



1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 | fpf.org

FPF Testimony Before the Federal Commission on School Safety

On behalf of the Future of Privacy Forum, thank you to the Federal Commission on Student Safety for allowing me to testify today. My name is Amelia Vance, and I am FPF's Director of Education Privacy. Among other initiatives, I run a monthly student privacy working group for districts and state privacy staffers representing 45 states. In my previous role at the National Association of State Boards of Education, I wrote a report on school surveillance, privacy, and equity proposing a framework for schools seeking to ensure student safety while also protecting their privacy.

I am here today to ask that any Commission recommendations include appropriate privacy "guardrails" around school safety measures to ensure that student privacy and equity are protected.

Parents trust schools with their children, and we want schools to act to ensure student safety. In order for that to happen, schools must engage in some forms of surveillance. This includes everything from ensuring preschoolers do not wander off, to keeping third graders on task, as well as preventing or identifying instances of bullying or potential violence.

These responsibilities are not new, but, as technology has evolved, schools have an increased ability to monitor students continually, both in and out of the classroom. Schools are using services such as social media monitoring, digital video surveillance linked to law enforcement, and visitor management systems to help protect their students. These can be effective tools; however, they can also harm students if there are not appropriate measures in place to regulate and guide their use.

Many recent state school safety proposals include surveillance as a tactic to reduce or prevent future school violence. For example, Florida's new law creates a database combining data from social media, law enforcement, and social services agencies.

The school safety plan from Texas proposes combining local, state, and federal resources to scan and analyze not only public student social media posts, but also "private or direct messages" and "Information exchanged in private chat groups [or] via text message." To be clear, we are talking about the government actively seeking out children's social media accounts, both public and private, and combining this information with existing law enforcement or social services records to profile which students are threats.

Individual districts and states can and should set their own policies of whether and how to monitor students and protect school safety. However, privacy guardrails

must be drawn so parents and students can be reassured that their rights will be protected.

The negative effects of surveillance should be considered as well. Research shows that surveillance can undermine a student's sense of safety, creating a prison-like environment where students feel big brother is always watching. Students are still maturing and need to know schools are safe spaces where they can ask questions, think creatively, and make mistakes. Increased surveillance can also create a "permanent record" that can limit a student's future opportunities.

These effects can be mitigated by adopting privacy protections, such as those laid out in the Fair Information Practice Principles or my report. Any surveillance that is undertaken should have policies about what data is collected, why it is collected and how the data will be used.

However, privacy should never get in the way of preventing school violence. In the wake of the Virginia Tech shooting, the Family Educational Rights and Privacy Act (FERPA) was amended to clarify when information can be shared during a health or safety emergency. However, that is not enough; districts have shared that they need more guidance on when they are able to report potential safety threats, and not enough teachers are aware of what FERPA allows. The Department of Education's Privacy Technical Assistance Center has been vital for schools seeking practical guidance on FERPA. The Commission should recommend that PTAC publish guidance and provide more technical assistance on this issue.

Schools across America are looking to this Commission's recommendations to guide their decisions around safety and surveillance. The Commission should recommend that programs or proposals to collect and analyze additional student data should be targeted at the most serious threats to school safety. If applied broadly to less serious violations of school rules, the programs could overwhelm school administrators with data, cast suspicion on students who show no signs of violent behavior, and fail to promptly identify individuals who pose genuine threats to school safety. The Commission should also urge schools to be transparent about their data-driven safety initiatives. Trust is a crucial pillar of school communities. Student opportunities should not be limited, either by school safety concerns or by violations of their privacy. Thank you.

Amelia Vance, Director of the Future of Privacy Forum's Education Privacy Project