Claire Morra
EDUC 6426
Research Paper

Introduction

On May 25, 2022, the Human Rights Watch published a paper about the failure of 49 world governments to protect K-12 student data privacy during the COVID-19 pandemic, when classes were virtual. The privacy issue was caused by the urgency of the pandemic. Parents and students with Internet access and computer hardware were "told or required to use [online learning products] during Covid-19 school closures" (Human Rights Watch, 2022). Governments sought out agreements with educational technology (EdTech) companies that would defray the cost of digital infrastructure, as they traded children's data for free access to EdTech products (Human Rights Watch, 2022).

In the collection process, trackers track the websites students visited outside of the classroom and which apps the students use, as well as tracking contact lists and personal details about contacts. The purpose is to determine how the student might be influenced. The data is then sent to advertising technology (AdTech) companies who put together a profile of the student to predict how they might be influenced into buying products or their viewpoint on certain issues. These third-party AdTech companies sell the data to advertisers and data brokers with an interest in the type of user this profile represents (Human Rights Watch, 2022).

This sale of the private information of minors violates international law outlined by the United Nations Guiding Principles on Business and Human Rights. The HRW makes several recommendations to governments, departments of education, EdTech companies, and AdTech companies, an interdisciplinary approach. Echoed by Reidenberg & Schaub, they write that "privacy safeguards will need to be developed through technological tools, organizational

approaches, and law" (264). Most of the writers researched for this paper agree that an interdisciplinary approach is needed, however this paper will focus on the design of technological tools.

Commercialism in schools goes back to the 1890s and represents marketers taking advantage of the assumption on the part of students that "the adults responsible for them in school have their best interests in mind" (Boninger, Molnar, & Murray, p. 5). Personalization intensified along with, "increased requirements for school data gathering and reporting" (Boninger, Molnar, & Murray, p. 5). For example, a school may send data to a for-profit third-party vendor for legitimate purposed of fulfilling a state requirement. But there is little regulation to stop these vendors from further selling the data once they have legitimately collected it from schools (Boninger, Molnar, & Murray, p. 5).

Partnerships between for-profit brands and schools can take many forms, including sponsoring stadiums, branding clothing, using toys to create educational material, offering incentives for using a brand's product, such as an incentive for walking or running in a certain style of tennis shoe. Educational digital marketing began to emerge in the late 1990s. It began with TV advertisements and grew into Internet marketing through social networks such as Facebook and G-Suite for Education (Boninger, Molnar, & Murray, p. 11). The difference with pandemic learning was that there was no way to opt-out. It was required.

There are some advantages to big data in education, such as the ability to improve learning outcomes by analyzing student generated data on a large scale (Reidenberg & Schaub, 263). Other advantages include the fact that "artificial intelligence has a very long tradition in supporting the learning processes [2] with intelligent assistants or tutors [3], recommending educational materials [4], predicting students' behaviors [5,6], and managing vast amounts of

data [7]" (Garcia-Penalvo, Casado-Lumbreras, Colomo-Palacios, and Yadav, p. 1). The idea of the AI classroom is that the environment can adapt to changes and give "appropriate support in the right places and at the right time based on individual learners' needs, which might be determined via analyzing their learning behaviors, performance, and the online and real-world contexts in which they are situated [12]" (Garcia-Penalvo, Casado-Lumbreras, Colomo-Palacios, and Yadav, p. 2). The authors argue that personalization and collecting data to inform personalization is the method behind the adaptations and support. Personalization is driven not by information that the student reports, but by tracking activity. "The vectors are data structures formed by numerical or categorical variables such as learning style, cognitive level, knowledge type, or the history of the learner's actions in the system, which are computed by artificial intelligence algorithms" Garcia-Penalvo, Casado-Lumbreras, Colomo-Palacios, and Yadav, p. 3).

The cons to personalized digital learning are that tracking student interactions can increase student levels of stress and fear (Reidenberg & Schaub, 264), preventing students from naturally interacting with their virtual environment.

Human Rights Watch studied 164 EdTech products, across 49 countries in their 2022 investigation. These products included website, mobile apps, and products which had both website and mobile app availability. The methods of studying the apps were twofold: "static analysis, which analyzes an app's code and identifies its capabilities, or the functions and instructions that may be executed when the app is run" and also, "dynamic analysis, which runs the app under realistic conditions and observes what data is transmitted where, and to whom" (Human Rights Watch, 2022).

The results were that "EdTech companies that make educational apps for children decide to send a child's personal data to third-party companies and possibly to sell ads in their apps, in

order to generate revenue." AdTech companies put ads in the app, and as soon as the child logins to the educational app, "the app begins to collect personal data about the child. This can include who the child is, where she is, what she does, who she interacts with in her virtual classroom, and what kind of device her parents can afford for her to use" (Human Rights Watch, 2022).

From a human computer interaction design perspective, schools should prohibit the collection of personal student data, they should ban user profiling and behavioral advertising, and stop sharing student data with outside companies for non-educational purposes (Human Rights Watch, 2022).

Prohibit the collection of personal student data

There is so much information available online that personalization arose as an attempt to help people sift through “the flood of information and information overload” (Abu-Dalbouh, p. 75). Personalization is supposed to help people use the Internet by guiding them to websites and products they might be interested in. The problem with this is that issues of privacy have been partly or wholly unaddressed by “personalized web systems” and privacy issues affect “the quality of the existing personalized web” (Abu-Dalbouh, p. 75).

Shneiderman writes that “continuous user-performance data logging”, “may be well intentioned, but users’ rights to privacy deserve to be protected. Links to specific user names should not be collected unless necessary” (166). Not only are these EdTech apps collecting student usernames, but they are also populating profiles based on data logging and selling the information. The motivation for collecting user information is to “target them with ads tailored to their presumed interests and desires” (Human Rights Watch, 2022).

EdTech companies profited off collecting student data. Revenue for EdTech start-ups in 2019 was $7billion and was $16.1billion in 2020 (Human Rights Watch, 2022). “[T]he mass

collection of children's data, exposing their personal information to the risk of misuse and exploitation by the advertising-driven internet economy and resulting in the mass surveillance of children's lives, both inside and outside of the classroom" (Human Rights Watch, 2022). During the pandemic virtual learning period, there were also attacks from hackers, holding "student personal data for ransom" (Molnar et.. al, p. 3).

Schools need to be able to track certain data, such as attendance. That is because schools can lose state funding if they do not track attendance (Molnar et.. al, p. 109). Seven states proposed bills for recording "expectations for performance, attendance, and time in the classroom"; only six passed and were enacted (Molnar et.. al, p. 109). "A few states went so far as to require a "nontraditional" or "remote instructional plan" to include virtual learning in preparing for the 2020-2021 school year if districts wanted to count remote instructional days toward full attendance (enacted: NC SB 704, KY SB 177, NJ A 3904)" (Molnar et.. al, p. 109).

If governments are going to prohibit the collection of student data, then they need funding to purchase EdTech products so that they are not trading student data for free access. One recommendation in Molnar et al, states that governments should "[d]evelop new accountability structures for virtual schools, calculate the revenue needed to support them, and provide adequate funding" (p. 111). The solution needs to be a mixture of law, regulation, funding, and product design.

Ban user profiling and behavioral advertising

Behavioral advertising is targeted and personalized (Varnali, p. 93). Targeted marketing is made possible by tracking users (in this case, students) and creating profiles based on their activity. The data is automatically analyzed by an algorithm, which seeks to predict and to

influence future behavior and interests. Then digital ads are shown to users "based on their previous individual-level online behavior" (Varnali, p. 93). That is behavioral advertising.

The "privacy-personalization paradox (e.g., Chen et al. 2019; Christiansen 2011; Titiriga 2011)" states that as the relevance of personalized ads increases, users must grapple with "the expense of losing control over the use of personal sensitive information (Tucker 2012)" (Varnali, p. 98). As users lose control over information, advertisers increase "ad effectiveness and ad revenues" (Varnali, p. 98). Varnali goes on to state the situation schools found themselves in during the pandemic remote learning period. "In plain words, consumers pay for 'free' content with their personal data" (p. 98). Schools desperately needed EdTech products to facilitate the emergency of remote learning and apparently most of them willingly traded students' privacy.

At Aurora Public Schools, parents were asked to sign a permission slip: ""My contact information or that of my child's, will not be shared with anyone else, nor used for commercial purposes"" (Boninger, Molnar, & Murray, p. 25). This was put in place to allow students to use a badging system called Credly. The agreement is a good first step but falls short of stating how long the information is held by Credly and what Credly might do with the information. The badges this metadata supports are designed to be public and accessible to employers. That is an educational purpose. But there needs to be regulation set forth as to what happens to the badge metadata when the student graduates and no longer has communication with the school.

Badges might be useful to employers and job-seeking students, but the relationship between the school and the for-profit sponsor can lead to the "Corporate Socialization of Children" (Boninger, Molnar, & Murray, p. 25). This can happen with low-tech partnerships, such as branding clothing and high-tech partnerships, such as badges. "When for-profit corporations are involved in schools, irrespective of what the particular surface aspects of a

given relationship may be, the heart of the relationship is mis-educative" (Boninger, Molnar, & Murray, p. 26). The reason being that anything provided to the school in this relationship must benefit the bottom line of the for-profit company. The two missions: educational and corporate, exist with tension and pressure (Boninger, Molnar, & Murray, p. 26).

The tension and pressure raise a moral issue of whether advertising should be allowed in schools. The role of the state in public schools with advertising, further complicates this moral issue. "[W]hen advertising is conducted in schools, the immorality is compounded because the power of the state is twisted to the service of special interests, the ethical standing of educators is compromised, and the orientation of the school is shifted toward mis-educative experiences" (Molnar and Boninger, p. 9).

Researchers Nill and Aalberts (2014) created moral guidelines for behavioral advertising: "(1) free-of-deception, (2) active transparency, (3) control over information, (4) data security, (5) consideration of stakeholder interests, and (6) fairness" (Varnali, p. 99). One roadblock to implementing these guidelines is the role of the consumer and the burden of reading through transparent privacy policies created by companies (Varnali, p. 99). Ideally, if regulations were in place at the federal level, parents and students could trust schools to make the right decisions regarding student privacy.

Stop sharing student data with outside companies for non-educational purposes

A lack of regulation and implemented guidelines leads to the risk of "mis-educative experiences" (Dewey, 1938, as cited in Molnar and Boninger p. 9). This means that advertising in education could lead to stopping or distorting educational growth and represent a fundamental "barrier to freedom" (Molnar and Boninger p. 9). Why would EdTech companies share student data with personalized AdTech companies for non-educational purposes? The goals of web

personalization are "(1) to provide a resource, (2) to solve the impedance information to consumers and information providers, and (3) to provide information services and value-added products" (Abu-Dalbouh, p. 75). Initially, personalization was a reaction to the problem that there was simply too much available on the web: "People need more help to get the right information; namely, the information that is relevant and attractive to them" (Abu-Dalbouh, p. 76). For personalization to work, user data is needed to "understand the user's need" (Abu-Dalbouh, p. 76).

End-users responded to the rise of personalization by expressing that they wanted something in return for their data, such as "free goods or services, or even non-monetary incentives, such as not having to watch ads" and they wanted the ability to opt-out of participating in the data exchange (Abu-Dalbouh, p. 77). However, "[t]he last thing in the world that advertisers want is for a target audience to have self-control" (Molnar and Boninger, p. 9). Children are easy targets for the personalized attack on "self-control and judgement" (Molnar and Boninger, p. 9). They do not enjoy the same faculties and freedoms as adults, and many adults feel taken advantage of, as well. There is a difference between a partnership with Coca-Cola to put soda in schools and required engagement in EdTech products which create a link from K-12, to higher ed, into the job market. "Education, Big Data, and student privacy are a combustible mix" (Reidenberg & Schaub, p. 263).

Big data can lead to insights that produce learning improvements, but "inappropriate uses or disclosures may have [adverse effects] on student learning and social development" (Reidenberg & Schaub, p. 264). It can create fear and stress among the students. Reidenberg & Schaub go on to say that personalization can "curtail opportunities for self-discovery by charting

a path for learners personalized to their predicted aptitude instead of allowing learners to chart their own paths (Schouten, 2017)" (264).

Using this data for non-educational purposes could mean anything, "[s]ome AdTech companies will also follow the child across the internet and over time. Some may search for even more information about her from public and private sources, adding definition and detail to an intimate profile of the child" (Human Rights Watch, 2022). Variables, such as the child's gender are put into algorithms designed to predict future consumer behavior. Human Rights Watch makes the point that buyers of insight data can even include "law enforcement and governments", the very people who should be cracking down on this type of tracking.

Technical safeguards recommended by Reidenberg & Schaub include, "technological measures should provide transparency about data uses, provide accountability for algorithmic decisions, and ensure the security of learners' data" (264). Additionally, there should be clear governmental regulation surrounding the sale of big data from EdTech products to AdTech companies. It is not realistic for students and parents to read through privacy policies each year, even if the goal is transparency.

According to Shneiderman, "[o]ne way to overcome some [issues of privacy] is to build proprietary social software and develop a user base that is genuinely motivated to inhabit that online space" (353-354). I think this suggestion is unrealistic for most public K-12 schools. I also think it would be too unequal based on the resources of the school. The solution really needs to be an understanding that EdTech companies cannot share student data with outside companies for non-educational purposes.

Given the long history over the past 20 years of artificial intelligence used in education, it is not going away. AI in education can "provide specialized support and raise knowledge-gap

awareness" (Chen, Zou, Xie, Cheng, and Lui, p. 28). Recent research has shown that AI in education is able to determine "learner affect and emotion" (Chen, Zou, Xie, Cheng, and Lui, p. 37). For students who only want to communicate with their instructors and classmates, this can be intrusive. Shneiderman writes, "[i]n some cases, users' privacy may be violated because of algorithmic interferences. For instance, by analyzing what users "like" on Facebook, algorithms can be used to predict a range of sensitive personal information like sexual orientation, personality traits, ethnicity, and mental health (Lee, 2014)" (373).

Conclusion

In conclusion, the actions of EdTech companies violating students' privacy are shocking and illegal. It is a violation of UN international law to commodify the private data of minors who are in many cases unaware of the fact that they are being tracked. Students had no alternative during the pandemic-era remote learning period. They were required to use these products and if they did not, they would forfeit crucial learning years at a vulnerable age. Many of the texts reviewed for this paper discuss the need for transparency. I somewhat disagree about the practical applications of sharing privacy policies with users. It would be better if apps did not sell data in the first place and the only way for that to happen is through federal regulation.

Parents should be able to trust the schools they send their children to. Low-income parents might not have other options. Students should feel safe in school. Governments should step in and prohibit the collection of personal student data, ban user profiling and behavioral advertising, and stop sharing student data with outside companies for non-educational purposes.

References

Abu-Dalbouh, Hussain. “Implementing End-User Privacy through Human Computer Interaction for Improving Quality of Personalized Web.” *Computer and information science (Toronto)* 9.1 (2016): 75–. Web.

Boninger, F. Molnar, A., & Murray, K. (2017). Asleep at the Switch: Schoolhouse Commercialism, Student Privacy, and the Failure of Policymaking. Boulder, CO: National Education Policy Center. Retrieved [June 12, 2022] from http://nepc.colorado.edu/publication/schoolhouse-commercialism-2017

Chen, X., Zou, D., Xie, H., Cheng, G., and Lui, C . “Two Decades of Artificial Intelligence in Education: Contributors, Collaborations, Research Topics, Challenges, and Future Directions.” Educational technology & society 25.1 (2022): 28–47. Print.

Garcia-Penalvo, J., Casado-Lumbreras, C., Colomo-Palacios, R., and Yadav, A. “Smart Learning.” Applied sciences 10.19 (2020): 6964–. Web.

Human Rights Watch. (May 25, 2022). *“How Dare They Peep into My Private Life?”* Human Rights Watch. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Molnar, A. and Boninger, F. “The Commercial Transformation of AMERICA’S SCHOOLS.” Phi Delta Kappan 102.2 (2020): 8–13. Web.

Molnar, A. (Ed.), Miron, G., Barbour, M.K., Huerta, L., Shafer, S.R., Rice, J.K., Glover, A., Browning, N., Hagle, S., & Boninger, F. (2021). Virtual schools in the U.S. 2021. Boulder, CO: National Education Policy Center. Retrieved [date] from http://nepc.colorado.edu/publication/virtual-schools-annual-2021

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. Theory and Research in Education, 16(3), 263–279.

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., and Diakopoulos, N. (2017). Designing the User Interface: Strategies for Effective Human-Computer Interaction. 6th ed. Pearson Higher Education.

Varnali, Kaan. “Online Behavioral Advertising: An Integrative Review.” *Journal of Marketing Communications* 27.1 (2021): 93–114. Web.