Statement of John Verdi
Before the Federal Commission on School Safety
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
July 11, 2018

I. Introduction

Thank you for the opportunity to testify today. My name is John Verdi, and I am VP of Policy at the Future of Privacy Forum (FPF). FPF thanks the Commission Chairs for convening today's meeting, and for working to make students and schools safer. This is a vital mission.

FPF is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. We are optimists about data. We believe that the power of information technology is a net benefit to society, and that it can be well-managed to control risks and offer the best protections and empowerment to consumers and individuals.

FPF has a substantial portfolio of work regarding the intersection of privacy and education. We analyze policy proposals and provide guidance to policymakers. We routinely convene leading stakeholders – including leaders from the corporate, public sector, and non-profit communities – to exchange best practices and knowledge regarding emerging privacy issues. We lead privacy bootcamps to help key stakeholders understand the regulatory requirements and industry best practices regarding proper handling of student educational data. We co-founded (with the Software & Information Industry Association) the Student Privacy Pledge, a self-regulatory framework that safeguards student privacy regarding the collection, maintenance, and use of student personal information. More than 300 leading education technology companies have signed the pledge.

FPF's core view is that data-driven efforts have the potential to improve educational outcomes, and that privacy requirements should enhance, rather than undermine, students' safety. Today, my testimony focuses on:

- defining privacy risks that can arise when personal information is collected, used, or shared;
- discussing how the use of children's data can present unique or heightened risks;
- identifying existing legal authorities, particularly portions of the 2008 FERPA regulations, that permit appropriate data sharing in response to health and safety risks while maintaining meaningful privacy safeguards; and
- recommending that the Commission explore opportunities to: 1) better educate stakeholders regarding existing legal authorities that permit data sharing; and 2) engage in additional fact-finding concerning the risks at issue in this important discussion – the development of additional empirical evidence regarding privacy risks and safety risks is crucial to promoting better understanding and better policies.

II. Data Collection, Use, and Sharing Practices can Create Privacy Risks; Common Sense Privacy Rules are Necessary to Mitigate the Harms that can Arise from these Risks

Schools have long used students' personal information to improve learning outcomes, better manage classrooms, and help ensure the health and safety of teachers and children. As digital technologies have become more integral to economic and social life in the United States, schools have implemented data-driven programs that can make education more personalized, effective, and efficient. Teachers, administrators, and companies work tirelessly to develop and improve educational resources and student outcomes. Many of these resources rely on students' personal data. Parents recognize the potential benefits of data-driven initiatives and information sharing.[1] At the same time, parents and children worry that personal information can be collected, used, and shared in inappropriate ways that can cause real harm to students and families.[2]

It should come as no surprise that parents, students, and schools want meaningful privacy safeguards to protect student data.[3] Judges, lawmakers, and citizens have long recognized the benefits – and countervailing privacy risks – associated with emerging technologies.[4] Abundant data, inexpensive processing power, and sophisticated analytical techniques can drive innovation and economic growth in our increasingly networked society. Data plays a crucial role in educating, employing, and entertaining Americans. Researchers use medical data to identify public health issues and cure diseases. Data helps government agencies respond to natural

---

[1] *See* Amelia Vance, *New Survey Finds Parents Support School Tech and Data, But Want Privacy Assurances*, FUTURE OF PRIVACY FORUM (Dec. 8, 2016), https://fpf.org/2016/12/08/2016-parent-survey/.
[2] *Id.*
[3] *Id.*
[4] *See, e.g.*, Carpenter v. United States, 585 U.S. ___ (2018); United States v. Jones, 565 U.S. 400, 428 (2012); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798; Privacy Act of 1974, 5 U.S.C. § 552a.

disasters and protect public safety. However, the benefits of connected technologies and data analysis are not risk-free. Americans value privacy and expect protection from intrusions by both private and governmental actors. Strong privacy protections are also necessary to sustain the trust that supports data-driven initiatives; without trust, individuals rush to freeze data use and sharing – even when it facilitates crucial services.[5]

Privacy protections are typically implemented in response to a demonstrated harm, a perceived future risk, or a combination of both. For example, the Driver's Privacy Protection Act (DPPA)[6] was passed after the California DMV's data disclosure practices contributed to the stalking and murder of actress Rebecca Schaeffer,[7] the Children's Online Privacy Protection Act (COPPA) was enacted after a reporter posed as a notorious child killer while purchasing personal dossiers regarding 5,000 children,[8] and the Family Educational Rights and Privacy Act (FERPA) was passed after sponsors heard stories about racial slurs in student records that parents were not allowed to see, and inappropriate data sharing between schools and other parties.[9] Recent state student privacy laws focused on preventing future risks; one privacy advocate argued that

---

[5] Alia E. Dastagir, *Equifax Data Breach: I Tried to Freeze My Credit. There Were Problems,* USA Today (Sept. 13, 2017), https://www.usatoday.com/story/money/2017/09/13/equifax-data-breach-tried-freeze-my-credit-there-were-problems/663014001.

[6] 18 U.S.C. §§ 2721–2725 (2006).

[7] David G. Savage, *Privacy of Driver's License Data Upheld*, L.A. Times (Jan. 13, 2000), http://articles.latimes.com/2000/jan/13/news/mn-53647.

[8] *Largest Database Marketing Firm Sends Phone Numbers, Addresses of 5,000 Families with Kids to TV Reporter Using Name of Child Killer*, Electronic Privacy Info. Ctr. (May 13, 1996), https://www.epic.org/privacy/kids/KCBS_News.html.

[9] *Family Educational Rights and Privacy Act (FERPA)*, Electronic Privacy Info. Ctr., https://epic.org/privacy/student/ferpa (last visited July 6, 2018) ("[I]n a speech explaining the Act to the Legislative Conference of Parents and Teachers, Senator Buckley said FERPA was adopted in response to 'the growing evidence of the abuse of student records across the nation.'"); Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 Drexel Law Review 339 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2821837.

"[c]ompanies with rich student dossiers could market aptitude and attitude profiles to college admissions or corporate recruiting offices."[10]

The legislative, regulatory, academic, and popular record is replete with discussion and debate regarding privacy risks.[11] Several frameworks can be used to identify and mitigate privacy harms.[12] I find it helpful to organize privacy risks into five categories, including risk of:

- Physical harms;
- Financial harms;
- Loss of Liberty;
- Loss of Opportunity; and
- Social Detriment.[13]

These categories of privacy risks manifest in a range of circumstances. Privacy risks leading to physical harms can arise from inappropriate disclosure of public or private sector data, disproportionately impacting at-risk populations, including stalking victims, domestic violence survivors, the elderly, and the young. Privacy risks can result in widespread financial harm;

---

[10] Stephanie Simon, *Data Mining Your Children*, Politico (May 15, 2014), https://www.politico.com/story/2014/05/data-mining-your-children-106676?o=2.

[11] Lauren Smith, *Unfairness By Algorithm: Distilling the Harms of Automated Decision-Making*, Future of Privacy Forum (Dec. 11, 2017), https://fpf.org/2017/12/11/unfairness-by-algorithm-distilling-the-harms-of-automated-decision-making.

[12] See, *e.g.,* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1202–03 (1998); Christopher Wolf, *A Practicing Privacy Lawyer's Perspective on Use Analysis as a Way to Measure and Mitigate Harm*, 12 Colo. Tech. L.J. 353 (2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C.L. Rev. 93 (2014); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006); Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman & Ellen Nadeau, An Introduction to Privacy Engineering and Risk Management in Federal Systems, NISTR Publication 8062 (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[13] Future of Privacy Forum, Unfairness By Algorithm: Distilling the Harms of Automated Decision-making (Dec. 2017), https://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf.

millions of consumers file complaints each year with the Federal Trade Commission (FTC) alleging that they are victims of identity theft or financial fraud.[14] Inaccurate data can pose risks to individuals' liberty, with incorrect data in government databases leading to wrongful detention, search, arrest, and incarceration.[15] When used to make decisions regarding employment, insurance, housing, and admission to schools, illegal or unfair data practices can result in loss of opportunity for individuals or groups.[16] Similarly, unfair data use can result in dignitary harms, including emotional distress and reinforcement of stereotypes.[17]

These privacy harms can result from a range of factors, including: unlawful data collection; inappropriate use and sharing of personal information; unaccountable data practices; failure to provide individuals with appropriate redress; and unreasonable security measures.[18] They can occur even with the best of intentions and when undertaken to support the most laudable educational purposes.[19]

Regardless of the taxonomy one employs or the precise characterization of a particular harm one prefers, the privacy risks and harms noted above are widely recognized.[20] And the

---

[14] Press Release, FTC, FTC Releases Annual Summary of Complaints Reported by Consumers (Mar. 1, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers.
[15] Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 Minn. L. Rev. 541, 559–562 (2016).
[16] Elana Zeide, *The Limits of Education Purpose Limitations*, 71 University of Miami L. Rev. 2 (2017)
[17] Future of Privacy Forum, *supra* note 11.
[18] *See* Center for Democracy & Technology, Comment Letter on Informational Injury Workshop P175413, FTC (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00027-141555.pdf.
[19] Elana Zeide, *The Limits of Education Purpose Limitations*, 71 University of Miami L. Rev. 2 (2017).
[20] *See, e.g., Informational Injury Workshop*, FTC, https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop (last visited Jul.6, 2018) (featuring discussion of the nature of privacy risks and harms by government officials, advocates, industry, and academics); *Pubic Comments on FTC Announcement for Workshop on Informational Injury*,

appropriate response is likewise well understood: establishment of appropriate privacy safeguards that support the benefits of data while mitigating the risks arising from collection, use, and sharing of sensitive personal information. Congress and state legislatures pass laws in attempts to mitigate privacy risks; more than 120 state laws specifically targeting student privacy have passed since 2013.[21] Private litigants and government enforcement agencies bring actions to redress privacy harms.[22] Companies and other stakeholders establish self-regulatory frameworks to build trust between individuals and entities who collect and use personal data.[23] Government agencies develop standards and programs to ensure accountability and transparency. Most efforts are based on the Fair Information Practice Principles (FIPPs), flexible standards that have guided data protection efforts for decades.[24] Contemporary articulations of the FIPPs call for privacy

---

FTC, https://www.ftc.gov/policy/public-comments/2017/10/initiative-721 (last visited Jul.6, 2018); Consumers Union, Comment Letter on Informational Injury Workshop P175413, FTC (Jan. 26 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00039-142816.pdf (citing with approval Acting FTC Chairman Maureen Ohlhausen's characterization of privacy harms as "deception injury or subverting consumer choice, financial injury, health or safety injury, unwarranted intrusion injury, and reputational injury"); Consumer Technology Association, Comment Letter on Informational Injury Workshop P175413, FTC (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00011-141540.pdf (identifying privacy harms as "[s]ubverting consumer choice; [f]inancial injury, such as direct financial loss; [h]ealth and/or safety injury; [u]nwarranted intrusion; and [r]eputational injury"); Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 52 J. Econ. Literature 1, 6 (2016), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf ("[P]rivacy trade-offs often mix the tangible (the discount I will receive from the merchant; the increase in premium I will pay to the insurer), with the intangible (the psychological discomfort I experience when something very personal is exposed without my consent), and the nearly incommensurable (the effect on society of surveillance; the loss of autonomy we endure when others know so much about us.)").

[21] State Student Privacy Laws 2013-2017, FERPA|Sherpa, https://ferpasherpa.org/state-laws/.

[22] *E.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).

[23] *E.g.*, Student Privacy Pledge, https://studentprivacypledge.org (last visited July 6, 2018).

[24] *E.g.*, *U.S. Department of Education Safeguarding Student Privacy*, U.S. Dept. of Educ. (2011), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/safeguarding-student-privacy.pdf; Shannon Dahn, *Fair Information Practice Principles (FIPPS)*, Homeland Security (June 12,

protections that promote transparency, user control, respect for context, security, access and accuracy, focused collection, and accountability. These principles form the essential backbone of privacy protections in the United States, and should be carefully considered when weighing changes to the privacy rules that govern student data.[25]

III. Data Practices Regarding Children and Students can Create Unique or Heightened Privacy Risks

The privacy risks discussed above pose particular challenges when they arise in the context of children's or students' personal information.[26] Physical harm and loss of liberty are especially egregious when the victim is a child. Financial fraud and identity theft increasingly target young Americans, who are often unable to discover or combat the crimes until years later.[27] Worse,

---

2014) https://www.dhs.gov/publication/fair-information-practice-principles-fipps; *Executive Orders 13636 and 13691: Privacy and Civil Liberties Assessment Report*, U.S. Dept of Homeland Sec. Privacy Office & the Office for Civil Rights and Civil Liberties at 8 (Jan. 26, 2018) https://www.dhs.gov/sites/default/files/publications/2017%20EO%2013636_13691%20Section%205%20Report_Signed%20012618_Final.pdf; *Federal Health IT Stragetic Plan 2015-2020*, U.S. Dept of Health and Hum. Serv. at 39 (2015), https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf; *Internet of Things: Privacy & Secuirty in a Connected World*, FTC (January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; *Records, Computers, and the Rights of Citizens*, U.S. Dept of Health and Hum. Serv. (July 1, 1973), https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

[25] Elana Zeide, Student Data Privacy: Going Beyond Compliance, NASBE.

[26] Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs* 8 Drexel L. Rev. 339 (2016); The Limits of Education Purpose Limitations, 71 University of Miami Law Review, 2 (2017); The Proverbial Permanent Record; Education Technology and Student Privacy, Elana Zeide, Education Technology and Student Privacy, 70–84 (Evan Selinger, Jules Polonetsky, & Omer Tene eds., 2018) The Cambridge Handbook of Consumer Privacy; Unpacking Student Privacy, 327-335, Handbook of Learning Analytics, Society for Learning Analytics Research (SoLAR).

[27] *Child Identity Theft*, FTC (Aug. 2012), https://www.consumer.ftc.gov/articles/0040-child-identity-theft. *See also*, Beth A. Steele, *FBI Tech Tuesday: Building a Digital Defense Against Child ID Theft*, FBI (Feb. 22, 2018), https://www.fbi.gov/contact-us/field-

children are susceptible to specialized schemes – including medical identity theft – that can create substantial health risks when multiples individuals' medical records are merged as a result of the crime.[28] In recognition of the heightened risks to children, COPPA provides privacy protections for children that exceed adult safeguards, and FERPA grants enhanced protections to students and their parents.

FERPA's statutory and regulatory protections provide parents and students with the opportunity to access education records, correct inaccurate or inappropriate information, and prevent disclosure of education records in a range of circumstances. Congress enacted these protections in the wake of citizen complaints – complaints that schools were depriving parents of access to basic education records while filling records with inappropriate, inaccurate data and disclosing students' personal information to unauthorized third parties unaffiliated with the school, the student, or their parents.[29] Congress enacted these provisions, and amended them over the years, in an effort to strike the right balance – supporting the benefits of student data for children and schools while mitigating privacy risks to vulnerable students.[30] FERPA covers student "personally identifiable information" maintained in schools' "educational records." In

---

offices/portland/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-against-child-id-theft.

[28] Herb Weisbaum, *Millions of Children Exposed to ID Theft Through Anthem Breach*, NBC Universal (Feb. 18, 2015), https://www.nbcnews.com/better/money/millions-children-exposed-id-theft-through-anthem-breach-n308116; Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Report (Aug. 25, 2016), https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/.

[29] Electronic Privacy Info. Ctr., *supra* note 9.

[30] Dalia Topelson Ritvo, *Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies*, Cyberlaw Clinic Berkman Center for Internet & Society at Harvard University, June 2016.

many cases, FERPA, not HIPAA, governs handling of student health records, including mental health records.[31]

IV. FERPA Provides Schools with Appropriate Authority to Share Data to Protect Health and Safety; Additional Education and Guidance May Promote Greater Understanding of Existing Tools

FERPA is designed to protect student privacy and student safety, not foil appropriate law enforcement investigations or endanger schools. The law includes provisions that permit disclosure of student records in response to legal process, as well as in circumstances involving health and safety emergencies.[32] It has been amended over the years to ensure the law is sufficiently flexible in cases of emergency and physical threat.

The FERPA statute and regulations promulgated by the Department of Education include a range of provisions that permit schools to use and share data to promote students' health and safety.[33] For example, the FERPA statute permits disclosure of students' personal information in response to a subpoena.[34] However, the most likely way that information in this context would be shared as allowed under a FERPA exception that permits disclosure "in connection with an emergency … to protect the health or safety of the student or other persons."[35]

---

[31] *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records,* U.S. Dept of Health & Hum. Ser. and U.S. Dept of Ed (November 2008) https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

[32] Lynn Daggett, *Sharing Student Information With Police: Balancing Student Rights with School Safety,* ABA (2012) https://www.americanbar.org/content/dam/aba/events/state_local_government/2012/10/2012_fall_councilmeeting/Daggett_Paper.authcheckdam.pdf.

[33] *See* 20 U.S.C. § 1232g.

[34] Mia Little & Amelia Vance, *Law Enforcement Access to Student Records: What is the Law?*, Future of Privacy Forum (Sept. 25, 2017) https://fpf.org/2017/09/25/law-enforcement-access-to-student-records/.

[35] 20 U.S.C. § 1232g(b)(1).

In 2008, the Department amended FERPA regulations "to remove the language requiring strict construction of this [health and safety] exception and add a provision stating that if an educational agency or institution determines that there is an articulable and significant threat to the health or safety of a student or other individual, it may disclose the information to any person, including parents, whose knowledge of the information is necessary to protect the health or safety of the student or other individuals."[36] This amendment was designed to address concerns articulated in the wake of the April 2007 shootings at the Virginia Polytechnic Institute and State University. The Department provided additional guidance. The FERPA regulation:

> makes clear that educational agencies and institutions may disclose information from education records to appropriate parties … if there is a significant and articulable threat to the health or safety of a student or other individual, considering the totality of the circumstances.[37]

Indeed, the Department assured school officials:

> if, considering the information available at the time of the determination, there is a rational basis for the determination, the Department will not substitute its judgment for that of the educational agency or institution in evaluating the circumstances and making the determination.[38]

The key legal aspects of the 2008 amendments are the adoption of the "totality of the circumstances" test and the "rational basis" approach to Department review of school officials' decisions. The "totality of the circumstances" test authorizes disclosure of protected student information when the totality of the circumstances suggest that disclosure would mitigate a health or safety threat; this test broadened schools' authority, replacing the previous "strict construction" standard, which suggested that disclosure was only authorized when strictly

---

[36] Family Educational Rights and Privacy, 73 Fed. Reg. 74,806 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99).
[37] Raymond Simon, *Dear Colleague Letter about Family Educational Rights and Privacy Act (FERPA) Final Regulations*, U.S. Dept. of Educ. (Dec. 17, 2008), https://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht12-17-08.html.
[38] *Id*.

necessary to preserve health and safety. The "rational basis" approach assures districts that the Department does not second-guess disclosure decisions from a perspective of perfect hindsight; instead, the Department will view assertion of the health and safety exception as appropriate if the district identifies an articulable threat that serves as the rational basis for the disclosure.

These amendments substantially broadened school officials' legal and practical ability to share student information in response to emergent health and safety threats. At the same time, they retain some protections for students: the amendments prohibit disclosure of personal information in the absence of an articulable threat or based on determinations that lack any rational basis.

Some have urged further expansion of the disclosure exemption, which could grant schools authority that is unconstrained by the requirements that officials identify an articulable threat and base determinations on a rational basis. However, such expansion would likely have negative consequences for both privacy and safety.[39] While schools should be able to set their own policies for ensuring school safety, privacy guardrails must be drawn so parents and students can be reassured that their rights will be protected.[40] Untethered expansion of schools' authority could also further complicate administrators' decisions to share or withhold student records from other government agencies.[41]

---

[39] Elana Zeide, *The Proverbial Permanent Record* (October 9, 2014). https://ssrn.com/abstract=2507326 or http://dx.doi.org/10.2139/ssrn.2507326.

[40] Amelia Vance, *Ensuring School Safety While Also Protecting Privacy: FPF Testimony Before the Federal Commission on School Safety* (June 6, 2018), https://fpf.org/2018/06/06/ensuring-school-safety-while-also-protecting-privacy-fpf-testimony-before-the-federal-commission-on-school-safety/.

[41] Amelia Vance and Sarah Williamson, *Law Enforcement Access to Student Recoreds*, Future of Privacy Forum (Sep. 2017) https://fpf.org/wp-content/uploads/2017/09/Law-Enforcement-Access-to-Data-Final.pdf.

Untethering disclosure authority from the "totality of the circumstances" and "rational basis" tests would necessarily increase privacy risks to students. And a dramatic broadening of authority could increase sharing of student information in a way that overwhelms administrators with data, casts suspicion on students who show no signs of violent behavior, and fails to promptly identify individuals who pose genuine threats to school safety. For example, mentally ill students can be disincentivized from seeking help if they fear that their privacy will not be protected; their worries include stigma and reduced access to academic opportunities.[42]

The National Association for School Psychologists reports that school surveillance can corrode learning environments by instilling an implicit sense that children are untrustworthy, and has also been linked to increased future criminality.[43] With increased surveillance, minor offenses can be escalated, leading to arrests and court trials, in effective criminalizing normal adolescent behavior.[44]

---

[42] Megan M. Davoren, Comment, *Communication as a Prevention to Tragedy: Ferpa in a Society of School Violence,* 1St. Louis U. J. Health L. & Pol'y 425 (2008) (citing Judge David Bazelon Center For Mental Health Law, Supporting Students: A Model Policy for Colleges and Universities) ("Because students struggling with mental health problems must be able to receive care, amendments to privacy law must avoid any breaches of privacy that might create disincentives for these students to pursue the help they need. Students with mental illness already face many disincentives: they fear being stigmatized; they fear their peers will retaliate against them; they fear that by receiving help they will no longer be able to obtain licensure in certain professions. Often colleges and universities are at a loss on how to best help the student and resort to punitive actions, such as requiring them to leave university housing or charging them with disciplinary violations for suicidal gestures or thoughts. These actions create more disincentives for students to seek help, isolating them from counselors and teachers and, in turn, increasing the risk of harm.")

[43] Research on School Security, The Impact of Security Measures on Students, *National Association of School Psychologists,* (2014) http://www.audioenhancement.com/wp-content/uploads/2014/06/school-security-by-NASP.pdf

[44] Amanda Ripley, "How America Outlawed Adolescence," *Atlantic,* November 2016. https://www.theatlantic.com/magazine/archive/2016/11/how-america-outlawed-adolescence/50114; *State Student Privacy Laws*, FERPA SHERPA (June 21, 2018) https://ferpasherpa.org/state-laws.

Paradoxically, when schools increase surveillance in an effort to enhance safety, students' sense of safety can be undermined - leading to a perception that big brother is always watching.[45] Without clear pathways for how surveillance data will be shared with schools, families and law enforcement, data collection can also put students at risk for abuse within their homes. Studies of messaging to parents have found that, for parents already prone to aggressive and abusive behavior, messages from schools increase the likelihood of domestic violence, and the anxiety over this messaging negatively impacts students' performance.[46]

Rather than expand legal bases for disclosure of student data, the Commission should recommend additional initiatives to educate school officials and other stakeholders regarding the existing legal authorities for sharing data to support school safety. Misinterpretation of FERPA provisions has resulted in officials' failure to share information in circumstances when the disclosures would have been lawful.[47] The Department of Education's Privacy Technical Assistance Center (PTAC) has been vital for schools seeking practical guidance on FERPA. PTAC could publish guidance, hold training sessions, and provide additional technical assistance on this issue. It could be particularly useful for guidance that includes illustrative case studies and examples of when a school may or may not use FERPA's exceptions to report potential threats.

---

[45] Research on School Security, The Impact of Security Measures on Students, *National Association of School Psychologists,* http://www.audioenhancement.com/wp-content/uploads/2014/06/school-security-by-NASP.pdf.

[46] Gurland, S.T. and Grolnick, W.S. (2005). "Perceived threat, controlling parenting, and children's achievement orientations." *Motivation and Emotion, 29* (2), 103-121.

[47] Daggett, *supra* note 32 ("A report commissioned by Virginia's governor to investigate includes a finding that a misunderstanding of FERPA prevented appropriate sharing of information about the student to parents, school employees, and others."); Zeide, Student Privacy Principles *supra* note 9.

It is also important that schools are aware of other legal requirements that they may have under state or federal law. For example, state tort laws may require schools to "warn or take other steps if a student poses a threat to herself or others."[48] State laws requiring reporting of child abuse may cover reporting "suspected abuse not only by adults but also at the hands of a peer."[49] PTAC can collaborate with other entities - as they have in the past to provide guidance on the intersection of FERPA and HIPAA with the Department of Health and Human Services[50] - to provide a full picture of what schools are allowed - and required - to share in order to ensure school safety.

V. Further Research Could Identify the Best Methods to Promote Health and Safety in Schools while Safeguarding Privacy

In September 2017, the bipartisan Commission on Evidence-Based Policymaking released its final report, calling for a commitment to "a future in which rigorous evidence is created efficiently, as a routine part of government operations, and used to construct effective public policy." To reach this future, the report notes that "policymakers must have good information on which to base their decisions about improving the viability and effectiveness of government programs and policies." The issues at stake regarding school safety are of the utmost importance. They involve complex risk assessments concerning potential threats to student safety as well as potential privacy harms. They implicate the interests of individuals, communities, and society. This analysis could be better informed by empirical data regarding the nature, extent, and leading causes of the key privacy risks and safety risks facing students and schools.

---

[48] Daggett *supra* note 32.
[49] *Id.*
[50] *See* U.S. Dep't. of Health & Human Servs., Report to the President on Issues Raised by the Virginia Tech Tragedy (2007), https://www.justice.gov/archive/opa/pr/2007/June/vt_report_061307.pdf.

The Federal Commission on School Safety should consider calling for further research regarding these issues.

VI. Recommendations

As discussed above, FPF recommends that the Commission:

- be mindful of the full range of privacy risks and harms, as well as the importance of privacy safeguards, as it considers options to improve school safety;
- support efforts to better educate and communicate with stakeholders regarding existing legal authorities that permit data sharing to promote health and safety within a framework that mitigates privacy risks to students; and
- call for neutral, expert analysis of empirical data regarding the nature, extent, and leading causes of the key privacy risks and safety risks facing students and schools.

As the National Association of School Psychologists noted in their 2013 recommendations for school safety policies, trust between students and adults is crucial in ensuring that students reach out to get the help they need and report concerns about other students when they have them.[51] Appropriate student privacy safeguards create that trust and promote school safety.

[51] *Policy Recommendations for Implementing the Framework for Safe and Successful Schools*, NASP (last visited July 6, 2018), https://www.nasponline.org/resources-and-publications/resources/school-safety-and-crisis/a-framework-for-safe-and-successful-schools/policy-recommendations-for-implementing-the-framework-for-safe-and-successful-schools.