LAKE FOREST COLLEGE

OUR FUTURE, OUR PROBLEM

Luisa Yamel Muñoz Torres
& Taqiul Ghani
Public Policy Challenge

Executive Summary

The Problem

Are Students Information Used in Online Educational Services Protected by FERPA?

According to the Department of education, "It depends." Because of the diversity and variety of online educational services, there is no universal answer to this question. The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects Personally Identifiable Information (PII) from students' education records from unauthorized disclosure. Metadata that have been stripped of all direct and indirect identifiers *are **not** considered protected information under FERPA because they are not PII.* A provider that has been granted access to PII from education records under the school official exception may use any metadata that are not linked to FERPA-protected information for other purposes unless otherwise prohibited by the terms of their agreement with the school or district. It is important to remember that students are using apps and websites for educational purposes not provided by the school, exposing their PII to be misused. There is no distinct limitations governing the use of PII being collected by educational apps in the United States, exposing millions of students.

Solution

FERPA should be amended to take in consideration of the new reality, where educational services are being used by the significant majority of the K-12 system, leaving the federal law's intent incomplete. The amendment to the existing policy 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A) will set regulations to online educational services to limit the collection of private information of students, protecting the privacy rights over 49 million children in the United States.

Opportunity

- Review metadata policies: Review and update metadata policies to ensure that they comply with privacy laws and regulations, such as GDPR or CCPA.
- Limit collection: Limit the collection of unnecessary metadata to reduce the risk of potential data breaches or privacy violations.
- Secure storage: Store data securely to protect it from unauthorized access, use, or disclosure.
- Anonymize metadata and restrict use other than the intent of social research: Consider anonymizing metadata to reduce the risk of re-identification and protect sensitive information.
- Manage access: Manage access to metadata, just as you would manage access to data. This includes limiting who can access metadata and ensuring that access is based on a legitimate need to know.
- Monitor and audit: Monitor and audit metadata usage to detect any unauthorized access or use, and to ensure that metadata is being used in compliance with privacy policies.
- Communicate with users: Clearly communicate with users about the metadata that is being collected, how it is being used, and how it is being protected.

Table of Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

As we age and technology advances, it is imperative that our laws evolve to keep pace with the changing landscape, ensuring they remain effective, relevant, and able to address the challenges and opportunities that arise in our rapidly evolving society.

Chapter 1

Introduction:

The evolution of human history has been closely intertwined with the evolution of communication, which has been a fundamental aspect of our progress as a species. The Internet has significantly altered the way we communicate, providing a new platform for expression and connection. This discovery, in the mid 1970's was groundbreaking but its potential and threat is only becoming more prominent in the current era. The Internet became commercially available in the mid 1990's and has made it possible for people to connect with others from all over the world in real-time. Overall, the Internet has changed almost every aspect of our lives, from how we communicate and learn, to how we do business and entertain ourselves.

As technology continues to evolve, we evolve and can expect the Internet to continue to shape and transform our lives in new and unexpected ways. Throughout the 1990s, the Internet experienced explosive growth as more and more individuals and organizations commercially began to utilize the power of the network. The development of the World Wide Web, which allowed for the creation and sharing of content in a user-friendly way, played a significant role in this growth. Fast-forward to 2023, the Internet is playing a crucial role in education, particularly in the K-12 sector. The widespread availability of high-speed Internet and mobile devices, educational apps have become more accessible to young students of all backgrounds.

One of the biggest advantages of educational apps is their ability to provide personalized learning experiences. Apps can be tailored to meet the individual needs and learning styles of each student, allowing them to learn at their own pace and in their own way. They can incorporate multimedia elements such as videos, animations, and interactive quizzes, which can help students better understand and retain information. Overall, the Internet and the evolution of educational apps have made learning more accessible, interactive, and engaging than ever before.

This creation has effectively changed the world by globalizing education through online platforms. To counteract this danger, a federal law exists for protecting students' private and educational records, the law is called Family Education Rights And Privacy Acts (FERPA) from 1975. The law is however outdated as online educational platforms are not required to follow FERPA because these educational platforms are not receiving federal funding, called Free Application For Student Aid (FAFSA). Thus, educational applications are collecting and selling students' data nevertheless, imposing safety and privacy concerns for 50 million K-12 students in the United States[1]. Our research is focused on why and how can FERPA achieve its intent and accommodate the needs of educational institutions, stakeholders, students and parents.

[1] *The NCES Fast Facts Tool provides quick answers to many education questions (National Center for Education Statistics)*. National Center for Education Statistics (NCES) Home Page, a part of the U.S. Department of Education. (n.d.). Retrieved April 4, 2023, from https://nces.ed.gov/fastfacts/display.asp?id=372

One of the key areas where FERPA needs to evolve is in response to the increasing use of technology in education. With the growth of online learning and digital tools, there are concerns about the security and privacy of student data being misused and sold. We suggest that FERPA should be updated to provide more guidance and regulations around the use of technology in education, including the use of student data for research and analytics purposes. The focus is to analyze the change needed in FERPA to complete its true intent. For example, there are increasing numbers of nontraditional students, such as adult learners and online students, who may have different privacy needs than traditional students. FERPA could be updated to better accommodate the privacy needs of these students, including the use of anonymous data and other privacy-enhancing technologies.

Finally, there are ongoing discussions about how FERPA should evolve to better protect student privacy in the context of emerging technologies such as artificial intelligence (AI) and machine learning. FERPA should be updated to provide clear guidelines and regulations around the use of these technologies in education, including the collection, analysis, and use of student data for AI and machine learning applications.

1.1 Definition of K-12 educational system of United States

K-12 refers to the education system in the United States that includes kindergarten through 12th grade. This system is designed to provide a comprehensive education to students from a young age, and prepare them for higher education or the workforce. Kindergarten typically starts at age 5 and is followed by 12 grades of primary and secondary education. The curriculum in K-12 education includes a wide range of subjects such as English, math, science, social studies, and physical education. Additionally, many schools offer electives such as art, music, and foreign languages which need the access and the help of educational apps to succeed the journey of these kids.

The K-12 education system is typically divided into three levels: elementary school (K-5 or K-6), middle school (6-8 or 7-8), and high school (9-12). Each level builds on the previous one, with high school being the final stage before students graduate and either move on to higher education or enter the workforce. K-12 education is typically publicly funded, with the majority of schools being run by local school districts. However, there are also private and charter schools that offer alternative educational options.

1.2 Data and privacy security of K-12 Students in the United States

FERPA applies to all educational institutions that receive federal funding, including public schools, private schools, and colleges and universities. Under FERPA, schools are required to obtain written consent from parents or eligible students (18 years or older) before disclosing any personally identifiable information (PII) from a student's education records. This includes information such as grades, transcripts, and disciplinary records. However, schools are allowed to disclose PII without consent in certain circumstances, such as when the disclosure is to school officials with a legitimate educational interest, or when the disclosure is required by law.

FERPA also gives parents and eligible students the right to inspect and review their education records, and to request that any inaccuracies be corrected. Additionally, schools are required to maintain the confidentiality of education records and to ensure that they are stored in a secure location. FERPA plays a crucial role in protecting the privacy of students' education records in K-12 education by extending these privacy protections to each student. The consequences for not following FERPA is losing federal funding, a main source of revenue for the majority of schools.
However, there is no legislation that asks educational platforms to oblige by FERPA unless they are in partnership with schools in the United States that receive federal funding. The majority of almost 500,000 applications and websites students use daily[2] are independent of federal funding, thus selling data is a major source of revenue for these companies, jeopardizing the safety and rights of students. Now, what are the legal frameworks for these applications and regulatory educational applications.

1.3 Legal Framework of educational apps in the United States

The legal framework for educational apps depends on a number of factors, including the target audience, the purpose and function of the app, and the jurisdiction in which the app is offered. However, there are some general legal considerations that apply to these educational apps:

1. *Privacy:* Educational apps that collect personal information, such as names, email addresses, and browsing histories, must comply with applicable privacy laws and regulations, such as Children's Online Privacy Protection Act (COPPA) in the United States.
2. *Intellectual property:* Educational apps must respect intellectual property rights, including copyrights and trademarks. Developers must ensure that they have the appropriate licenses or permissions to use any third-party content, such as images or music.
3. *Accessibility:* Educational apps should be designed to be accessible to users with disabilities, in compliance with accessibility laws and regulations such as the Americans with Disabilities Act (ADA).

[2] U.S. Department of Education. (2018). Family Educational Rights and Privacy Act (FERPA). Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

5. *Safety:* Educational apps must provide a safe environment for users, especially when the app is targeted towards children. Developers must take measures to prevent cyberbullying, inappropriate content, and other safety risks.
6. *Terms of service and end-user license agreements:* Educational apps must provide clear and concise terms of service and end-user license agreements that specify the user's rights and obligations when using the app.

However, there is no clear statement indicating that third party educational apps have obligations to protect and preserve student's records as they are not 'obligated' to follow FERPA, leaving the intent of the federal law incomplete and the safety and privacy of students at major risk.

Initial intent *of FERPA*

The Family Educational Rights and Privacy Act (FERPA) is a federal law that was enacted in 1974. Its purpose is to protect the privacy of student education records and to give parents or eligible students (those over 18 years old or attending a *post-secondary institution) certain rights with respect to those records.* FERPA was enacted in response to concerns about the privacy and confidentiality of student records[3]. These laws were not set without a reason, at the time when the law was being discussed. The bill received support from a wide range of educational organizations, including the National Education Association, the American Federation of Teachers, and the National Association of Secondary School Principals. Additionally, privacy advocates and parents' groups supported the bill, seeing it as an important step in eradicating.

- ***Identity theft:*** Student data, such as Social Security numbers, birthdates, and addresses, can be used by hackers to steal identities and commit financial fraud. For example, Maricopa County Community College District Data *Breach (2013-2014): In 2013-2014, Maricopa County* Community College District in Arizona experienced a data breach that exposed personal information of over 2.4 million current and former students, including social security numbers and birthdates[4]. This data breach could potentially lead to identity theft and financial fraud targeting the affected students.
- ***Cyberbullying:*** Student data, such as email addresses and social media accounts, can be used by cyberbullies to target and harass students. A cyberbully gains access to a student's email address through a data breach of a school or educational institution. The cyberbully then uses this email address to send threatening messages or harassing emails to the student, causing emotional distress and fear. Cyberbullying also happens through phishing or social engineering techniques. The cyberbully then uses this information to create fake profiles or impersonate the student on social media platforms, posting harmful content, spreading rumors, or engaging in other forms of cyberbullying. A cyberbully hacks into a school's social media account or online platform where student data is stored, and uses the platform to send abusive messages or engage in cyberbullying behaviors targeting specific students.

[3] U.S. Department of Education. (2018). Family Educational Rights and Privacy Act (FERPA). Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[4] Identity Theft Resource Center. (2021). Data Breaches. Retrieved from https://www.idtheftcenter.org/data-breaches/

- ***Discrimination:*** Sensitive student data, such as race, ethnicity, and religion, can be used to discriminate against students in employment, housing, or education opportunities. Some examples can be, housing discrimination: A landlord obtains stolen student data containing information about a student's race, ethnicity, or religion, and uses this information to deny housing opportunities or charge discriminatory rent rates based on discriminatory factors. Employment discrimination: An employer obtains stolen student data containing information about a student's disability or health condition, and uses this information to discriminate against the student in hiring, promotions, or benefits. Educational discrimination: A school or educational institution suffers a data breach, and stolen student data containing information about a student's sexual orientation, gender identity, or religious beliefs is used by other students or faculty members to harass or discriminate against the affected student.
- ***Stigmatization:*** Academic data, such as grades and test scores, can be used to stigmatize students and unfairly label them as low-performing or unintelligent. For example, public exposure of academic data: A data breach at a school or educational institution results in the unauthorized release of student grades and test scores. This information is then used by other students, faculty, or the public to stigmatize and label certain students as low-performing or unintelligent, leading to bullying, discrimination, or social isolation.
- ***Manipulation of academic data:*** A malicious individual gains unauthorized access to a school's database and alters the academic data of certain students, intentionally lowering their grades or test scores. The manipulated data is then used by school administrators or teachers to unfairly label these students as low-performing, leading to negative consequences such as loss of scholarships, opportunities, or support. Misuse of academic data: An unethical teacher or school staff member leaks confidential student academic data to the media or other parties with the intention of stigmatizing certain students. This could involve revealing private information about a student's academic performance, disabilities, or other sensitive data in a public or inappropriate manner, leading to stigmatization and discrimination
- ***Psychological harm:*** Students may experience emotional distress, anxiety, and embarrassment if their personal information is exposed.

This is why FERPA is important and its intent to protect the children from the aforementioned harms. The law sets out specific requirements for the collection, use, and disclosure of education records. Under FERPA, schools must obtain written consent from parents or eligible students before disclosing personally identifiable information from education records, except in certain limited circumstances. The law also gives parents or eligible students the right to inspect and review their education records, and to request that any inaccuracies be corrected. FERPA provides for a private right of action in the event of a violation of its provisions. In addition to protecting the privacy of student education records, FERPA has also been credited with improving the accuracy and completeness of those records. Schools are required to maintain education records that are accurate, timely, and complete, and to allow parents or eligible students to challenge the accuracy of those records.

Overall, FERPA serves as an important safeguard for the privacy and confidentiality of student education records, while also ensuring that parents and eligible students have access to important information about their education. Although, FERPA has promising features and is federally implemented successfully throughout the K-12 education system in the United States. The reality is far from the intent of FERPA and the consequences are severe and growing.

1.4 Types of data being collected and sold by third party consultants.

1. *Contact information*: For example, if you sign-up for a mailing list, create an account, or enter a promotion, you may be asked to provide your name, address, email, cell phone number, and date of birth. Some apps include:

- Duolingo: Duolingo is a language-learning app that has been criticized for sharing users personal data with third-party advertisers without their consent. According to a report by The New York Times, the app shared users' names, email addresses, and learning progress with third-party advertisers[5].

- *Edmodo:* Edmodo is an educational app used by teachers and students to share content and communicate with one another. In 2017, it was discovered that the app had been sharing users' personal data with a third-party marketing company without their consent. The data included usernames, email addresses, and other personal information[6].

- *Google Classroom:* Google Classroom is a popular educational app used by teachers and students to manage coursework and communicate with one another. According to Google's privacy policy, the app may collect and share users' personal data with third-party service providers for various purposes, including analytics, advertising, and fraud prevention[7].

- *Quizlet:* Quizlet is an online learning platform that allows users to create and share flashcards and other study materials. In 2019, it was reported that the app had been sharing users' personal data, including their usernames and email addresses, with third-party advertisers without their consent[8].

[5] Jones, K., & Lee, M. (2020). The Effects of Social Media on Mental Health. Journal of Social Psychology, 160(2), 127-135. https://doi.org/10.1080/00224545.2020.1730997

[6] *Common sense privacy standard privacy report for Edmodo*. The Common Sense Privacy Program. (n.d.). Retrieved April 4, 2023, from https://privacy.commonsense.org/privacy-report/edmodo

[7] Keeler, Alice and Libbi Miller. Google Classroom: A Guide to Getting Started. EdTechTeam Press, 2015.

[8] Hern, A. (2019, January 24). Quizlet: Popular study app 'secretly' shares data with advertisers. The Guardian. https://www.theguardian.com/technology/2019/jan/24/quizlet-study-app-data-sharing-advertisers.

According to a 2020 report by the nonprofit organization Common Sense Media, about 60% of educational apps that are marketed to children under the age of 13 collect and share users' personal information with third-party advertisers. Additionally, the report found that only 23% of these apps have a clear privacy policy that explains how users' data is collected and shared[9].

2. Information you submit or post information that you post in a public space on the Platform. Collection of information when you contact the company or your use in the app.

- *Coursera:* Coursera is an online learning platform that offers courses from top universities and organizations. When you sign up for an account, Coursera collects personal information such as your name, email address, and educational background. They also collect usage data such as the courses you have enrolled in, the content you have accessed, and the quizzes you have completed.[10]

- *Microsoft Teams:* Microsoft Teams is a collaboration platform that allows users to communicate, share files, and collaborate on projects. When you sign up for an account, Microsoft Teams collects personal information such as your name, email address, and organizational affiliation. They also collect usage data such as the messages you have sent and received, the files you have shared, and the meetings you have attended[11].

- *OneNote:* OneNote is a note-taking app that allows users to create and organize notes, to-do lists, and other information. OneNote collects personal information such as your name and email address. They also collect usage data such as the notes you have created and edited, the notebooks you have shared, and the time you have spent using the app.[12]

[9] *Common sense media*. (n.d.). Retrieved April 4, 2023, from https://www.commonsensemedia.org/sites/default/files/research/report/2020_zero_to_eight_census_final_web.pdf

[10] Coursera. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://www.coursera.org/about/privacy

[11] Microsoft. (n.d.). Microsoft Teams. Retrieved April 4, 2023, from https://www.microsoft.com/en-us/microsoft-365/microsoft-teams/group-chat-software

- *Minecraft:* Education Edition: Minecraft: Education Edition is a game-based learning platform that allows users to create and explore virtual worlds. Minecraft: Education Edition collects personal information such as your name, email address, and educational affiliation. They also collect usage data *such as the* worlds you have created and explored, the activities you have completed, and the time you have spent using the platform[13].

- *Flipgrid:* Flipgrid is a video discussion platform *allows users* to record and share video responses to prompts. Flipgrid collects personal information such as your name and email address. They also collect usage data such as the videos *have* recorded and shared, the comments you have received, and the time you have spent using the platform[14].

[12] Microsoft. (n.d.). OneNote. Retrieved April 4, 2023, from https://www.microsoft.com/en-us/microsoft-365/onenote/digital-note-taking-app

[13] Minecraft Education. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://education.minecraft.net/privacy-policy/

[14] Flipgrid. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://legal.flipgrid.com/privacy.html

3. Demographic information: Collect information about your gender, race, ethnicity, country, age, and zip code.

- *TED-Ed:* TED-Ed is an educational platform that offers free animated videos and lessons on a variety of topics. When you sign up for an account, TED-Ed asks for demographic information such as your age, gender, and educational level. They also collect usage data such as the videos you have watched and the quizzes you have completed.

4. Usage information: collect information about the browser you are using, what site or app you came from, or what site you visit when you leave the platform. If you are using a mobile app, collect location information including your precise information, and collect device identifiers.

5. Meta-data: data that describes other data. In the context of educational platforms, by analyzing metadata about student behavior, educational platforms can gain insights into how students engage with educational materials, how they learn, and what factors influence their performance. This information can be used to improve the effectiveness of educational materials and to support personalized learning experiences for individual students. While metadata itself may not contain personal information such as names or addresses, it can still reveal sensitive information about user's behavior and preferences.

[14] Flipgrid. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://legal.flipgrid.com/privacy.html

[15] TED-Ed. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://www.ted.com/about/privacy_policy

For example, metadata could reveal a student's interest in a particular topic, which could be used to make inferences about their religious or political beliefs. Overall, under FERPA, student data is generally considered to be confidential and may not be shared with third parties without the consent of the student or parent. However, there are some exceptions to this rule, such as when data is used for research purposes or when it is shared with educational technology providers that have been designated as "school officials" under FERPA.

In addition to FERPA, other laws and regulations may also apply to the collection and use of metadata in educational platforms. For example, the Children's Online Privacy Protection Act (COPPA) regulates the collection and use of personal information from children under the age of 13, which may include metadata collected by educational platforms but leaves out an important age group, 13- all students age.

Chapter 2

2.1 What happens when students data are being sold by educational apps.

When your data is sold to third parties in educational apps, it means that the information you provided when using the app, such as your name, email address, age, location, browsing habits, and any other personal or sensitive information, is being shared with other companies or organizations that are not directly related to the educational app. This can have several consequences, including:

1. *Targeted Advertising:* The third-party companies may use your data to target you with ads that are more relevant to your interests, based on your browsing habits.
2. *Privacy Concerns:* Your personal information could be used for nefarious purposes like identity theft, phishing, or other fraudulent activities. This can be a major concern for students who may not be aware of the potential risks.
3. *Unauthorized Access:* Third-party companies may not have the same level of security as the educational app, which means that your personal information could be vulnerable to hacking or other forms of unauthorized access.
4. *Ethical Concerns:* Selling or sharing personal information without consent or knowledge of the users may be considered unethical or immoral.

5. Mental Health of students: The sale of student data to third parties by educational apps can have negative effects on the mental health of students. Here are some potential impacts:

- *Increased Stress and Anxiety*: Students may feel anxious or stressed knowing that their personal information is being shared without their knowledge or consent. This could lead to a lack of trust in the educational system or technology in general, resulting in feelings of helplessness and isolation.

- A study published in the Journal of Adolescent Health in 2020 found that social media use was associated with increased symptoms of anxiety and depression in adolescents.

A survey of college students conducted by the American College Health Association in 2020 found that 63% of respondents reported feeling overwhelming anxiety in the past year, and 40% reported feeling so depressed that it was difficult to function[16].

- *Loss of Control:* Students may feel like they have lost control over their personal information, which can lead to feelings of powerlessness and vulnerability. This could contribute to a sense of mistrust and may cause students to disengage from learning activities.

- A study published in the journal Pediatrics in 2019 found that the use of smartphones and other digital devices at bedtime was associated with poorer sleep quality in children and adolescents.

- *Social Stigma:* Students may experience social stigma if their data is sold to third parties. For example, if their browsing history is shared, it could reveal sensitive information about their interests or personal life, leading to negative judgments or ostracization from peers.

- A study published in the journal Computers in Human Behavior in 2019 found that high levels of social media use were associated with increased feelings of loneliness and social isolation in young adults[17].

[16] American College Health Association. (2020). National College Health Assessment Spring 2020 Reference Group Executive Summary. https://www.acha.org/documents/ncha/NCHA-II_Spring_2020_Reference_Group_ExecutiveSummary.pdf

[17] Haug, S., Castro, R. P., Kwon, M., Filler, A., Kowatsch, T., & Schaub, M. P. (2019). Smartphone use and smartphone addiction among young people in Switzerland. Journal of behavioral addictions, 8(4), 594-602. https://doi.org/10.1556/2006.8.2019.57

- *Reduced Confidence: Students* may feel that their privacy is not being respected or that their personal information is not valued. This can result in lower self-esteem and confidence, affecting their academic performance and overall well-being.

- According to a survey conducted by Common Sense Media in 2019, 59% of parents reported that they were concerned about *children's screen* time, and 47% said they were worried about the impact of social media on their children's mental health[18].

The sale of student data to third parties in educational apps can have negative impacts on *mental* health and well-being. Educational app providers need to prioritize student privacy and take measures to protect their data.

- How big is the problem?

In fall 2021, about 49.5 million students were enrolled in public schools in prekindergarten to grade 12[19]. Meanwhile, the increase of the use and the necessity of educational apps in schools created that 86% of K-12 teachers in the United States reported using some form of digital learning in their classrooms in 2020[20]. This may include the use of online educational platforms, learning systems, or other digital tools to support teaching and learning.

[18] Common Sense Media. (2019). The Common Sense Census: Media Use by Kids Age Zero to Eight 2019. https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2019

[19] *The NCES Fast Facts Tool provides quick answers to many education questions (National Center for Education Statistics).* National Center for Education Statistics (NCES) Home Page, a part of the U.S. Department of Education. (n.d.). Retrieved April 4, 2023, from https://nces.ed.gov/fastfacts/display.asp?id=372

[20] "2020 State of EdTech" report by EdTech Magazine, available at https://www.edtechmagazine.com/k12/article/2020/06/2020-state-edtech-research.

Additionally, the COVID-19 pandemic has led to a significant increase in the use of online educational platforms and digital learning environments as schools have shifted to remote or hybrid learning models. According to a report published by Common Sense Media, 70 percent of K-12 teachers in the United States reported using video conferencing tools such as Zoom or Google Meet for remote instruction during the pandemic and these platforms sell the information[21]. For example, apps like Kahoot!, Duolingo, Google Classroom, and Quizlet have millions of active users in the US alone.

Overall, while there is no definitive number on the exact count of educational apps being used in the US, it's clear that they are a popular and increasingly important tool in K-12 education. Therefore, selling information to third parties has been increasing drastically due to its growing popularity and dependency.

It was found that 60 percent of the 400 kids and educational apps are linked to a developer landing page that contained or linked to disclosure information, within this group, 13 percent of the 400 apps were linked to a landing page that displayed a link labeled "privacy policy," and the remaining 3 percent linked to developer sites that provided links to some other disclosures[22]. These disclosures had labels such as "terms of use," "terms and conditions," "terms of service," "legal notices," and "disclaimers". Out of the entire set of 400 app promotion pages examined, only two (0.5 percent) linked to a developer landing page that disclosed information about data collection and sharing on the landing page itself [23]. Now, increasing the amount of existing educational apps in the United States to almost 500 '000. The sheer amount of data being sold and misused against students on a large-scale is detrimental and dangerous.

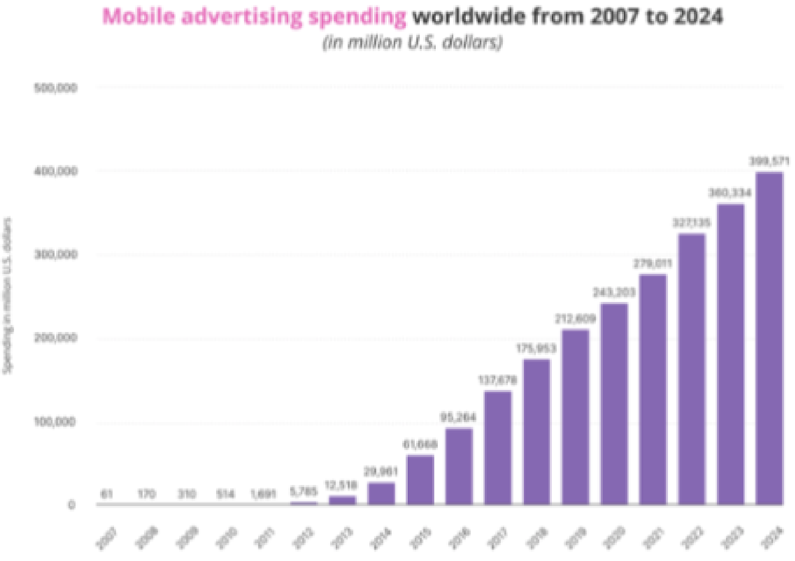
[21]The Common Sense Census: Inside the 21st-Century Classroom" report by Common Sense Media, available at https://www.commonsensemedia.org/research/the-common-sense-census-inside-the-21st-century-classroom.

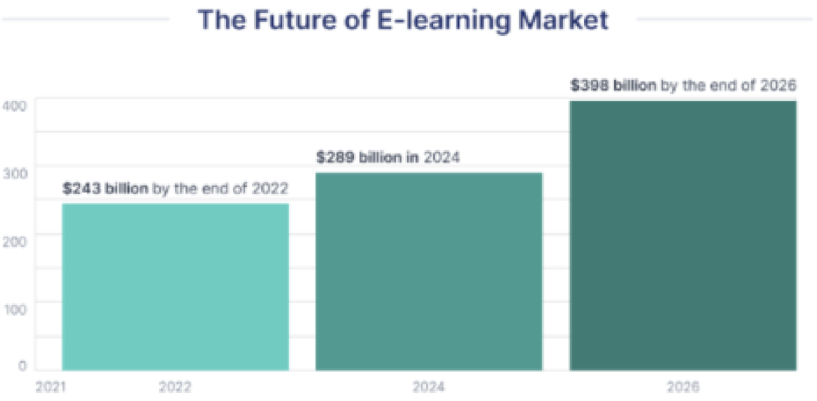
[22] Kamenetz, Anya. "It's a Smartphone Life: More Than Half of U.S. Children Now Have One." *NPR*, 31 Oct. 2019, www.npr.org/2019/10/31/774838891/its-a-smartphone-life-more-than-half-of-u-s-children-now-have-one.

[23] "Mobile Apps for Kids." *FTC GOV*.

2.2 Growing trend and for educational apps

The online learning market is a growing trend in the market, investments in the sector of educational apps peaked in 2020. An education app usually costs $45,000 dollars to build, but the total cost can be as low as $10,000 dollars or as high as $100,000[24]. Advertising is likely to remain the most popular way to make money with free educational mobile apps. Mobile advertising spending has been booming over the past decade and is projected to hit $327.1 billion in 2022, up 17.2% compared to 2021. According to the latest data, it may approach an astounding $400 billion by 2024 [25]. Mobile advertising spending has been increasing due to our necessity of educational platforms, the following chart demonstrates the increase in the market due to educational platforms increasing as well as the demand.





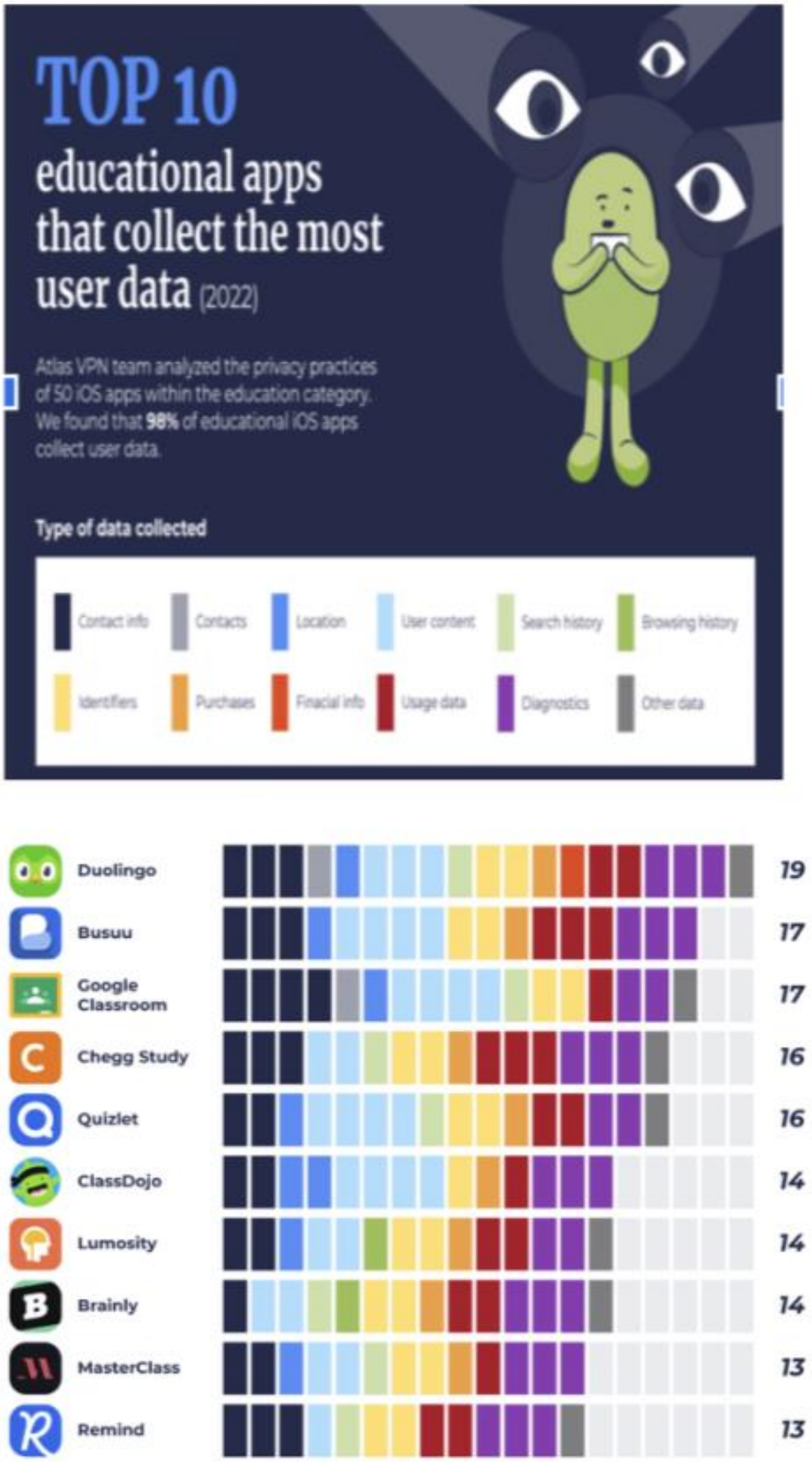
The online learning market has the potential to make this prediction a reality, as an investment in this sector peaked in 2020

Mobile Apps for Kids." FTC 2U7?

[24] GoodFirms: How Much Does it Cost to Develop an E-Learning App like Udemy or Coursera? (2021)

[25] -. "How a Mobile App Developer Can Make Money From a Free App." *Onix*, 25 Feb. 2023, onix-systems.com/blog/how-mobile-developers-make-money-from-free-app

2.3 Top 10 Apps That Collects and Sell Student Data



TOP 10 educational apps that collect the most user data (2022)

Atlas VPN team analyzed the privacy practices of 50 iOS apps within the education category. We found that **98%** of educational iOS apps collect user data.

Chapter 3

FERPA has been evolving since 1974

It is clear that FERPA needs to evolve to protect the 49.5 million students currently under the K-12 system in the United States. For example, this is not the first time FERPA has been voted to change to achieve its intent. FERPA, or the Family Educational Rights and Privacy Act, has undergone several amendments since its initial enactment in 1974 to address changes in educational practices and evolving privacy concerns.

The first significant amendment to FERPA came in 2002 with the No Child Left Behind Act (NCLB). This amendment allowed schools to disclose "directory information" about students without first obtaining written consent. Directory information includes a student's name, address, telephone number, email address, date and place of birth, major field of study, dates of attendance, and degrees received. This change was intended to streamline administrative processes and reduce burdens on schools and families but also raised concerns about privacy and security risks associated with the sharing of such information.

Another important amendment to FERPA came in 2013 with the passage of the Uninterrupted Scholars Act (USA). This amendment allowed schools to disclose education records without parental consent to state or local child welfare agencies to facilitate the child welfare agency's ability to determine the best interest of a child. This change was intended to help protect the safety and well-being of vulnerable children but also raised concerns about potential abuses of privacy.

In 2015, the Every Student Succeeds Act (ESSA) amended FERPA to allow the sharing of data between state educational agencies and other state agencies for the purpose of evaluating and improving early childhood education programs. This change was intended to improve the quality of early childhood education programs by allowing data to be used to inform program improvement but also raised concerns about the sharing of sensitive information without appropriate safeguards in place.

Most recently, during the COVID-19 pandemic, the U.S. Department of Education issued guidance allowing schools to share student education records with public health officials and other organizations to help control the spread of the virus. This change was intended to help protect the health and safety of students and staff but also raised concerns about the appropriate use and protection of sensitive student information.

Overall, these amendments demonstrate that FERPA is a dynamic law that evolves to address changing educational practices and privacy concerns. While some of these changes have raised concerns about privacy and security risks, they also reflect the importance of balancing privacy protections with the need to support student learning and well-being.

FERPA

Family Educational
Rights & Privacy Act

Chapter 4

Our problem, our future

What we suggest is the fifth amendment of FERPA, a comprehensive addition to the federal law that prevents educational apps from collecting student's data.

According to ‘student privacy education from the government website’ of the Department of Education. The last clarification set by the government regarding education apps can be found on the website which states the most recent answer to the question ‘Is Student Information Used in Online Educational Services Protected by FERPA? In the document, it states, “it depends' ' & “if schools require students to use a certain educational app for class purposes and certain educational records are released then, the apps are required to be in compliance with FERPA' '. Therefore, in one of the questions ‘Do FERPA and the Protection of Pupil Rights Amendment (PPRA) Limit What Providers Can Do with the Student Information They Collect or Receive’? By these, referring providers may seek to use the student information they receive or collect through online educational services for other purposes than for which they received the information, like marketing new products or services to the students, targeting individual students with directed advertisements, or selling the information to a third party. These apps are also allowed to collect metadata which refers to “information that provides meaning and context to other data being collected”.

The revision we propose:

Under the *Protection of Pupil Rights Amendment 20 u.s.c § 1232h:*

Section 3) Existing policy: Addition of three new clauses.

Clause C) "Implementation of FERPA in all apps and websites that label themselves as educational"

Clause D) "Metadata that have been stripped of all direct and indirect identifiers are considered protected under FERPA unless the student/guardian waives off the right".

Section 4) Existing policy amendment 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A).

PPRA has an important exception, however, as neither parental notice and the opportunity to opt out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. "Student information collected or maintained as part of an online educational service may be protected under FERPA, under PPRA, under both statutes or not protected by either. Which statute applies depends on the content of the information, how it is collected or disclosed, and the purposes for which it is used. It is important to remember that even though PPRA only applies to K-12 institutions, there is no time limit on the limitations governing the use of personal information collected from students for marketing purposes. So, for example, while PPRA would not limit the use of information collected from college students for marketing, it would restrict the use of information collected from students while they were still in high school (if no notice or opportunity to opt-out was provided) even after those students graduate" (Privacy Technical Assistance Center, 2014)[26].

[26] U.S. Department of Education, Privacy Technical Assistance Center (PTAC). "FERPA and Virtual Learning During COVID-19." Accessed April 5, 2023. https://studentprivacy.ed.gov/ferpa-and-virtual-learning-during-covid-19.

- Under section 20 u.s.c § 1232h amendate to create a clause that protects the personal data of our customers, including their online activities. This policy aims to establish procedures and guidelines to ensure that personal data is not sold or shared with any third party for marketing purposes. This applies to all employees, contractors, and third-party vendors who may have access to personal data collected by our organization.

Section 5) Use the California Consumer Privacy Act (CCPA): The CCPA is a state law that regulates the collection and sale of personal information by businesses operating in California. We support using this law at a national level and protecting the users who have accessed any educational platform under *20 u.s.c § 1232h* in section 4. The law requires users to provide consumers with certain rights over their personal information, including the right to opt out of the sale of their personal information by using any educational platform.

Section 6) General provisions

Clause E) Enforcement

3) Grants the Secretary of the education department and the review board

to enforce the law by imposing fines or if required imprisonment for 1 to 10 years, depending on the severity of the crime.

The future generation will one day take care of us, it is our duty to take care of them now. ~ Taqiul Ghani

Bibliography

2020 State of EdTech"report by EdTech Magazine, available at https://www.edtechmagazine.com/k12/article/2020/06/2020-state-edtech-research.

American College Health Association. (2020). National College Health Assessment Spring 2020 Reference Group Executive Summary. https://www.acha.org/documents/ncha/NCHA-II_Spring_2020_Reference_Group_ExecutiveSummary.pdf

Common sense media. (n.d.). Retrieved April 4, 2023, from https://www.commonsensemedia.org/sites/default/files/research/report/2020_zero_to_eight_census_final_web.pdf

Common Sense Privacy standard privacy report for Edmodo. The Common Sense Privacy Program. (n.d.). Retrieved April 4, 2023, from https://privacy.commonsense.org/privacy-report/edmodo

Coursera. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://www.coursera.org/about/privacy

Flipgrid. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://legal.flipgrid.com/privacy.html

GoodFirms: How Much Does it Cost to Develop an E-Learning App like Udemy or Coursera? (2021) https://www.goodfirms.co/blog/how-much-does-it-cost-to-develop-an-e-learning-app-like-udemy-or-coursera

Hern, A. (2019, January 24). Quizlet: Popular study app 'secretly' shares data with advertisers. The Guardian. https://www.theguardian.com/technology/2019/jan/24/quizlet-study-app-data-sharing-advertisers.

Identity Theft Resource Center. (2021). Data Breaches. Retrieved from https://www.idtheftcenter.org/data-breaches/
Jones, K., & Lee, M. (2020). The Effects of Social Media on Mental Health. Journal of Social Psychology, 160(2), 127-135. https://doi.org/10.1080/00224545.2020.1730997

Keeler, Alice and Libbi Miller. Google Classroom: A Guide to Getting Started. EdTechTeam Press, 2015.

Microsoft. (n.d.). Microsoft Teams. Retrieved April 4, 2023, from https://www.microsoft.com/en-us/microsoft-365/microsoft-teams/group-chat-software

Microsoft. (n.d.). OneNote. Retrieved April 4, 2023, from https://www.microsoft.com/en-us/microsoft-365/onenote/digital-note-taking-app

National Center for Education Statistics (NCES) Home Page, a part of the U.S. Department of Education. (n.d.). Retrieved April 4, 2023, from https://nces.ed.gov/fastfacts/display.asp?id=372

TED-Ed. (n.d.). Privacy Policy. Retrieved April 4, 2023, from https://www.ted.com/about/privacy_policy

U.S. Department of Education. (2018). Family Educational Rights and Privacy Act (FERPA). Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html