Technological School Safety Initiatives:
Considerations to Protect All Students

Schools, districts, and states are turning to data and technology to address school safety issues such as shootings, bullying, and self-harm. Despite the growing recognition of poor data quality and limited research on school safety,[1] federal and state policymakers are recommending increased use of technological school safety initiatives to improve school safety.[2]

The tech-based school safety initiatives that are being discussed include integrating students' education data with other types of personal information; expanding data access to more entities, especially law enforcement; surveilling social media and email; providing law enforcement with real-time access to school video cameras; deploying facial recognition; creating databases that track behavior threat assessments and are accessible by multiple stakeholders; and promoting anonymous reporting tools.

However, these initiatives have the potential to harm the students they are intended to protect.

Considerations to Protect All Students

As decision-makers are turning to data and technology to try to make schools and students safer, there are important considerations that should inform policymaker and practitioner decisions:

- **Efficacy and accuracy**: Most technological school safety initiatives are unproven,[3] have known technical limitations,[4] are difficult to audit, and almost certainly produce false positives[5] that could subject students to unnecessary scrutiny and interactions with law enforcement.

- **Invasiveness and chilling effects**: Overbroad surveillance, mandatory threat reporting, and law enforcement access to expansive data create serious risks to students' privacy, free expression, and ability to learn. Excessive monitoring can chill students' speech, associations, movements, and access to important resources, and can transform a school from a learning environment to one of surveillance that actually makes students feel less safe.[6]

- **Discriminatory outcomes**: Increased monitoring and use of algorithmic risk assessments are likely to disproportionately affect students of color and other underrepresented or underserved groups, such as immigrant families, students with previous disciplinary issues or interactions with the criminal justice system, and students with disabilities.[7]

- **Cost and resource management**: Schools have limited resources and lack expertise to evaluate school security technologies,[8] so they should not over-rely on a particular technology or data system, particularly with a dearth of evidence that technological school safety initiatives make schools safer.

- **Governance mechanisms**: New technologies and data systems will not be effective, and may increase school safety risks, if they are introduced without clear policies, informed by parental and community engagement, for how these systems will be used and governed.[9]

Actions for Education Leaders and Policymakers

Education leaders and policymakers should consider students' rights to privacy, free expression, and equal opportunity before rushing to implement potentially dangerous technologies or collecting and sharing sensitive data, starting with the following actions:

- **Start with a more inclusive definition of "safety":** Although school shootings are devastating, they are far from the only safety concerns that students face. In particular, students of color have experienced disproportionate negative impacts from overbroad policing and surveillance in schools.[10] If school safety initiatives are not designed with a holistic and inclusive definition of safety in mind, they may be counterproductive and actually endanger the most vulnerable students.
- **Ground school safety in what schools are positioned to address**: Schools are being asked to do more than ever to predict and respond to safety concerns. In particular, schools are facing increased pressure to monitor and respond to off-campus activities, such as what students are saying on social media when they get home. Placing unreasonable burdens on schools to monitor students can detract from their educational mission.[11]
- **Balance urgency to act with acknowledgement of a lack of evidence about what works**: Schools and districts should look for solutions that have a proven track record of improving school safety and students' wellbeing. Many of the current trends in data and technology for school safety are experimental. While appropriately tailored and thoughtful data collection can be part of a holistic program to help address students' needs, more data is not necessarily better.[12]
- **Inform policymaking by parents and students from all impacted communities**: Policymaking around school safety should center the input and needs of students and their families, but students and parents are not a monolith. Policymakers and education officials should affirmatively reach out to and engage underrepresented communities, particularly students and families of color and immigrant students,[13] who have been disproportionately impacted by disciplinary, policing, and surveillance policies in schools.[14]
- **Engage CIOs and CPOs in school safety technological initiatives**: Chief information officers (CIOs) and chief privacy officers[15] (CPOs) can be valuable resources for assessing the values, limitations, and risks of new technology and data initiatives, but they are often not involved early enough in the process of procuring new technologies or drafting school safety recommendations. Privacy and technical advice from CIOs and CPOs should be integrated into every step of adopting and implementing new data and technology initiatives and making school safety recommendations.
- **Have a plan for how to use and manage new technologies and data systems**: Too often, institutions invest in new technology or data systems first, and figure out how to use and govern them later. The problem to be solved should dictate the type of data collected and who can access it—not the other way around. To realize the benefits of data and technology while protecting students' rights, data governance policies should include privacy and security protections, purpose limitations, data minimization, access controls, retention limits, and data deletion procedures.[16]

Conclusion

States, districts, and schools are under immense pressure to adopt new security measures, but rushing this process could hurt students without measurably contributing to school safety. Many technological initiatives that have been proposed or implemented are unproven and come with significant risks to students' privacy, free expression, and safety. Before ramping up data collection and digital surveillance in schools, decision-makers should consider the real effects and unintended consequences of these measures on students and families, and take steps to mitigate them.

◻◻◻◻◻ *Endnotes*

1. Anya Kamenetz, "The School Shootings That Weren't," *NPR*, August 27, 2018, https://www.npr.org/sections/ed/2018/08/27/640323347/the-school-shootings-that-werent.
2. U.S. Departments of Education, Justice, Homeland Security, and Health and Human Services, *Final Report of the Federal Commission on School Safety*, December 18, 2018, https://www2.ed.gov/documents/school-safety/school-safety-report.pdf; *Marjory Stoneman Douglas High School Public Safety Commission Initial Report*, January 2, 2019, http://www.fdle.state.fl.us/MSDHS/Commission Report.pdf.
3. Drew Harwell, "Parkland school turns to experimental surveillance software that can flag students as threats," *Washington Post*, February 13, 2019, https://www.washingtonpost.com/technology/2019/02/13/parkland-school-turns-experimental-surveillance-software-that-can-flag-students-threats/?utm_term=.8493b6c9ea35.
4. Natasha Duarte, Emma Llanso, and Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis,* Center for Democracy and Technology, November 28, 2017, https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/.
5. Aaron Leibowitz, "Could Monitoring Students on Social Media Stop the Next School Shooting?" *New York Times*, September 6, 2018, https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.
6. Melinda D. Anderson, "When School Feels Like Prison," *Atlantic*, September 12, 2016, https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556/.
7. Hope Ford, "Proposed school safety bill could create student profiles based on risk factors," *Alive*, February 11, 2019, https://www.11alive.com/article/news/proposed-school-safety-bill-could-create-student-profiles-based-on-risk-factors/85-e982ec3f-7e9a-481a-99d3-b8d3f21052de.
8. *Final Report of the Federal Commission on School Safety*.
9. Benjamin Herold, "Facial-Recognition Systems Pitched as School-Safety Solutions, Raising Alarms," *Education Week*, July 18, 2018, https://www.edweek.org/ew/articles/2018/07/18/facial-recognition-systems-pitched-as-school-safety-solutions-ra.html.
10. Advancement Project and the Alliance for Educational Justice, *We Came to Learn: A Call to Action for Police-Free Schools*, https://advancementproject.org/wecametolearn/.
11. Jon Schuppe, "Schools are spending billions on high-tech security. But are students any safer?" NBC News, May 20, 2018, https://www.nbcnews.com/news/us-news/schools-are-spending-billions-high-tech-security-are-students-any-n875611.
12. John Woodrow Cox and Steven Rich, "Armored school doors, bulletproof whiteboards and secret snipers," *Washington Post*, November 13, 2018, https://www.washingtonpost.com/graphics/2018/local/school-shootings-and-campus-safety-industry/?utm_term=.3023eeacd473.
13. Hanna Dreier, "He Drew His School Mascot – and ICE Labeled Him a Gang Member," *ProPublica*, December 27, 2018, https://features.propublica.org/ms-13-immigrant-students/huntington-school-deportations-ice-honduras/.
14. Nora Gordon, *Disproportionality in student discipline: Connecting policy to research*, Brookings, January 18, 2018, https://www.brookings.edu/research/disproportionality-in-student-discipline-connecting-policy-to-research/.
15. Elizabeth Laird, *Chief Privacy Officers: Who They Are and Why Education Leaders Need Them*, January 30, 2019, https://cdt.org/insight/chief-privacy-officers-who-they-are-and-why-education-leaders-need-them/.
16. Justine Brown, "School Safety: A Shared Responsibility," *Government Technology*, October 30, 2015, https://www.govtech.com/em/safety/School-Safety-A-Shared-Responsibility.html.