CENTER FOR DEMOCRACY & TECHNOLOGY

A SERIES ON STUDENT PRIVACY & DATA ETHICS

SAFETY TECH

Responsible Use of Data and Technology in Education:
School Safety Technology Carries Big Risks for Vulnerable Students

One of the top priorities for schools during the tumultuous past few years has been keeping students and staff safe on campus. In many cases, education officials are turning to technology-driven solutions offered by vendors such as systems that use computer vision to detect guns, automated visitor management systems to try to keep unauthorized people off of school grounds, and systems that try to predict students who may be prone to committing violence.

The most prevalent such technology is student activity monitoring. According to recent CDT research, nearly 90% of teachers report that their school uses software to track what students are doing online.

These technologies are often deployed with good intentions, but their use in education contexts can raise concerns that may ultimately undermine student privacy, diminish trust in schools, and disproportionately impact students from historically marginalized communities.

Here are some of the ways schools can mitigate these harms if they choose to deploy these technologies.

Student Privacy and Equity Considerations and Recommendations

Consent and Responsible Data Practices

Transparency should be accompanied by responsible data practices (e.g. minimizing harm to individuals and supporting the public good) and, where possible, alternative options for those who are not comfortable using or interacting with the technology.

Schools should take steps to only gather necessary data (in accordance with data minimization principles), limit the purposes for which data can be used, and evaluate whether using a system that includes a given feature, such as facial recognition, is necessary, or whether that feature can be disabled. Monitoring devices like thermal cameras and wearables can feel intrusive to students.

Data Management and Transparency

In many cases, companies developing safety technologies are not transparent about their data management practices (e.g., where and how data is stored, for how long it will be retained, and what technical steps the company has taken to secure that data), making it difficult to evaluate the strength of those practices. Deploying a technology without disclosing to stakeholders how their data will be managed or having security procedures in place can threaten student privacy and undermine families' trust in the school's administration.

School authorities should ensure that they and their vendors have adequate security policies and procedures in place and plans for safekeeping data — including retention and deletion procedures. This is especially important for systems with various components (e.g., all-in-one management software), as it can be difficult to understand how data is shared across features. Additionally, schools should disclose to students and their families how information will be managed and safeguarded. Currently, parents are not well briefed on schools' use of certain technologies as they should be; CDT research has found that one in five parents do not know if their school uses student activity monitoring software.

Efficacy

Schools should also make sure that technologies they use are effective. Many AI-driven tools are the subject of misleading promotion, claiming to improve student wellbeing and safety but with little or no proof that they do so. Vendors who assert that gun detection systems reduce crime in schools and ensure a safe environment, for instance, might lack the evidence to support their claims. Similarly, systems not specifically created for schools might not be suitable for that environment. For example, visitor management systems designed to be deployed in work places could fail to recognize children's faces and perform poorly in a school context.

Schools should also request information from vendors about how they designed or adjusted their systems for a school context, and how they validate that their system is effective. If vendors are unable or unwilling to provide the school with evidence of the system's effectiveness, the school should consider dropping the system or finding another vendor.

Disproportionate Impact

Schools should also be attentive to the risk that emerging safety technologies can disproportionately impact different groups of people, especially when nuanced social factors are not captured by technological systems. Examples of disproportionate impact include:

- Tools that aim to predict who may commit a crime may consider factors like being a victim of bullying, but this could disproportionately flag LGBTQ students who face more bullying than their straight, cisgender peers. Indeed, CDT research shows that more LGBTQ+ students say that they or someone they know got in trouble with the teacher or school when the school or district's student activity monitoring saw that the person visited an inappropriate site online or said something inappropriate in a document or message (56% LGBTQ+ vs. 40% non-LGBTQ+);

- Visitor management software, now repurposed for attendance tracking, might flag that some students are a mental health or threat risk due to truancy. Yet students could be missing out on school for a variety of reasons other than mental health; and

- Threat-detection systems that wrongly identify a "threat" and notify security personnel or local law enforcement authorities can result in unwarranted encounters with law enforcement. Such encounters disproportionately affect historically underrepresented groups, like Black and Hispanic students, and can undermine a student's well being and negatively affect their development. Parents appear to be aware of the potential negative impacts of law enforcement involvement in schools, as CDT research found that 58 percent of parents have some level of concern about student data being shared with law enforcement, a concern that is heightened for Black parents over white parents.

Schools should ask vendors how they audit their systems for disproportionate impact, and ask for data about how the system performs across different populations. If the company does not perform such testing, cannot provide the data, or performs differently for different groups, the school should not use that system. Schools should also consider the nuanced social situation of each student, rather than rely solely on the baked-in indicators from vendor tools.

Conclusion

To protect their communities, schools are considering using student safety technologies. Although deployed with the expectation that these tools will safeguard student well being, they can often produce the opposite result by undermining student privacy and equity. Schools should be aware of the potential concerns that AI-driven decision-making systems can raise, evaluate whether employing them is the best option, and know the best practices for successfully using them.

This is one in a series of information sheets designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. Find more of our work at cdt.org/student-privacy.