Media > Ethics > Initiative >

The University of Texas at Austin
Center for Media Engagement
Moody College of Communication

PROMOTING SAFETY OR INFRINGING ON PRIVACY?

THE ETHICS OF ED-TECH SURVEILLANCE IN ONLINE TEACHING

Due to the global COVID-19 pandemic and subsequent need for stay-at-home measures, both K-12 and higher-ed institutions have had to transition to remote learning online. While software like Zoom, a popular video conferencing platform that can host large class sessions and meetings on the web, have been adopted with little pushback, others have been shrouded in controversy. In particular, "thousands of school districts across the United States have installed surveillance software on school-provided devices to monitor their students' online interactions" (Crispin, 2021). Indeed, programs "such as Bark, Gnosis IQ, Gaggle, and Lightspeed can cost the schools tens of thousands of dollars to implement," and are deliberately used to observe student behavior (Crispin, 2021). Some have argued that such surveillance programs are important to protect students and ensure the integrity of their work. Others, however, believe that these advanced educational technologies (ed-tech) are unnecessary and invasive. Since advanced ed-tech software may continue be utilized even after the pandemic wanes, it is crucial to consider its ethical implications.

For many, ed-tech surveillance may be viewed as morally justifiable. In addition to using ed-tech like proctoring apps which are used to prevent cheating on course exams, school districts have argued that "high-profile mass tragedies such as Columbine, Sandy Hook, and Parkland are driving the national conversation and a lot of decision making around school safety and security" (Kshetri, 2021; Herold, 2021). As students move to remote online education where teachers and administrators cannot look out for them like they would during in-person education, ed-tech "can be set up to search for language and online behavior indicating the possibility of violent tendencies, suicidal ideation, drug use, pornography use, or eating disorders" (Crispin, 2021). For example, Gaggle, a large online education surveillance company claimed that their software "helped districts save the lives of more than 700 students who were planning or actually attempting suicide" (Beckett, 2019). Another company, Bark, claimed that their ed-tech was able to "help prevent 16 credible school shootings and detect twenty thousand severe self-harm situations" (Beckett, 2019).

Others worry that privacy concerns render advanced ed-tech morally unjustified. For example, in 2018 the FBI cautioned educational institutions that "the consequences of ed-tech companies collecting too much data on students could result in social engineering, bullying, tracking, identity theft, or other means for targeting children" (Liberman, 2021). Unfortunately, this warning fell on deaf ears and in July 2020 "online proctoring service 'ProctorU' suffered a cyber breach in which the sensitive personal information for 444,000 students

–including their names, email addresses, home addresses, phone numbers, and passwords– was leaked" (Kshetri, 2021). In response to data exploitation incidents like this one, students across the nation "are taking measures [like filing petitions] to force universities to stop the use of invasive software" (Kshetri, 2021). Furthermore, though "more than 80% of teachers say their schools use software to monitor students' online behavior… only one in four said that tracking is limited to school hours" (Anannd, 2021). This activity goes far beyond the duties of teachers and administrators monitoring students for questionable behavior and work integrity.

As ed-tech programs continue to become more advanced, the experiences and challenges of digital education are casting doubt as to whether they can appropriately balance security and privacy. While some argue that "any harm [caused by ed-tech surveillance] pales in comparison to the benefits of what is caught," others believe such a view sets a dangerous precedent (Herold, 2021). Currently, "the United States has no uniform, comprehensive federal privacy law" (Toczauer, n.d), so Timothy Libert –an instructor in Carnegie Mellon University's Computer Science Department– argues "there's a huge gap between how up to date our technology is and how up to date the laws are" (Johnson, 2020). Perhaps developing clear, universal standards surrounding ed-tech surveillance can help mitigate concerns, but until then, where do we draw the line between ensuring student safety and creepily spying on them?

Discussion Questions:

1. What ethical values are in conflict when schools utilize ed-tech to surveil students?
2. Should ed-tech be used to surveil students at all? Why or why not?
3. How should we weigh interests in preventing school shootings or suicides against the privacy concerns of students?
4. What guidelines or standards would you suggest for the use of surveillance technology in remote online education?

Further Information:

Anand, P. (2021, November 3). "The Rise of Education Surveillance." *Bloomberg*. Available at: https://www.bloomberg.com/news/newsletters/2021-11-03/the-rise-of-education-surveillance

Beckett, L. (2019, October 22). "Under Digital Surveillance: How American Schools Spy on Millions of Kids." *The Guardian*. Available at: https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle

Crispin, J. (2021). "American Schools Gave Kids Laptops During the Pandemic. Then They Spied on Them. *The Guardian.* Available at: https://www.theguardian.com/commentisfree/2021/oct/11/us-students-digital-surveillance-schools

Fritchen, K. (2021). "Why Student Data Privacy Is Important Beyond Compliance." *Security Boulevard.* Available at: https://securityboulevard.com/2020/01/why-student-data-privacy-is-important-beyond-compliance/

Herold, B. (2021). “Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming.” *Education Week*. Available at: https://www.edweek.org/leadership/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05

Johnson, T. C. (2020, November 19). “The Cameras Are Always on: Student Surveillance and Privacy Protection in the Age of E-Learning.” *PublicSource*. Available at: https://www.publicsource.org/the-cameras-are-always-on-student-surveillance-and-privacy-protection-in-the-age-of-e-learning/

Kshetri, N. (2021). “Remote Education is Rife with Threats to Student Privacy.” *The Conversation.* Available at: https://theconversation.com/remote-education-is-rife-with-threats-to-student-privacy-148955

Kshetri, N. (2021). “School Surveillance of Students via Laptops May do More Harm than Good.” *The Conversation*. Available at: https://theconversation.com/school-surveillance-of-students-via-laptops-may-do-more-harm-than-good-170983

Liberman, M. (2021). “Massive Shift to Remote Learning Prompts Big Data Privacy Concerns.” *Education Week.* Available at: https://www.edweek.org/technology/massive-shift-to-remote-learning-prompts-big-data-privacy-concerns/2020/03

Toczauer, C. (n.d.). “Privacy and Online Education: Concerns in the Age of Expansion.” *Online Education*. Available at: https://www.onlineeducation.com/features/privacy-concerns-in-the-age-of-online-education

Authors:

Shelby Kelly, Kat Williams, & Scott R. Stroud, Ph.D.
Media Ethics Initiative
Center for Media Engagement
University of Texas at Austin
June 16, 2022

Image: Compare Fibre on Unsplash

This case was supported by funding from the John S. and James L. Knight Foundation. These cases can be used in unmodified PDF form in classroom or educational settings. For use in publications such as textbooks, readers, and other works, please contact the Center for Media Engagement.