EdTech: Nurturing Minds or a Tool of Big Brother

Mikayla Howard

Introduction

"Big Brother is watching you."[1] 1984, George Orwell's novel centered around a fictional dystopian world plagued by mass surveillance, has become a literary classic and a hallmark of many high school English curriculums since its publishing in 1949. For many students today, the personification of mass surveillance in 1984 is closer to becoming a reality. Students, especially high school students, are feeling like "Big Brother" is always watching their every move, not only during school hours on school premises but outside of school as well. The rise of school violence, specifically the increase of mass school shootings, coupled with the massive increase in educational technology that sprouted up as a response to the Covid-19 pandemic, has turned educational technology into a booming industry. Educational technology companies have used the pandemic and the fears of parents and school districts to weasel various tracking and surveillance capabilities into their learning tools. Unfortunately for educational technology companies, this hyper surveillance of students is not having the impact that they claim it does. In fact, the hyper surveillance planted in some educational technology is raising some concerns and beginning to negatively impact students. This blog post will serve an introduction to what educational technology is, the issues present with it and the impact it has on students, what is currently being done to combat it, and some ways in which readers can protect themselves from some of the hyper surveillance in these tools.

What is Educational Technology?

If you have ever taken an online class, or, like many of us, had an in-person education experience abruptly transitioned to an online one during the Covid-19, you have had some experience with Educational Technology. Educational Technology, or EdTech as it is referred to in its industry), is the convergence of education and technology that helps to facilitate learning. It is the integration of hardware and software into the classroom that is aimed at enhancing "teacher led learning in classrooms" and improving "students' educational outcomes."[2] EdTech can come in many different forms, both inside the classroom and out. Some common examples include in class tablets, learning management systems such as Canvas or Blackboard, and online conferencing software such as Zoom.[3]

EdTech can also be the implementation of physical and cyber security measures which are aimed at protecting students both online and in person. This is where most of the concern lies. EdTech companies have been marketing technology such as surveillance cameras, environmental sensors, access control systems, alarms, window films, and even vape detectors towards school districts.[4] Artificial Intelligence (AI) is also being implemented in EdTech surveillance in what is being called "next generation surveillance cameras." School districts are beginning to implement surveillance cameras both inside and outdoors that can track an

---

[1] GEORGE ORWELL, 1984, 3 (Penguin Books UK 2008) (1949).
[2] Jake Frankenfield, *What is EdTech? Definition, Example, Pros &Cons*, INVESTOPEDIA (Sept. 28, 2023), https://www.investopedia.com/terms/e/edtech.asp#:~:text=EdTech%20.
[3] *Id.*
[4] Rebecca Torchia, *Safety in Schools: How Physical Security Tech Protects K-12,* EDTECH (Aug. 17, 2023), https://edtechmagazine.com/k12/article/2023/08/safety-schools-how-physical-security-tech-protects-k-12-perfcon.

individual's movement within the school buildings, recognize license plates, and send out alerts when the cameras detect any perceived "threats."[5] Companies such as GoGuradian and Gaggle offer monitoring tools that rely on AI that will go through student's online activities and alert school administrators or even the police to any materials of the students relating to sex, self-harm, or violence.[6] This monitoring is not just happening in the classroom or on school provided technology but is also occurring on personal devices that may have the specific software downloaded on to it without the student's or parent's knowledge.

The EdTech surveillance industry has been successful in their marketing by claiming that their surveillance deters harmful conduct and keeps students safe; all of these claims are unsubstantiated.[7] Despite these unsubstantiated claims, the marketing tactics of these devices are paying off. In 2021, K-12 schools and colleges have spent around $3.1 billion on security products, an increase from $2.7 billion in 2017.[8] Following the expansion of remote learning during the Covid-19 pandemic, the EdTech Company is now an $85 billion dollar industry with no signs of slowing down.[9]

The Issues and Impact of EdTech on Students

EdTech, while seemingly revolutionary to the way that students are educated, raises many concerns. Many of the claims that EdTech companies use in their marketing strategy, such as the fact that EdTech surveillance tools have prevented school shootings or student suicides, have been unfounded and almost entirely established on opinion based evaluations.[10] In fact, a 2023 audit of K-12 schools over the past 20 years revealed that in 8 of the 10 deadliest school shootings, surveillance cameras were present at the schools but did not prevent the shootings; [11] this show that hyper surveillance of students cannot prevent intraschool violence.

Human Rights Watch conducted their own investigation into various EdTech surveillance products. This investigation showed that out of the 163 products they reviewed, 89% (145 products) of them have surveilled, or had the capacity to surveil, students outside of the classroom.[12] Even more startling is the discovery of tracking technologies in many EdTech softwares, with 7.4% of these technologies using session recorders.[13] Session recorders are a type of tracker that documents a user's entire session on the site and makes note of information, such

---

[5] *Id.*
[6] Mark Keierleber, *Exclusive: Dems Urge Federal Action on Student Surveillance Citing Bias Fears*, THE74 (Oct. 19, 2023), https://www.the74million.org/article/exclusive-dems-urge-federal-action-on-student-surveillance-citing-discrimination-fears/.
[7] Chad Marlow, *New ACLU Report Shines Light on Shadowy EdTech Surveillance Industry and the Dangerous Consequences of Surveillance in Schools*, ACLU (Oct. 2, 2023, 9:30 AM), https://www.aclu.org/press-releases/new-aclu-report-shines-light-on-shadowy-edtech-surveillance-industry-and-the-dangerous-consequences-of-surveillance-in-schools.
[8] Id.
[9] Mark Keierleber, *How Ed Tech Tools Track Kids Online — And Why Parents Should Care*, THE74 (Sept. 22, 2023), https://www.the74million.org/article/how-ed-tech-tools-track-kids-online-and-why-parents-should-care/.
[10] Marlow, *supra* note 7.
[11] Marlow, *supra* note 7.
[12] *Online Learning Products Enabled Surveillance of Children*, HUM. RTS. WATCH (July, 12, 2022, 12:01 AM), https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children.
[13] Keierleber, *supra* note 9.

as which links they clicked on, what images they hovered over, and even more terrifying, the data that the user entered into fields but did not submit, including any autofill information.[14]

Another concern surrounding EdTech is found with the software created to track students academically and allow parents/guardians to see the tracked progression.[15] Many school districts are more focused on the educational capabilities and allow data privacy and cyber security concerns to fall by the wayside. Schools are not doing their due diligence in properly vetting the tools they are using and educating themselves on the data privacy terms associated with the systems they are implementing. Instead, schools are opting to trust vendors, who are assuring school districts that they are only sharing and collecting student data to help with the development of better educational software and tools. This is only partially true. Students' data is also shared with partners and other affiliates for non-educational purposes, such as more targeted adverting. [16] There is also a fear that collected data about a student can be collected and shared as the student progresses through his or her academic journey using EdTech software and could be used to negatively predict future academic potential.[17] This ultimately harms students, as this information continues to be used and shared to unknown entities beyond the school district.

A staggering 87% of students in an American Civil Liberties Union (ACLU) survey of students between the ages of 14 and 18 claimed that their school used some form of EdTech surveillance to monitor their behaviors.[18] In a national survey of educators parents and students about school districts use of digital tools to monitor students online by the Center for Democracy and Technology (CDT), two thirds of teachers said that they know of a student who was disciplined as a result of their activity being monitored.[19] A third of teachers said that they know of a student who had been contracted by the police due to an alert generated by monitoring software.[20] More than a third of educators have said that their school monitors students online outside of school hours and occasionally on their personal devices.[21] In the ACLU survey, this number jumps to 40% of teachers knowing that their schools monitor students' personal devices outside of school. [22]

Hyper surveillance through EdTech software has the potential to negatively impact already marginalized groups of students. In fact, this impact is already being felt. LGBTQ+ youth were more likely to report that they or someone they knew were disciplined as a result of monitoring.[23] A third of LGBTQ+ students reported that they or someone they knew were outed due to technology.[24] 18% of students were concerned that school surveillance could be used against immigrant students.[25] One in five students were concerned that this surveillance

---

[14] Keierleber, *supra* note 9.
[15] *Ed Tech Was a Godsend During Pandemic, But It May Have Opened a Pandora's Box of Data Privacy and Security Issues, Says CSUN Prof*, CSUN TODAY (Mar. 7, 2023), https://csunshinetoday.csun.edu/education/ed-tech-was-a-godsend-during-pandemic-but-it-may-have-opened-a-pandoras-box-of-data-privacy-and-security-issues-says-csun-prof/.
[16] *Id.*
[17] Id.
[18] Marlow, *supra* note 7.
[19] Keierleber, *supra* note 6.
[20] Keierleber, *supra* note 6.
[21] Keierleber, *supra* note 6.
[22] Mark Keierleber, *ChatGPT Is Landing Kids in the Principal's Office, Survey Finds,* THE74 (Sept. 20, 2023), https://www.the74million.org/article/chatgpt-is-landing-kids-in-the-principals-office-survey-finds/.
[23] Keierleber, *supra* note 6.
[24] Keierleber, *supra* note 6.
[25] Marlow, *supra* note 7.

technology could be used to identify and potentially punish students who are seeking information on abortions or gender affirming care.[26] Black parents expressed a fear that information from online monitoring tools would fall into the hands of law enforcement and negatively impact their child.[27] Surveillance by EdTech software has the potential to make the school to prison pipeline much more of a reality for black and brown students. It also makes students, especially LGBTQ+ students, less comfortable being their authentic selves, as they no longer have a safe space either in school or out.

What is Being Done and What Can You Do?

Educators', parents', and students' concerns about the privacy issues surrounding EdTech have not fallen on deaf ears. A coalition of House Democrats called on the Education Department to investigate school districts using digital surveillance and other AI tools that would potentially violate students' civil rights. The coalition wrote a letter that discussed concerns over the monitoring and surveillance of students; they emphasized how this negatively impacts already marginalized youth, such as the LGBTQ+, black and brown, immigrant, and students with disabilities.[28] The letter asks for the Education Department's Office for Civil Rights to issue guidance on how to appropriately use the various emerging classroom technologies and tighten the reins on practices that could trample on existing federal anti-discrimination laws. The coalition also urges the Education Department to help educators determine how they "can fulfill their civil rights obligations" while developing appropriate policies relating to EdTech, specifically to AI.[29]

The ACLU recommends working with communities to evaluate the costs and benefits of surveillance tools before implementing them. The ACLU urges schools not to let "fear drive decision-making," to curb some of the fear associated with data privacy surveillance.[30] For educators and school districts, the best thing to do is probably vet the technology that is being brought into the schools. If necessary, have an IT professional help with any due diligence that needs to be done to help protect students. Be aware of the way that students' data is being tracked, stored, and used and if any monitoring happens outside of the school. For parents, do not be afraid to ask questions about the technology that schools are requiring for your child. Advocate for you child and speak up if you feel like the EdTech tools used by your student is intruding out of the classroom. While EdTech has the potential to revolutionize the way students learn, it is important to be cautious of the real word implications that the surveillance aspect of EdTech has on all students, but especially those already marginalized.

---

[26] Marlow, *supra* note 7.
[27] Keierleber, *supra* note 22.
[28] Keierleber, *supra* note 6.
[29] Keierleber, *supra* note 6.
[30] Lexi Lonas, *School surveillance leading to 'digital dystopia' for students, ACLU says*, THE HILL (Oct. 5, 2023, 11:15 AM), https://thehill.com/homenews/education/4240002-school-surveillance-leading-to-digital-dystopia-for-students-aclu-says/.