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

U.S. Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

July 23, 2019

Dear Chairman Johnson, Ranking Member Peters, and Members of the Senate Homeland, Security & Governmental Affairs Committee,

As the Senate Homeland, Security and Governmental Affairs Committee holds a hearing on July 25th regarding "Examining State and Federal Recommendations for Enhancing School Safety Against Targeted Violence," the Future of Privacy Forum (FPF) writes to highlight key privacy issues regarding school safety initiatives and to offer our expertise on how to best address them:

- Students deserve safety measures that are evidence-based. Decisions about threats should be made by, among others, school administrators, counselors, and educators who understand students' particular needs and circumstances. Non-evidence based protocols are more likely to trigger false alarms, fail to identify actual threats, and increase the workload on already overburdened administrators—administrators who could otherwise be doing things that actually make schools safer. And there is a model on how to do this: Utah's 2019 school safety law found ways to bake-in evidence-based policies and privacy guardrails without hindering school safety.
- Increased surveillance and data sharing without clear justification frequently overwhelms administrators with information, undermines effective learning environments, increases inequities, and can fail to promptly identify individuals who may pose genuine threats to school safety. In particular, overbroad school surveillance programs can place important data-driven school initiatives at risk: data collected to help ensure students are treated equitably under the Every Student Succeeds Act, for example, should not be repurposed in the name of school safety to harm or stigmatize those students.
- Finally, even when policies are evidence-based and don't repurpose sensitive data in ways that break trust, without sufficient privacy and equity guardrails, certain information collected for school surveillance purposes will disadvantage particular minority groups. School safety policies must be created in an evidence-based way that avoids creating a disparate impact on vulnerable communities.

We invite the committee to seek answers about how privacy and equity guardrails are or are not being incorporated into state and local school safety initiatives. Prior to implementing school safety programs, officials ought to 1) seek out and analyze the best-available evidence to inform policy; 2) perform privacy impact assessments, commonly-used and established processes for ensuring the appropriate balance between the benefits and risks of data collection and use initiatives, particularly as they related to already vulnerable communities; and 3) transparently engage with all stakeholders, including parents, students, and educators.

FPF is a nonprofit organization focused on finding solutions to consumer privacy questions that lack clear legal or ethical answers. FPF's core view is that data-driven efforts can improve educational outcomes and that privacy requirements should enhance, rather than undermine, student safety. FPF has a substantial portfolio of work on the intersection of privacy and education. We regularly analyze policy proposals and provide guidance to policymakers; convene leading stakeholders, including districts, states, companies, and advocacy groups, to exchange knowledge and best practices regarding emerging privacy issues; and lead privacy boot camps to help key stakeholders understand the regulatory requirements and industry best practices around proper handling of student data. We have testified on student privacy before the House

Education and Workforce Committee and the Federal Commission on School Safety, and were invited to present at the U.S. Department of Education and the Federal Trade Commission workshop on student privacy and educational technology.[i]

We share the concerns of students, parents, educators, lawmakers, and others who want nothing more than to fulfill students' right to be safe and flourish in school. New monitoring tools, however, threaten student safety in unexpected ways. As technology has evolved, schools are increasingly able to monitor students continually, both in and out of the classroom. Schools use services such as visitor management systems, digital video surveillance linked to law enforcement, and social media monitoring to help protect their students. These tools can be effective, but they can also harm students without appropriate measures to regulate and guide their use. These harms include creating a culture of pervasive surveillance that compromises learning, subjecting students to unproven safety strategies that criminalize normal behavior, exacerbating implicit bias and the school-to-prison pipeline, and using flawed evidence and protected statuses to label students as threats.

**Evidence-Based Strategies Are Crucial**
First and foremost, students deserve safety measures that are evidence-based. FPF has been closely tracking school safety bills and policies introduced in 2018-2019 that are largely reactive. Driven by fear and a desire to do *something* to keep kids safe, many are hastily put together, rather than methodically and systematically developed with evidence and efficacy front of mind. Not only are many of these proposals not evidence based, but some even run contrary to long-standing and replicated research. Rather than support school safety, non-evidence based protocols like these are more likely to trigger false alarms, fail to identify actual threats, and increase the workload on already overburdened administrators—administrators who could otherwise be doing things that have been actually proven to keep schools safe.

For example, Florida's 2018 Marjory Stoneman Douglas High School Public Safety Act[ii] mandated the creation of a database combining data from social media, law enforcement, and social service agencies. *Education Week* recently detailed the types of information to be collected in the database, including flagging children who have been victims of bullying based on protected statuses such as race, religion, disability, and sexual orientation, as well as children who have been homeless or in foster care. This database, scheduled to go online on August 1, will combine highly sensitive information in one state-level data system without a clear, evidence-based rationale for collecting such data.[iii] As a result, the system will effectively use protected statuses to flag children as potential threats. As our organization wrote in a letter to Florida Governor DeSantis,[iv] children who have been victims of bullying or whose only "risk" factor is a disability should not be included in a database intended to identify threats. Moreover, parents cannot know which information about their children are included in the database, because the law states that anyone whose data is part of the system must obtain that data from the original agencies that provided it.

Other states and districts are adopting surveillance technologies that, unfortunately, have not been shown to be effective. In New York, Bill No. A04484 would require that schools, in consultation with law enforcement, install "security cameras supported by artificial intelligence" as appropriate, without clarifying what is meant by AI or providing privacy protections for the data to be collected.[v] Many districts are spending school safety grant money to adopt technologies like social media monitoring, despite little evidence to suggest that it keeps students safer. [vi] It would be far better to create lasting and effective school safety measures that come from the careful consideration of evidence-based safety goals, strategies, and their potential consequences.[vii]

Worse, privacy impact assessments and privacy guardrails—like deletion requirements to ensure an appropriate balance between privacy safeguards and security risks—have been generally absent from such policies. But that doesn't have to be the case. In fact, there exists at least one state model for how to codify privacy protections into law from Utah.

Utah has been a leader in school safety and student privacy, in part by recognizing that privacy is a key part of safety. With four full-time staff devoted to student privacy work at the state education agency and robust student privacy laws, Utah had already established a privacy guardrails process when state lawmakers created their school safety bill—a bill that found ways to bake-in evidence-based policies and training throughout, without hindering school safety in any way.[viii] The bill, signed into law in late March

2019, references evidence-based policies seven times, ranging from the need to create model policies for school districts on “evidence-based procedures for the assessment of and intervention with individuals whose behavior poses a threat to school safety” and “evidence-based approaches in identifying an individual who may be showing signs or symptoms of mental illness,” to conducting and disseminating evidence-based research on school safety concerns and effective school safety initiatives. The bill also pairs training for school administrators and school resource officers, among others, with these requirements to make sure that all personnel conduct school safety initiatives with evidence in mind.

**Risks of Increased Surveillance, Data Sharing, and Data Repurposing**

When schools increase surveillance in an effort to enhance safety, they can paradoxically undermine safety. The National Association of School Psychologists reports[ix] that school surveillance can corrode learning environments by instilling an implicit sense that children are untrustworthy. Many organizations have noted that surveillance technologies such as social media monitoring[x] and facial recognition[xi] can harm students by stifling their creativity, individual growth, and speech. The sense that “Big Brother” is always watching can destroy the feelings of safety and support that students need to take intellectual and creative risks—to do the hard work of learning and growing.

Beyond potentially harming student learning, overbroad school surveillance programs can put important data-driven school initiatives at risk. Schools collect sensitive data about students for many laudable purposes—purposes like enhancing educational outcomes, ensuring all students are treated equitably, and providing mental health services and accommodations to improve learning. This data collection, some of which is mandated by the Every Student Succeeds Act, is vital for schools, parents, and policymakers to understand whether or not they are serving different students well. Hastily created school surveillance programs that seek to use this same data in ways that could harm or stigmatize students breaks down often hard-earned trust between parents, schools, and governmental entities. Students who may be considering self-harm or violent acts can be disincentivized from seeking help if they fear that seeking help means their data could be later used to label them a threat.

This is especially important when the data being repurposed is extremely sensitive data, such as disability status, religion, or sexual orientation. Using this data for school surveillance programs disincentivizes individuals from getting help when they need it, ultimately undermining keeping *all* students safe and ensuring educational supports for any child that needs them. Schools collect sensitive data about students to enhance educational outcomes, such as fulfilling individualized education programs (IEPs); to ensure that all students are treated equitably regardless of race, gender, religion, and sexual orientation; to reduce bullying; to provide mental health services and accommodations, and more. When data originally intended to ensure that schools serve all children equitably is repurposed in way that could harm or stigmatize them, the state has broken the public’s trust in school and government institutions.

If evidence-based school safety measures include physical or digital monitoring, it must be developed transparently, in consultation with experts and community stakeholders, and focus on real threats. In addition, students deserve schools where decisions about threats are made by school administrators, counselors, and educators—human beings who can account for students’ particular needs—not by algorithms. And when a student is identified as a threat, they and their families deserve access to the information used to make that decision, as well as an opportunity to dispute it.

Moreover, when schools use surveillance tools in classrooms and hallways, students deserve clear policies on which data is collected, who has access to it, how it will be used, and when it will be destroyed. Students deserve assurances that their data will not be misused and that data collection and storage will comply with relevant privacy laws.

In sum, increased surveillance and data sharing without clear justification frequently overwhelms administrators with information, undermines effective learning environments, casts suspicion on already marginalized students who show no signs of violent behavior, tends to criminalize normal behavior and increase inequities, and can fail to promptly identify individuals who may pose genuine threats to school safety. Repurposing data initially collected to help students and ensure equitable treatment and learning for students can break the trust between students, parents, and schools. Students, parents, and educators all deserve transparency about data-driven safety initiatives. Trust is a crucial pillar of school communities.

Students' opportunities should not be limited, either by school safety concerns or by violations of their privacy.

### Avoiding Disparate Impacts on Vulnerable Communities is Crucial

Finally, even when policies are evidence-based and don't repurpose sensitive data in ways that break trust, without sufficient privacy and equity guardrails, collecting certain information for school surveillance purposes disadvantages certain minority groups. For example, there is a common misconception that people who are mentally ill are more likely to commit violence, even though, when researchers controlled for other risk factors, they found people with mental health issues no more likely to be violent than anyone else.[xii]

And while no evidence demonstrates that creating a massive digital surveillance infrastructure helps to prevent school violence, studies do suggest that such an apparatus may harm the most vulnerable students—the opposite of its intended effect. [xiii] Without privacy safeguards and protections, policymakers may risk building a structure that systematically discriminates against students.

Studies have also shown that surveillance is linked to more frequent student interactions with the criminal justice system. When schools increase surveillance, they tend to escalate minor offenses, leading to arrests and court trials, in effect criminalizing normal adolescent behavior. [xiv] Studies also show that school surveillance can disproportionately target students with disabilities[xv] and students of color,[xvi] thereby aggravating implicit bias and the school-to-prison pipeline. What's more is that law enforcement may be unaware of teen slang or common practices in a particular cultural context, causing them to misunderstand certain words and erroneously assume that a particular student is a threat. Understanding the cultural context and possessing the knowledge that comes from the trusted relationships school administrators and educators have with their students is key to preventing such misunderstandings.

School safety policies must be developed in an evidence-based way that avoids creating a disparate impact on vulnerable communities. Utah's 2019 school safety law, described above, was built upon the importance of evidence-based best practices and policies, and is a shining example of how to mitigate discrimination.[xvii] Training, another important and laudable aspect of the Utah law, can also go a long way toward preventing unintentional harm to vulnerable communities. Utah's law includes:

- Training for school resource officers and principals, developed by the Utah state education agency, on topics such as student privacy rights; working with disabled students; techniques to de-escalate and resolve conflict; cultural awareness; restorative justice practices; negative consequences associated with youth involvement in the juvenile and criminal justice systems; and strategies to reduce juvenile involvement in the justice system;
- Additional training, created by the state education agency, on evidence-based approaches to improving school climate and addressing bullying behavior; evidence-based approaches to identifying individuals who may pose a threat to the school community; evidence-based approaches to identifying individuals showing signs of mental illness; and what the laws permit regarding data collection and disclosure to law enforcement and other support services.

Of course, policies and laws are only as strong as the people implementing them. Acknowledging this, Utah's school safety law also includes technical support for local education agencies to develop and implement school safety initiatives. All states should seek to mitigate harm to vulnerable communities by following Utah's example. Utah's legislature also respected the fact that each school district is different and may require different kinds of support; rather than mandating particular policies or creating a state-wide database of sensitive student information, Utah opted to give districts the flexibility to choose how to best protect the students in their communities—the students they know and understand better than any policymaker does.

### An Important Federal Role

The primary federal student privacy law, the Family Educational Rights and Privacy Act (FERPA), also provides effective protections for students. The law was originally enacted by Congress in 1974, and amended over the years in an effort to strike the right balance between supporting the benefits of collecting and using student data for children and schools while also mitigating privacy risks.[xviii]

FERPA is designed to protect student privacy and student safety, not foil appropriate law enforcement investigations or endanger school communities. Thus, the law also includes effective provisions for using and sharing students' personal data in response to a legal process, as well as during health or safety emergencies. For example, the FERPA statute permits disclosure of students' personal information in response to a subpoena, or "in connection with an emergency ... to protect the health or safety of the student or other persons." This exception provides a well-balanced approach: if a school believes it must disclose information to prevent an imminent threat, the Department of Education has said through regulation and in guidance that the school's judgment will not be second-guessed. However, as made apparent by the Marjory Stoneman Douglas High School Public Safety Commission report[xix] and our discussions with schools and districts, many school administrators, educators, school resource officers, and law enforcement officials do not sufficiently understand these provisions. More training, as Utah's law requires, would increase appropriate data sharing and use.

Specifically, the Department of Education's Privacy Technical Assistance Center (PTAC) has been a vital resource for schools seeking practical guidance on FERPA. Congress could allocate funding to PTAC to provide more guidance, more training sessions, and more technical assistance on this issue. In particular, guidance that includes case studies and examples of when schools can and cannot use FERPA's exceptions to report potential threats would help districts better understand how to balance school safety and privacy issues. Congress could also provide grants to regional educational entities or districts to develop model training materials. Doing so would help all education stakeholders better understand the fact that school safety and student privacy can not only coexist, but are integral to each other and should not stand in each other's way.

**Conclusion**

In the current climate of public fear, many student safety initiatives have focused narrowly on targeted and random acts of school violence. Yet, many educators know that school safety is about more than preventing shootings. It also encompasses issues such as hallway behavior, monitoring visitors, technology use, anti-bullying programs, and ensuring that schools avoid discriminatory practices. It includes equity, mental health, and student well-being. Protecting student privacy is integral to these goals.

For these reasons, we invite the committee to examine the extent to which local school safety initiatives incorporate privacy and equity guardrails. We recommend that prior to implementing school safety programs, officials engage in evidence-based policymaking to seek out and analyze efficacy-based solutions; perform a privacy impact assessment, which is the most common way that government and corporate entities appropriately balance the benefits and risks of data-use initiatives; and transparently engage with all stakeholders, including parents, students, and educators—the people on the ground, whose lives stand to be affected by these policies day in and day out.

Individual districts and states can and should set their own policies on whether and how to monitor students and ensure school safety. However, they must draw privacy guardrails in order to ensure that the rights of parents and students will be protected. FPF recommends that the committee examine the *Principles for School Safety, Privacy, and Equity*,[xx] a list of ten principles designed to protect student rights to privacy, dignity, and an equitable education, which we signed along with 40 other diverse organizations.

Lastly, students, parents, and educators all deserve transparency. We urge the committee to require state and local entities be transparent about their data-driven safety initiatives. Trust is a crucial pillar of school communities. Students' opportunities should not be limited, either by school safety concerns or by violations of their privacy.

We appreciate your important work on student privacy. Please feel free to contact us before or after the hearing if we can assist you in any way or answer questions about school safety and student privacy.

Sincerely,

Amelia Vance

Director of Education Privacy

Future of Privacy Forum

[i] Amelia Vance, Hearing on "Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe" Before the House Education and Workforce Committee, (May 17, 2018) https://republicans-edlabor.house.gov/uploadedfiles/testimony_vance_5.17.18.pdf; John Verdi, Statement Before the Federal Commission on School Safety U.S. Department of Health and Human Services, (July 11, 2018) https://fpf.org/wp-content/uploads/2018/07/Statement-of-John-Verdi-School-Safety.pdf.

[ii] Marjory Stoneman Douglas High School Public Safety Act, https://www.flsenate.gov/Session/Bill/2018/07026

[iii] Benjamin Herold, *Florida Plan for a Huge Database to Stop School Shootings Hits Delays, Legal Questions*, Education Week, May 30, 2019, https://www.edweek.org/ew/articles/2019/05/30/florida-plan-for-a-huge-database-to.html.

[iv] *33 Organizations Send Letter to Florida Governor DeSantis*, July 9, 2019, https://ferpasherpa.org/letterdesantis.

[v] New York State Assembly Bill A04484, 2019, https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A04484&term=2019&Summary=Y&Actions=Y&Text=Y.

[vi] Faiza Patel, Rachel Levinson-Waldman, Jun Lei Lee, Sophia DenUyl, *School Surveillance Zone*, Brennan Center for Justice, April 30, 2019, https://www.brennancenter.org/analysis/school-surveillance-zone.

[vii] Examples of reports examining the efficacy of school safety technologies: National Criminal Justice Technology Research, Test & Evaluation Center, *A Comprehensive Report on School Safety Technology*, Johns Hopkins University Applied Physics Laboratory in cooperation with The Johns Hopkins University School of Education Division of Public Safety Leadership, October 2016, https://www.ncjrs.gov/pdffiles1/nij/grants/250274.pdf; Heather L. Schwartz, Rajeev Ramchand, Dionne Barnes-Proby, Sean Grant, Brian A. Jackson, Kristin J. Leuschner, Mauri Matsuda, Jessica Saunders, The Role of Technology in Improving K–12 School Safety, RAND Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1488.html.

[viii] Utah Code 53g-8-801 (2019) https://le.utah.gov/~2019/bills/static/HB0120.html#53g-8-801. [HB 120, 2019]

[ix] National Association of School Psychologists, School Security Measures and their Impact on Students, (2018) https://www.nasponline.org/Documents/Research%20and%20Policy/Research%20Center/School_Security_Measures_Impact.pdf

[x] Faiza Patel and Rachel Levinson-Waldman, *Monitoring kids' social media accounts won't prevent the next school shooting*, The Washington Post, March 5, 2018, https://www.washingtonpost.com/news/posteverything/wp/2018/03/05/monitoring-kids-social-media-accounts-wont-prevent-the-next-school-shooting.

[xi] Stefanie Coyle and John Curr III, New York School District Seeks Facial Recognition Cameras for Public Schools, ACLU, June 20, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/new-york-school-district-seeks-facial-recognition.

[xii] Autistic Self Advocacy Network, Make Real Change On Gun Violence: Stop Scapegoating People With Mental Health Disabilities, accessed July 23, 2019, https://autisticadvocacy.org/policy/briefs/gunviolence.

[xiii] National Association of School Psychologists, *School Security Measures and Their Impact on Students*, 2018,https://www.nasponline.org/Documents/Research%20and%20Policy/Research%20Center/School_Security_Measures_Impact.pdf; Jason P. Nance, *Student Surveillance, Racial Inequalities, and Implicit Racial Bias*, 66 Emory Law Journal 765 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830885.

[xiv] Amada Ripley, *How America Outlawed Adolescence, The Atlantic* (November 2016) https://www.theatlantic.com/magazine/archive/2016/11/how-america-outlawed-adolescence/501149/.

[xv] Azza Altiraifi and Valerie Novack, Efforts to Address Gun Violence Should Not Include Increased Surveillance, Center for American Progress, February 20, 2019, https://www.americanprogress.org/issues/disability/news/2019/02/20/466468/efforts-address-gun-violence-not-include-increased-surveillance.

[xvi] Melinda D. Anderson, *When School Feels Like Prison*, September 12, 2016, https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556.

[xvii] Utah Code 53g-8-801 (2019) https://le.utah.gov/~2019/bills/static/HB0120.html#53g-8-801. [HB 120, 2019]

[xviii] 20 U.S.C. § 1232g; 34 CFR Part 99.

[xix] Marjory Stoneman Douglas High School Public Safety Commission, Initial Report, January 2, 2019, http://www.fdle.state.fl.us/MSDHS/CommissionReport.pdf.

[xx] *Principles for School Safety, Privacy, and Equity*, March 29, 2019, https://ferpasherpa.org/schoolsafetyprinciples.