they are "native speakers" of the digital language of computers, video games, and the Internet (Prensky, 2012). However, as previously discussed merely being a digital native is not enough to conclude that students all possess the same computer skills and knowledge. In a fairly recent study by the International Computer and Information Literacy 2018[1], they found that only 2% of students from Generation Z (people born between the mid to late 1990s) were able to score highly in computer and information literacy- more specifically they were able to independently work with technology to gather and manage information while using evaluative judgment. From this study, one can conclude that digital literacy is a learned skill, like reading and writing, and therefore, falls under school leaders and teachers to properly educate students in this area (Strauss, 2020).

EdTech companies are set out to help find advancements in education by personalizing education, and creating more automated schools through data-driven insights. With the help of students' interactions with connected Internet of Things (IoT) devices and tools, data will be gathered and used for further advancements (Marr, 2020). This data is what provides EdTech companies the information they need to create their programs and platforms. They are able to analyze students' technological skills and knowledge, and test their digital literacy abilities. However, there are two perspectives here: for one, the best way for companies to provide effective educational technologies they need data. However, the gathering of data has been a preceding topic. As Ng's model (Fig. 1) displays, social-economic awareness is a responsibility to use best practices to communicate on these platforms. It addresses security; however, it does not mention privacy. Which brings up questions such as, who is viewing this data? Where is it being gathered? Are students, teachers, and parents aware of this usage? How long is data stored?

Digital Citizenship

From K-12, students are now primarily learning how to safely use the basics of digital literacy such as what information to keep private on the Internet, and how to go to safe places on the computer while using the alphabet to help (www.commonsense.com, 2020).
From grades 3rd through 5th, children begin to learn the responsibilities that come with using these digital platforms and devices, and how to take action in situations that appear as a threat (www.commonsense.com, 2020). These threats include identity theft, how to handle "bullying" and mean/scary remarks online, and lastly, how to be respectful to others. This is important because it is teaching action to students, while making them proactive good digital citizens.

Digital Citizenship falls under a socio-emotional dimension because it involves "the ability to participate in society online" (Mossberger, 2008). Many organizations such as EdSurge and Fractus Learning[2] conclude that there are nine elements involved in digital literacy: digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital health and wellness, digital law, digital rights and responsibilities, and digital security (See Figure 8). Digital citizenship addresses security issues while ignoring a critical aspect that involves digital privacy. Security helps educate children to take online precautions of "stranger danger", cyber bullying, and "fake news". It does not address the knowledge and importance of data gathering by third parties and how it is an invasion of privacy.

Figure 8. Mike Ribble's 9 Elements of Digital Citizenship

Kelli. (2019, January 21). Home. Retrieved June, from http://kellicarlson.org/values-ethics-and-foundations-in-digital-education-ectc-6101/

Privacy Disruption in EdTech

In 1967 there was a significant shift in the use of technology in the US from only government and scientific use to household use by the average American. This shift started to bring attention to how technology had begun to be used as surveillance. Alan F Westin (1967), a legal scholar and author of Privacy and Freedom, tried to warn us of the unforeseen privacy issues that could potentially arise from these advancements; describing us as "the greatest data-gathering society in human history" (pg. 159). Due to the evolving and dynamic nature of technology, it is challenging to identify and address privacy and security issues.
From online transactions, research data, communication, etc., to education, technology is changing everyday lives throughout the years (Westin, 1967). Students have grown up using social media. This means that they are developing a permanent online identity. Educators, parents, and students themselves need to understand that they are leaving a digital footprint due to their online activities and acknowledge that their data is being stored online. More awareness has to be made on privacy, privacy settings, privacy policies and taking the right steps in their personal use. Not managing an online identity can lead to negative consequences at some point without students being aware of this most of the time (Stenger. 2018).

Another complication with EdTech and digital literacy stem from cultural and economic issues. Demographics play a big role in the use of technology and digital literacy. Some households do not own devices such as laptops, tablets, or computers, which can create a difficulty for students and parents to know how to use these devices and platforms. Fortunately, organizations and EdTech companies are beginning to donate devices and programs to help students that are at an economic disadvantage. For example, a middle school from the

Glendale Unified School District in California received free Chromebooks with a four-year data plan from Verizon's Innovate Learning Program –a non-profit (Castenada, 2020). This is a big help for technologically disadvantaged schools and students, however "free" sometimes comes with a price. In another example, the US government funded free smartphones to low income households through the Lifeline Assistance program, however, these devices had pre-installed Chinese malware which endangered their private data. (Brewster, 2020) This is an example of how vulnerable groups tend to be more at risk when it comes to privacy.

Resources

There are resources that help parents increase their digital literacy. The Internet Crimes Against Children (ICAC) Task Force identified an increase in the number of predators attempting to entice kids online (ICAC, 2020). Another issue is that "Kids are using apps and meeting people that are talking them into doing things that compromises their safety" (Bailey, 2020). Some guidelines for parents include having conversations about online safety, requiring your child to gain your permission before accessing new apps, limiting their time online, and also knowing about their children's online friends and habits. Parents might assume that even the most common or popular applications are safe since everyone is on them. Do parents really know what TikTok, one of the most popular and downloaded apps, does? They should be aware that when their child signs up for TikTok, the account is public by default, meaning anyone can see the child's video and location, as well as send them messages. Another app, *Kik*, offers users anonymity and a platform that makes it easy for them to connect with strangers. (Bailey, 2020).

Parents need to be educated about their children's use of technology so that they can make informed decisions for their kids. Common Sense has been a leading nonprofit organization dedicated to improvement of kids' lives and families. There's information for parents, educators, and advocates. The information ranges from Digital Citizenship, EdTech and Expert Advice. (Common Sense, 2020) According to Common Sense young people are now the most tracked and surveilled generation. Children's lives are now online, and the privacy of kids is essential to their safety and well-being. Common Sense has great resources on Digital Citizenship. They have a whole curriculum with lesson slides, videos, customizable resources and bilingual materials for the Spanish community (Common Sense, 2020).

Digital Literacy, Stakeholders and COVID-19

With the shift from classroom learning to remote learning due to COVID-19, the importance of knowledge and understanding of digital literacy is most crucial for parents/caretakers and school teachers. Schools across the US shut down forcing students to continue learning from digital platforms such as EdTech programs and technological devices. "People who never expected –nor ever wanted –to use digital technology to communicate or work now must, and so they are learning how" explained Sean Michael Morris, director of the Digital Pedagogy Lab at the University of Colorado Denver (Morris, 2019). Also adding that the use of these technologies at home requires a new level of digital literacy for everyone. (Bishop, 2020) This shift in learning highlighted the importance of digital literacy, especially of parents and educators. During remote learning, parents have to help their children with their digital device use. If they have poor digital literacy skills, it results in hurting their child's education advancements.

Another challenge that was faced during this time is economic discrepancy between users. Some households do not own a computer or device for their children to use, therefore resulting in a divide that was not present in classroom-based education (Bishop, 2020) Although COVID-19 has impacted the vast majority, there are some that were affected the most. This is yet another example of implications that people face with digital literacy and digital technologies.

K-12 Privacy Post-COVID-19

With the advent of the COVID-19 crisis, teachers had to think of the quickest and most effective way to teach their students from a "distance." As previously mentioned, this has given EdTech companies an opportunity to target and advertise their services to them. Teachers have had a plethora of EdTech vendors contacting them to use their services (Wan, 2020). Educators have been burdened with the task of adjusting to the shift to online education which leaves no time for them to even consider their offerings, however, this goes to show that Edtech companies are really trying to push their services during this crisis. COVID-19 seems like the "perfect" time for tech companies to gain potential customers and potentially-more data.

One of the main platforms that many schools and teachers have had to resort to is Zoom, an online video chat service. In the midst of the crisis, Zoom has become the best alternative for online teaching and keeping students and teachers connected. However, within a few weeks, Eric Yuan, Zoom CEO had to send out an apology for "falling short" of privacy and security measures as users were encountering 'hijacking' and 'video-bombings' –also known as 'Zoombombing'. Unidentifiable individuals were connecting and cyber harassing meetings by using profane words and/or graphic images. New York Schools abandoned Zoom, and moved to other video conferencing services. Also, bringing privacy awareness to end-users. (Chavez and Jorgen, 2020) This is just one example of the consequences that come with the lack of attention to privacy and security of technological platforms. Out of thousands of teachers using Zoom, about 100 were affected within the first month of using it (Wan, 2020). Students in K-12, being 'zoombombed' is unacceptable. It is imperative for educators and parents to know how EdTech companies handle privacy measures.

Through the examples portrayed pre-COVID-19 to the analysis post-COVID-19, it is clear that digital literacy is an important factor to educational technologies. There are many stakeholders involved who have a lot at risk. Digital literacy will continue to benefit students throughout their lives, making it a mandatory skill (Lynch. 2017). For this reason, defining digital literacy is essential for the future of children and students.

Resources Post COVID-19

While society is currently living through history while the COVID-19 pandemic crisis continues to spread, another crisis that is spreading is the use of technology among the education industry. Forty-four million of the nation's 57 million K-12 students have been affected by school closures, and parents and educators are running around trying to adjust to switching in-person teaching to online teaching. Many school districts have been considering implementing E-learning for quite some time now. It's not a matter of consideration-it is REQUIRED. Kristina Ishmael, senior project manager of the teaching, learning, and tech team for New America's Education Policy Program believes that E-learning is rethinking what the K-12 system is capable of doing and meeting the needs of students, which requires the integration of digital learning (Castelo 2020). From the factors to consider, the fourth one is to keep data privacy and security a priority. Joe Phillips, director of technology for Kansas City Public Schools believes that schools might see a huge rise in phishing attempts, malware and spyware scams (Castelo 2020).

There are certainly resources out there for parents and educators to look through while being at home during the COVID-19 pandemic. Edreports.org is a great site to explore. This site is an independent nonprofit designed to improve K-12 education. They currently have a list of tools from the field to navigate the COVID-19 crisis. Making the transition to virtual classrooms is quite a change and the site has tips on how to deal with this change. What this means for Digital Literacy is that now is the time more people will be more involved with this topic if awareness keeps on spreading. People have to be more involved in their community and school districts need to step up their game. CoSN (the Consortium for School Networking) is a professional association for school system technology leaders. They provide resources, community, practices and advocacy tools to help leaders succeed in the digital transformation. They represent over 13 million students in school districts nationwide and continue to be a strong voice in K-12 education. Another resource to look into is the K-12 Cybersecurity Resource Center. This is the new home of a resource known as the K-12 Cyber Incident Map that was launched in March of 2017, and it has been very important since it draws attention to the emerging cybersecurity threats facing the U.S. K-12 public schools and districts.

Programs

This section addresses a few programs that are being offered by Edtech companies. When doing research and looking into a specific company, we would always find another company associated in some way. There are a lot of EdTech program companies and each one comes with more and more connections or partners (See Figure 9). The following information this report contains is just a minor glimpse at what we have been able to dig up so far when it comes to programs.

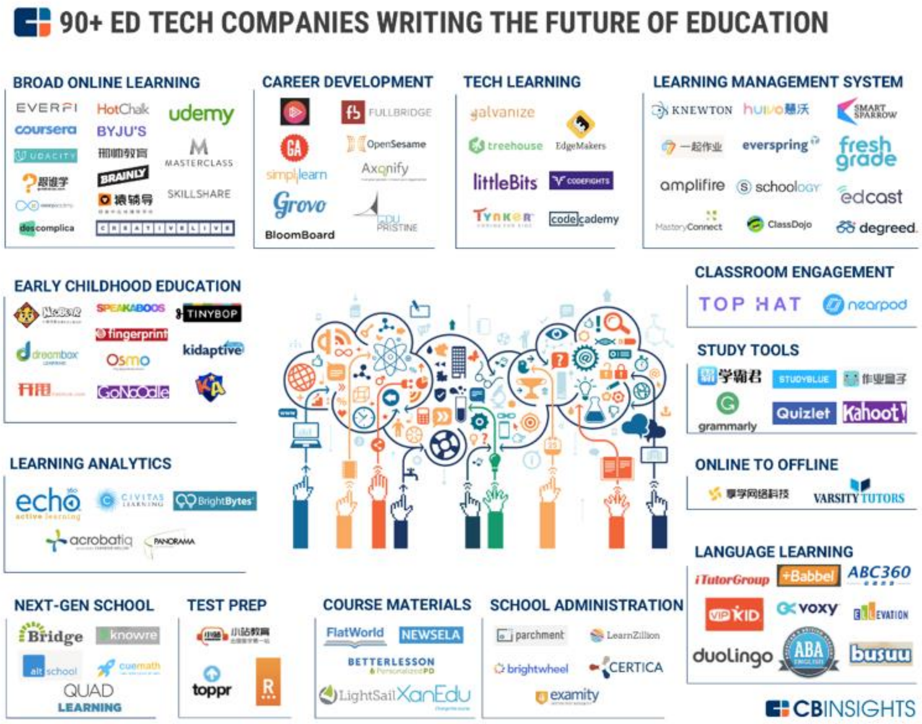

Figure 9. CBINSIGHTS Ed Tech Companies

CB Insights. (2017, June 21). The Ed Tech Market Map: 90+ Startups Writing the Future of Education. Retrieved June 11, 2020, from https://www.cbinsights.com/research/ed-tech-startup-market-map/

With progressions in education technology becoming more and more advanced, educators, parents, and law makers are beginning to notice some dangerous flaws with these programs regarding K-12 student's privacy. The first problem involves responsibility shift regarding privacy concerns from the education technology firms themselves, to other parties like teachers and school districts. Next, we see a series sales pitches unrelated to education technology being used to justify the risks of using the services. Finally, we see critical privacy concerns that users of these software's are often unaware of.

When privacy concerns with education technology first became apparent, the first instinct for stakeholders was to shift the responsibility of privacy to other parties. One popularly used education technology software is called GoGuardian. GoGuardian is a monitoring software that allows school administrators to limit what students are able to view and access from school distributed computers. The software not only blocks certain sites but also allows for administrators to see what students were using their laptops for. Larry Magid in his article on GoGuardian states that "Officials -- including administrators and teachers -- need to be accountable for how they use the service in terms of what they block and what information they access." (Magid, 2016). While it is vital that firm acknowledge that someone must be held accountable for the various uses of these software, stating that these responsibilities should be left up to administrators and teachers is just a way for education technology companies to protect themselves. If teachers and administrators are accountable for what information is being monitored, are they then also responsible for teaching users about their privacy when using school devices? The fact of the matter is that school administrators and teachers do not have the resources to take over these kinds of decisions, and the responsibility about privacy and what these software are capable of must be left up to the firms that create them.

The next issue that we see with education technology, are sales pitches based on unrelated problems. For example, GoGuardian makes claims about how its service has helped to prevent suicide. COO of GoGuardian Todd Mackey states "Our administrators continue to tell us how they have been able to positively intervene when students are searching in earnest on how to kill themselves. It's very very powerful" (Magid, 2016). Of course, preventing student's suicide is an important issue, but it should not be an issue for education technology software. The problem with this is that we eventually end up with firms making claims that they have a service that can "do it all" which ends up with amplified privacy concerns as the student data collected becomes more and more complex.

As education technology becomes more and more advanced, we still do not see privacy concerns as a main issue of discussion until after there is a problem. Many examples of this arose during the COVID-19 epidemic as education technology companies saw their chance to grow their services and educators had no choice but to switch to online learning. Zoom's CEO Eric Yuan was quick to reach out to K-12 schools and offer the zoom's video conferencing service for free (Conrad, 2020). Many K-12 learning facilities quickly jumped at the opportunity to use the platform as a way to continue face to face communication with their students. A problem was quickly uncovered as Zoombombing became more and more prevalent in online classes where "Calls have been hijacked by unidentified individuals and trolls who spew hateful language or share graphic images" (Chavez, 2020). Another example of this phenomenon is occurring as schools attempt to provide devices to students who may not be able to obtain them themselves. We see this with Glendale Unified School District's attempt to provide Chromebooks to their students at a ratio of three students to one device (Castaneda, 2020). Castaneda's article highlights all of the benefits of students participating in online learning but ignores the fact that doing so could lead to privacy risks, such as data collection, to the students and if anything is being done to remedy these risks.

Another commonly used education technology service that is gaining more and more traction through its usability is Googles G-suite. G-suite includes services like Gmail, Google Docs, Google Drive, and other online communication and collaboration tools. I believe G-suite is becoming so popular because of its convenience and familiarity among students and teachers. For many of the digital natives in K-12 schools today, using Google services outside of schools is nothing new for them so the transition to use it for online learning is much easier than a switch to unfamiliar services. The problem with this ease of use is that privacy concerns involved are easily overlooked or traded for convenience. In G-suites own privacy policy, it admits to not only collecting personally identifiable information like name, email and IP address, but also then sharing this information with "other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures" (Google For Education). As Google shares this information with "trusted" affiliates, it may become unclear what is happening with student data once it leaves Googles hands, and leave data exposed to dangers of data breaches or selling information. New Mexico attorney general, Hector Balderas, took notice of some of the practices Google participates in through his own investigation and discovered that Google also tracks student and teacher information outside of school and on all of their devices, violating COPPA regulations. Although Google denies the claims, the pending lawsuit will likely uncover the truth in this case and could lead to yet another fine for Google violating this same regulation that they have already been punished for in the past (Morrison, 2020).

The pattern that is developing within education technology is a tendency to be on polar ends of a spectrum when it comes to privacy. Either no one is talking about privacy concerns and education is marketed as the best thing to happen to education, or privacy is the only thing that is discussed and there is no reason to change to technology from traditional learning. Obviously, our world is becoming more and more digital every day and whether we like it or not, younger generations need to become accustomed to using this platform from early stages of communication. What is needed is a middle ground, where children learn to use technology through education technology services, but in a way that takes privacy and childrens' safety online as the most important factor when developing and choosing to use these services.

Abre was named EdTech startup of the Year in 2019 at the EdTech Breakthrough Awards. Abre gives administrators, teachers, students, parents and community members access to information and provides them with tools to manage students and staff, and delivers instructions while engaging with school operations. In 14 months of operating, Abre has been used by over 38 school systems and over 240 schools and has been making waves in the technology software used in classrooms. (PR Newswire)

Abre offers flexible platforms that focus on school management, professional learning, learning management, communication, data visualization, and community engagement. Navigating its website, we noticed they have partnerships that include *Google Cloud, Google for Education, Student Privacy Ledge, Project Unicorn, IMS Global, and Certica*.

Abre has a K – 12 School Service pledge to safeguard student privacy. These school service providers are supporting teachers, students, and parents to manage student data, carry out school operations, support instruction and other learning opportunities as well as developing and making improvements on products or services that are intended for educational use. One thing Abre commits to is to not collect, maintain, use or share student personal information that isn't intended for educational purposes. They only collect, use, share and retain personal student information only for purposes of education which is a bit confusing. (Student Privacy Ledge)

Issues in the ***Student Privacy Pledge*** are in the definitions section, according to an Electronic Frontier Foundation article. A loophole in the pledge is its definition of "school service provider." It's limited to providers of applications, online services, or websites that are marketed for education purposes. Although it's marketed for classrooms, the product itself might not be "designed" for educational purposes. The pledge isn't transparent in informing about other providers of devices like laptops and tablets, and those are free to collect and use student data. (Cope and Gebhart, 2016)

Project Unicorn is an organization or a program of various committees. Its mission is to improve data interoperability within K-12 education. They want to determine shared priorities by working in partnerships with school systems and certain vendor. They have quite a few names on their committee. Some include Common Sense, EdSurge, InnovateEdu, and SIIA.

Another program that we looked at is ***CENTEGIX***. They are known to be a leader in safety and security for K-12 schools. They have developed a Crisis Alert program with Classroom Video Solutions. (PR Newswire) CrisisAlert provides a reliable management solution that uses a secure network for instant alerting at schools. (CENTEGIX)

Next up is ***Zearn,*** one of the top and best EdTech programs out there for kids. It's targeted for grades K-5 and it's an innovative combination of live instruction and adaptive online math classes. It has an 88% Privacy Rating from Common Sense which is pretty good but there are still some concerns. When it comes to data safety, there are still warning signs on personal information being displayed publicly and user-created content is not filtered for personal information before being made publicly visible. When it comes to data rights, users can create or upload content. Then on the ads and tracking aspect, it is still unclear whether this product displays traditional or contextual advertisements. (Common Sense) Zearn is one of the best programs out there and these issues are still present, which means that many other programs must really be breaching into the privacy factor in kids or using that as an excuse to find more information for their benefit.

<u>Programs in high demand due to COVID-19</u>

Schools and educators have been scrambling to keep students engaged as the world has shifted to virtual learning. During this Pandemic, certain programs are on the rise. Google classroom has been one of companies to benefit from the crisis right now. Google Classroom which is a company for posting and collecting assignments, collaboration, and discussion is also adding Meet integration to quickly generate video calls. Google Classroom has over 100 million users. (Li 2020)

Another program that should be considered right now is ***Nepris***. Its mission is to industry engagement part of the everyday classroom by empowering teachers to engage students in steam. By facilitating virtual connections, Nepris effectively removes student barriers to access while providing companies the opportunity to efficiently reach out to students. With this program, teachers can pick a curriculum topic or student project and Nepris finds and invites a certain industry professional to show how the topic is applied in their work. With Nepris, students gain early exposure to high tech professionals.

Programs (Nodes and Networks)

Refer to the Spreadsheet for findings

This part of the research focuses on studying EdTech companies to find nodes and networks in order to create a map of the digital landscape. These connections are useful in analyzing the relationships and interdependencies of various EdTech companies, and how student data becomes a shared resource. The first step of the process in this investigative research was to find out which programs are being used in schools across California. The number and variety of programs used by different schools is diverse, and the relevant information is hard to find. Schools/school districts typically do not have this information on their website. General information about programs can be found online, but more sophisticated information like tracking each program to the parent company and to see interconnections between these companies is challenging. Two popular LMS used in elementary schools are Schoology and Haiku Learning. Both these LMS are owned by the same parent company which is called Powerschool. Any information shared by students on either one of these LMS goes to Powerschool. Other major Edtech companies are Houghton Mifflin Harcourt and Mc GrawHill. Both these companies are known as textbook publishers, but they also offer Edtech programs to schools. Houghton Mifflin Harcourt owns popular preschool educational games Reader Rabbit aimed for students preschool to age nine, and Cluefinder for older students, aged seven to twelve. McGraw Hill owns various popular programs like Connect, Inspire Science and Aleks Math program. Due to the nature of this investigative work, the research is still a work in progress so new findings are anticipated along the way.

Due to the COVID-19 crisis, schools all over the US have shifted to online learning. As mentioned earlier, the two most widely used tools during this time are Zoom and Google Classroom. Zoom joined the Centrify alliance partner program in 2013. This partnership features joint sales initiatives, targeted marketing campaigns and technology integrations (Centrify, 2013). Google classroom is a free web service which allows file sharing between teachers and students. Due to easy accessibility and zero economic costs, the service is being used by many school districts during COVID-19 school shutdowns. The number of users has doubled to 100 million since the outbreak (Schoon 2020). According to App Brain, “the Classroom app wasn’t even in the top 100 education apps until early March 2020. However, starting March 10, the app saw a huge spike and went to reach the top 5 most popular apps in the U.S.”

COVID-19 RESPONSE WITH EDTECH

During the COVID-19 Pandemic, an unprecedented reliance on educational technology took place as schools were forced to transition to online learning alternatives. This crisis situation exposed many privacy concerns and security tradeoffs with some of the most dominant educational technology service providers, including Zoom and Google. Initially, many schools relied on the video conferencing services that Zoom offered for free as the pandemic escalated (Konrad, 2020). On the limited amount of time that educators had to make the transition to online learning, there was no resources for much research to be done on these services and educators were forced to have faith in software and surrender their own, and their students, information in an attempt to have a successful end to the school year. Not long after Zoom was implemented, major privacy concerns began to arise leading to some schools suspending the use of the service (Chavez and Jorgensen, 2020). Schools and companies began to notice many of the flaws with Zoom, from its limited security measures and vulnerability to “Zoombombing” (Dawn, 2020) to attention tracking abilities allowing managers to receive alerts when employees were using other programs on a computer during Zoom meetings (Grauer, 2020).

Unsatisfactory security measures did not stop with Zoom however, Google was another culprit that seemed to take advantage of the COVID-19 pandemic to further push its own personal agendas. With many employees having multiple Google accounts, it was found that Google can link work or school and personal accounts based on things like phone number and personal data (Grauer, 2020). This security flaw is beneficial to Google’s compilation of consumer data and may be seen as a strategy to expand this data. Through complex privacy policies, Google is effectively able to stay out of legal trouble while using questionable measures to take advantage of vulnerable consumers and using a pandemic to expand their data.

Although it took a major global crisis, we are beginning to uncover many of the privacy concerns with online services that have gone largely unnoticed since their conception. As consumers were forced to move online, more and more of these security “flaws” or intentional security policies came to the foreground of conversation. As the COVID-19 pandemic progresses, it will be worth noting whether or not companies resolve these privacy concerns to better protect their consumers, or if they continue to act based on what benefits them as a company. So far, the crisis has proven that many companies are willing to take advantage of any situation to collect customer data, and it is not likely that any of this will change without major public pushback.

NEXT STEPS

In the months to come, we will be continuing with the interview process; outreach, scheduling, conducting, and transcribing. We will be using the data gathered in our qualitative interviews to inform the design and content of a quantitative survey that will be disseminated to these and other school districts across California.

As we continue outreach and interviews for school districts, we also plan to begin reaching out and interviewing EdTech and MarTech firms themselves. As important as it is to get individual schools' points of view on educational technology, it is equally important that we get the point of views of the companies that develop these technologies in the first place. From these interviews, we hope to get a sense of how the technologies are developed and whether or not student's privacy is a concern in the development process. By completing school district and tech firm interviews, we hope to paint a complete picture of the education technology industry and uncover why it may have shortcomings and how they can be addressed.

We have already made our social media accounts for Instagram and Twitter, @K12PrivacyTeam on both. In the next few weeks, we will be working with a social media marketing class (MKT 459) at California State University, Northridge to help manage the accounts. We hope this gives the students a good opportunity to practice what they are learning and to also help us find our voice on the platforms. About halfway through the spring 2020 semester, five of the research assistants started to work on the social media to try to build a following, there was not much luck. We hope with the help of the social media marketing students we can build a following and get insight on what type of posts that followers like to see.

As the COVID-19 pandemic develops, we will continue to research that the effects of EdTech and MarTech are having on K-12 students. We will continue in-depth research of both schools and EdTech/MarTech's response to the changing environment and whether or not they are capable of making necessary changes to continue online learning while also protecting student data and privacy. It will also be interesting to see what kinds of changes we see after the pandemic in looking at how and if schools will transition their students back to online learning.

The data gathered from our literature review, our interviews and surveys, and the COVID-19 outbreak will be used to inform a new endeavor. We hope to conduct a more exhaustive analysis of the EdTech procurement process in school districts across the country.

NEXT NSF PHASE OVERVIEW

- CA EdTech (and U.S.) and COVID-19 influence
- Outreach and Interviews (Transcribe)
- Survey Draft Development

School District Reports

- Social Media Account Content Progress
- Plan/hire faculty qualitative research
- Plan/hire/independent study options for graduate and undergraduate assistants as needed

- Administrative Goals:
    - NVivo how-to guide
    - Tableau how-to guide
    - Budget Planning (TUC processes)

References

A.G. Schneiderman Announces Results Of "Operation Child Tracker,". (2016). Retrieved from https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online

Alexander, Julia. "TikTok Will Pay $5.7 Million over Alleged Children's Privacy Law Violations." The Verge, The Verge, 27 Feb. 2019, www.theverge.com/2019/2/27/18243312/tiktok-ftc-fine-musically-children-coppa-age-gate.

Bailey. Michelle L. (27. Feb. 2020) Keep Kids Safe Online: Social Apps, Parental Controls & More. Retrieved April 23, 2020, from: https://www.northeastohioparent.com/technology/keep-kids-safe-online-social-apps-parental-controls-more/

Bishop. K. (24. Apr. 2020) We're embracing tech during lockdown – but can it replace the classroom?. The Guardian. https://www.theguardian.com/technology/2020/apr/24/remote-learning-classroom-technology-coronavirus

Castaneda. V. (21. Feb. 2020). 3 Glendale Unified middle schools are undergoing a technology update. Glendale News-Press. Retrieved https://www.latimes.com/socal/glendale-news-press/news/story/2020-02-21/tn-gnp-me-glendale-unified-verizon-program

Castelo. M. (25. Mar. 2020). Factors to Consider When Preparing for E-Learning. EdTech Magazine. Retrieved https://edtechmagazine.com/k12/article/2020/03/factors-consider-when-preparing-e-learning-perfcon

Chavez, N. (2020, April 5). New York City schools won't be using Zoom anymore because of security concerns. Retrieved from https://www.cnn.com/2020/04/04/us/nyc-schools-zoom-online-security/index.html

"Children's Advertising Review Unit: BBB National Programs." Retrieved from bbbprograms.org/programs/all-programs/caru.

Children's Internet Protection Act (CIPA). (2019, December 30). Retrieved from http://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Clark, L., & Gould, M. (2001, March 20). ALA files lawsuit challenging CIPA. Retrieved from http://www.ala.org/advocacy/advleg/federallegislation/cipa/alafileslawsuit

Couture, R., Schwen, J., & Couture, V. (2018). FERPA Fear or FERPA Flex: Student ... - sahe.colostate.edu. Retrieved from https://sahe.colostate.edu/ferpa-fear/

Cremin. J and Gallagher. K. (2016, Aug 03). How to Take Digital Citizenship Schoolwide During the 2016-17 School Year. EdSurge. Retrieved https://www.edsurge.com/news/2016-08-03-how-to-take-digital-citizenship-schoolwide-during-the-2016-17-school-year

Cunningham, Erin. “FERPA Compliance in the Digital Age: What K–12 Schools Need to Know.” *Technology Solutions That Drive Education*, EdTech Magazine, 5 June 2019, edtechmagazine.com/k12/article/2019/09/ferpa-compliance-digital-age-what-k-12-schools-need-know-perfcon.

Darling-Hammond. L. (19. Mar. 2020). Learning in The Time of COVID-19. Forbes. Retrieved https://www.forbes.com/sites/lindadarlinghammond/2020/03/19/learning-in-the-time-of-covid-19/#6d57860e7203

Der Hof, S. (2016). I agree ... or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal, 34*(2), 409-445

Family Educational Rights and Privacy Act (FERPA). (2018, March 1). Retrieved March 12, 2020, from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Fattal, T. (2020, March 12). Harvard-Westlake closes campus, halts spring athletics due to coronavirus concerns. Retrieved from https://www.dailynews.com/2020/03/11/harvard-westlake-closes-campus-stops-spring-athletics-due-to-coronavirus-concerns/

For K-12 School Administrators and Ed Tech Vendors. *Future of Privacy Forum*. Retrieved from https://fpf.org/2016/11/07/fpf-guide-student-data-protections-sopipa-k-12-school-administrators-ed-tech-vendors/

Gadbaw, T. (2016). Legislative update: Children's Online Privacy Protection Act of 1998. *Children's Legal Rights Journal, 36*(3), 228-232.

Grom social keeping kids safe online during COVID-19 pandemic. (2020, Mar 30). NASDAQ OMX's News Release Distribution Channel Retrieved from http://libproxy.csun.edu/login?url=https://search-proquest-com.libproxy.csun.edu/docview/2384145019?accountid=7285

“History of COPPA Violations.” PRIVO, www.privo.com/history-of-coppa-violations.

Horn, M. (2016). Moving EdTech Forward. Education Next, 16(1), Education Next, Winter 2016, Vol.16(1).

Improving the Effectiveness and Efficiency of FERPA Enforcement, Improving the Effectiveness and Efficiency of FERPA Enforcement (2018).

Jeup, Jeanne “*The adoption of Edtech in the Connected Classroom*” https://www.educationworld.com/a_curr/adoption_edtech_connected_classroom.shtml

Johnston. R. (2019. Aug 22). Lawmakers investigate tech companies' student data collection, usage. Edscoop. Retrieved https://edscoop.com/lawmakers-investigate-tech-companies-student-data-collection-usage/

Kelly, B. (2005). Process Defects. In *Industry Controls Over Food Marketing to Children: Are They Effective?* Stanford, CA: The Public Health Advocacy Institute.

Kern, Rebecca (2020) "House Bill Would Allow Suits Over Kids' Privacy Violations (1)." Bloomberg Government, 30 Jan. 2020, about.bgov.com/news/house-bill-would-let-parents-sue-over-kids-privacy-violations/.

Kohli, S. (2020, April 1). Public schools expected to remain closed for the rest of the academic year, Newsom says. Retrieved from https://www.latimes.com/california/story/2020-04-01/coronavirus-school-closures-california

Konrad, A. (2020, March 14). Exclusive: Zoom CEO Eric Yuan Is Giving K-12 Schools His Videoconferencing Tools For Free. Retrieved from https://www.forbes.com/sites/alexkonrad/2020/03/13/zoom-video-coronavirus-eric-yuan-schools/#dd2a7b64e714

Legislative History of Major FERPA Provisions. (2005, December 19). Retrieved March 12, 2020, from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html#:~:text=The 1994 IASA amendments extended, place at the local level.

Loveless. B. (2020) The Importance of Digital Literacy in K-12. Education Corner. Retrieved

https://www.educationcorner.com/importance-digital-literacy-k-12.html

Morrison, Sara. "Google's Education Tech Has a Privacy Problem." *Vox*, Vox, 21 Feb. 2020, www.vox.com/recode/2020/2/21/21146998/google-new-mexico-children-privacy-school-chromebook-lawsuit.

Morris. B. (2019. Jul 10). Schools Wrestle With Privacy of Digital Data Collected on Students. The Wall Street Journal. Retrieived https://www.wsj.com/articles/one-parent-is-on-a-mission-to-protect-children-from-digital- mistakes-11562762000

"Musical.ly's Agreement with FTC." Newsroom, Newsroom | TikTok, 14 Apr. 2019, newsroom.tiktok.com/musical-lys-agreement-with-ftc/.

O'Flaherty, K. (2020, April 10). Zoom Security: Here's What Zoom Is Doing To Make Its Service Safer. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2020/04/10/zoom-security-heres-what-zoom-is-doing-to-make-its-service-safer/

Overview of CIPA, COPPA, and FERPA. Dec. 2015, www.spps.org/cms/lib/MN01910242/Centricity/Domain/11270/OverviewofCIPACOPPAandFERPA12.2015.pdf.

Protecting the Privacy of Student Education Records. (1997, March). Retrieved from https://nces.ed.gov/pubs97/web/97859.asp

Prensky. M. (2001. Oct 01). Digital Natives, Digital Immigrants. NBC University Press, Vol. 9 No. 5. Retrieved 2020. May 07

Roscorla, T. (2015, August 27). More States Pass Laws to Protect Student Data. Retrieved from https://www.govtech.com/education/k-12/What-States-Did-with-Student-Data-Privacy-Legislation-in-2015.html

Rouse, M. (2010, May 03). What is COPPA (Children's Online Privacy Protection Act)? - Definition from WhatIs.com. Retrieved June 03, 2020, from https://searchcompliance.techtarget.com/definition/COPPA-Childrens-Online-Privacy-Protection-Act

SB 1177, 2014 Steinberg, 2017 reg Session. (CA 2014)

"SOPIPA: Common Sense Kids Action." Retrieved from, www.commonsensemedia.org/kids-action/about-us/our-issues/digital-life/sopipa.

St. Amour, M. (2020, March 25). Pivot to online raises concerns for FERPA, surveillance. Retrieved from http://www.insidehighered.com/news/2020/03/25/pivot-online-raises-concerns-ferpa-surveillance

Starting today, due to the COVID-19 pandemic, bulb digital portfolios is free for schools worldwide: This initiative will apply for the rest of the school year and through the summer. no commitment required. (2020, Mar 13). PR Newswire Retrieved from http://libproxy.csun.edu/login?url=https://search-proquest-com.libproxy.csun.edu/docview/2376681738?accountid=7285

Stenger. M. (22. Oct. 2018). 7 Ways to Teach Digital Literacy. Open Colleges. Retrieved https://www.opencolleges.edu.au/informed/edtech-integration/7-ways-teach-digital-literacy/

Stone J. Revisiting the Purpose and Effect of FERPA (2002, February)

Strauss. V. (2020. Mar 20). As schooling rapidly moves online across the country, concerns rise about student data privacy. Washington Post. Retrieved https://www.washingtonpost.com/education/2020/03/20/schooling-rapidly-moves-online-across- country-concerns-rise-about-student-data-privacy/

Strauss. V. (16. Nov. 2019) Today's kids might be digital natives but a new study shows they aren't close to being computer literate. Washington Post. Retrieved https://www.washingtonpost.com/education/2019/11/16/todays-kids-may-be-digital-natives-new-study-shows-they-arent-close-being-computer-literate/

The E-rate Technology Discount Program. (2020). Retrieved from https://www.ncea.org/NCEA/Lead/Public_Policy/E-Rate_Program.aspx

Truong. D. (1. Feb. 2020) More students are learning on laptops and tablets in class. Some parents want to hit the off switch. Washington Post.Retreived https://www.washingtonpost.com/local/education/more-students-are-learning-on-laptops-and-tablets-in-class-some-parents-want-to-hit-the-off-switch/2020/02/01/d53134d0-db1e-11e9-a688-303693fb4b0b_story.html

United States v. American Library Association. 539 U. S. 194. Supreme Court of the United States. 2003

Varella, L. (2016, Spring). When it rains, it pours protecting student data stored in the cloud. *Rutgers Computer & Technology Law Journal*, *42*(1), 94+. Retrieved from https://link-gale-com.libproxy.csun.edu/apps/doc/A455286508/EAIM?u=csunorthridge&sid=EAIM&xid=749e371b

Wan, T. (2019, September 16). Not Just Classroom Supplies: Teachers Also Buy Edtech With Their Own Money - EdSurge News. Retrieved from https://www.edsurge.com/news/2019-09-11-not-just-classroom-supplies-teachers-also-buy-edtech-with-their-own-money

Wan, Tony (2020) "*Want to help schools closed by COVID-19? Don't pitch them right now" Ed Surge* https://www.edsurge.com/news/2020-03-16-want-to-help-schools-closed-by-covid-19-please-don-t-pitch-them-right-now

Westin, A. F. (1970). *Privacy and freedom*. New York: Atheneum.

Zoom and FERPA Compliance. (2018, February). Retrieved from https://zoom.us/education

20 USC 1232g: Family educational and privacy rights, 2016, November. FPF Guide to Protecting Student Data Under SOPIPA