Kids & Technology Essay Series - November 2021

Improving Student Privacy Through Better Governance

Why Schools Need to Go Beyond Legal Compliance to Serve Students and Families, Especially Around Tech-Driven School Safety and COVID-19 Efforts

Elizabeth Laird

Centre for MEDIA, TECHNOLOGY and DEMOCRACY

McGill | MAX BELL SCHOOL of PUBLIC POLICY

Table of Contents

About the Series

Children and youth stand to be especially impacted by the attention economy of data-driven technologies, educational tools that support surveillance and data collection, and toxic online environments. Engaging with a broad network of interdisciplinary scholars, this project aims to understand and address the impact of media technologies on children and youth against a broader data privacy governance agenda. The project convenes leading experts, policymakers, and impacted stakeholders to question the challenges posed by digital technologies to children and youth.

About the Author

Elizabeth Laird

Director, Equity in Civic Technology, Center for Democracy & Technology

Elizabeth Laird serves as CDT's Director, Equity in Civic Technology, where she leads the organization's work in this critical area. Building on the work she leads in CDT's Student Privacy Project, her work engages civic institutions to promote the responsible, equitable use of data and technology to improve outcomes for individuals and the public good, while ensuring it does not come at the expense of privacy and civil rights.

Prior to joining CDT, Elizabeth served as deputy assistant superintendent of data, assessment, and research at the Office of the State Superintendent of Education (OSSE), DC's state education agency. In that role, she served as OSSE's privacy officer and led the implementation of student privacy training for all staff, reviewed and approved data requests and data systems application releases, and provided guidance to staff on how to collect and protect student data. Before joining OSSE, she was accepted into The Broad Residency in Urban Education and worked at the Louisiana Department of Education where she oversaw the implementation of a restrictive student privacy bill. She began her career in education data and privacy at the Data Quality Campaign, where she worked for seven years, most recently as the director of communications and external affairs.

Elizabeth holds a Bachelor of Science in Mathematics from Vanderbilt University, a Master of Public Affairs from the LBJ School of Public Affairs at the University of Texas at Austin, and a Master of Education in Educational Leadership from The Broad Center for the Management of School Systems.

Introduction

Despite the recent headlines about schools failing to protect student data or use it responsibly, student privacy is not a new issue. In the United States, the primary federal privacy law that protects sensitive student information was enacted in 1974, fifteen years *before* people started using the internet. Schools have decades of experience navigating privacy rules and regulations; however, there are still routine student privacy and data use failures like preventable data breaches, sharing student data without parental consent, or deploying technologies that actually exacerbate inequity. Although legislation is an important tool to encourage better privacy practices and policies in schools, it can be limited in what it can achieve. The legislative and related enforcement processes can be slow, unpredictable, and lack the precision that is needed to truly protect the privacy and civil rights of students and families. Effective and transparent governance of student data and technology, including the authority to make decisions, can work in concert with fulfilling legal obligations to strike the right balance between the promise and pitfalls of using data and technology to help students and families. The possibilities of improved governance are perhaps best seen in current efforts to use data and technology to make schools safer, both in the context of preventing acts of mass violence as well as reopening schools in the midst of a pandemic, in which data and technology are being used in ways that are likely legal but perhaps not in the best interest of students and families.

Defining Student Privacy and Why It Matters

In discussions about how to improve policies and practices around student privacy, it is important to first start with what is meant by student privacy. For example, privacy in a school setting conjures ideas of schools collecting more data than is needed and never deleting it (thus creating a de facto permanent record)[1], companies using student data for purposes that go beyond education to increase their profit[2], or parents sitting by helplessly as data about their children is shared with third parties without their consent or understanding of how this will help them[3]. In reality, all of these are legitimate privacy risks that are not only possible but have happened, with a direct and negative impact on students and families.

Student privacy is not just a legal or technocratic issue with theoretical harms but an important consideration that can make achieving the mission of schools – ensuring that all students, especially the most vulnerable, receive a high-quality education that positions them to be successful later in life – easier, or harder.

Student privacy is not just a legal or technocratic issue with theoretical harms but an important consideration that can make achieving the mission of schools – ensuring that all students, especially the most vulnerable, receive a high-quality education that positions them to be successful later in life – easier, or harder, depending on how well a school can balance the promises of education data and technology with harms it can inflict on students. Moreover, although it is true that student privacy entails legal compliance (for example, the United States has several federal student laws with student privacy considerations and almost 130 state student privacy laws across 45 states to which schools must adhere[4]), complying with legal requirements is the floor, not the ceiling, when it comes to protecting students and their families.

For purposes of this essay, student privacy is not just about legal compliance but about protecting the rights of individuals to make decisions about what happens with their data, which in the context of education means protecting the rights of students and families. This includes schools fulfilling their ethical obligation to ensure that the use of data and technology do not come at the expense of student safety and well-being, which almost always entails going above and beyond what is required by law. In fact, one of the most effective and powerful tools to strike the right balance between the potential of data and technology to improve educational outcomes while not endangering students in the process is governance. By centering the student and their family, student privacy becomes a core component of a school's work, and everyone's responsibility.

Defining Governance and Why It Matters

Governance is another term that can represent different ideas, ranging from technical decisions to theoretical values, but for purposes of this essay, governance means the people, processes, and structures that make decisions about how data and technology is used while protecting privacy. To further clarify, governance in this context extends beyond data governance, which can be more technical, and includes other processes, like policy decisions, budgeting, procurement, and regulations, which can set an overall direction and affect what happens with data and technology in a school setting.

Governance is important because it establishes a process, not a static solution, for navigating emerging education about data, technology, and privacy issues. Certainly laws are critical tools for protecting students and families, but they are limited in what they can achieve as they can take a long time to debate and enact (if they are enacted at all) and challenging to write in such a way that is specific enough to prohibit unethical behavior that is not in the interest of students but also broad enough to address evolving and emerging issues. Oftentimes this results in laws needing to be updated frequently, and as soon as they are, they are already outdated as new issues have emerged. Additionally, enforcement of privacy laws, not just in education, is an ongoing issue that can limit the effectiveness of laws in encouraging privacy-protective behavior. Enforcement can be uneven or nonexistent, so the existence of a privacy law may not actually change behavior if there is a perception of little to no consequences of noncompliance[5].

With legal obligations as the starting point, governance can be a better tool to respond to and address new issues. A core role of public agencies within the school system is to make administrative decisions and set policies to shape and direct behavior related to educational issues. This can and should include data, technology, and student privacy. The people and processes that compose governing bodies can serve as critical arbiters in making decisions about whether certain education data, technology, and privacy practices align with the vision and mission of their system, making difficult but critical values-based decisions. These bodies can navigate complex issues that go beyond legal compliance and assess privacy harms that students and families may experience from perfectly legal but bad ideas. As new issues arise, there are existing processes with the right people to respond in a timely and thoughtful manner. The need for improved governance of data, technology, and privacy in schools is perhaps most evident in current efforts to use data and technology to keep students safe.

Tech-Driven School Safety

The use of data and technology in service of making schools and students safer provides an illustrative example of how governance of data and technology used by public agencies is needed to redirect efforts beyond legal compliance and center the student in evaluating whether they are, in fact, any safer. Protecting students and creating a supportive environment is foundational to them learning, growing, and succeeding. In fact, recent research indicates that parents and teachers identify safety and well-being as among their top concerns, and if they are concerned with privacy, it is because of how it can negatively affect student safety and well-being. Their primary concern is not legal compliance but helping students be successful and learn, part of which is creating a learning environment in which they feel safe.

Unfortunately, high-profile but statistically rare events have put increased pressure on schools to take additional steps to keep schools and students safe, and just like in other aspects of our lives, schools are turning to data and tech-driven initiatives to support these goals. Tech-driven school safety initiatives include using facial recognition technology to monitor and determine who is allowed to be on school grounds[6], deploying social media monitoring algorithms that use keyword searches to find threatening language[7], providing law enforcement with real-time access to cameras on school campuses[8], sharing individual-level data across public agencies to assess whether someone poses a threat to themselves or others[9], and incorporating disparate data into behavioral threat assessment processes that are used to determine whether and how to intervene with a student who has been identified as potentially capable of harm [10]. These uses of data and technology might seem innocuous and typically do not violate student privacy laws with appropriate agreements and data practices in place; however, just because a public agency can do something does not mean that they should do it.

Student privacy laws typically focus on the collection, sharing, and use of education data and technology by public agencies and/or private companies. In the case of school safety, schools typically rely on vendors to deploy the aforementioned technology, so understanding the legal obligations of public agencies and vendors is important. For example, in the United States recent trends in state student privacy laws include limiting what vendors can do with data provided to them by schools, requiring deletion of student data after a specific period of time, prescribing further limitations on sensitive data like biometric information, and even detailing penalties if data is misused[11]. These laws will influence how some of these tech-driven school safety are deployed but not whether they should be deployed. In other words, schools and vendors can likely comply with student privacy laws but still implement technology that is actually harmful and does not fulfill their mission of keeping students safe and supporting their future success.

Many of the technologies that were just described are new to the education sector and unproven in their efficacy. However, it is inevitable that the technology and its accuracy will improve, so in addition to efficacy, it is also important to assess the cost of these initiatives. Not only could they be unreliable, but they divert resources (people, time, and money) from other people-driven school safety initiatives (counselors, behavior interventions, mental health supports) that could be more effective. Take a social media monitoring algorithm as an example of when the financial cost might be relatively low, but the opportunity cost could be quite high[12].

It is inevitable that the data generated by social media monitoring algorithms will be noisy and require quite a bit of human review due to a few reasons[13]. First, acts of mass violence, which many of these tools aim to prevent, are statistically rare, so there is no pattern or profile of language that predicts whether someone will commit a tragic act. Because of that, key word searches will certainly be overly inclusive as they include as many key terms as possible to compensate for the lack of evidence that predict whether someone will commit an act of mass violence. Second, social media monitoring algorithms do not understand tone, jokes, or slang. It cannot differentiate between someone saying, “This movie is the bomb,” and “I am bringing a bomb to school,” so both of these, along with many other posts, would be reported back to the school for human review. A third limitation is that they are trained on data that is not representative of student populations or all types of media, in particular slang, non-English languages, images, videos, and emojis. This leads to either a gap in the service provided or, perhaps worse, the social media monitoring algorithm will be even less accurate, resulting in less-quality data that diverts resources even further[14].

In addition to social media monitoring algorithms, other tech-driven school safety initiatives suffer from similar limitations in that they lack efficacy, have a chilling effect on students, perpetuate discriminatory outcomes, and waste scarce resources[15]. Therefore, what is most important to consider is what is meant by school safety and to be critical about whether tech-driven school safety initiatives are, in fact, keeping all students safer[16]. These initiatives likely have unintended consequences that will have a disproportionate effect on communities that are already vulnerable and marginalized[17]. In a school setting, equity is a crucial component of a school's mission, which makes these initiatives run counter to what they are trying to achieve. The school to prison pipeline in which students are over-exposed to law enforcement is a well-known issue that is plaguing schools[18], and tech-driven school safety initiatives have the potential to accelerate this trend, rather than abate it. Therefore, it is critical to ask whether these technologies actually make students safer and if so, for whom are they safe?

The school to prison pipeline in which students are over-exposed to law enforcement is a well-known issue that is plaguing schools, and tech-driven school safety initiatives have the potential to accelerate this trend, rather than abate it.

Governance of Data, Technology, and Student Privacy

Despite these limitations that could lead to making students less safe, schools are engaging these tech-driven services as they, for the most part, can fulfill legal student privacy requirements but may not actually keep students safer[19]. Some localities have attempted to address this issue with legislation[20], but most have not. If new or existing legislation cannot force further scrutiny of the use of these technologies, governance of how school systems are making these policy and administrative decisions offers a better opportunity to influence these choices. Therefore, the most timely solution to making these kinds of decisions is strong governance.

Who should be involved?

A make or break decision about whether data and technology are privacy-protective and used in ways that benefit individuals is who gets to make that call. Well-meaning individuals who lack technical and privacy expertise may not ask the right questions or fully comprehend the unintended consequences of utilizing certain types of technology for specific purposes. After a multi-state tour of the United States, the United States School Safety Commission released a report in which school district practitioners cited their primary challenge as evaluating the effectiveness and appropriateness of school safety technologies, as they lack this expertise and are overwhelmed by pitches from vendors [21].Moreover, decisions about education data, technology, and privacy require multidisciplinary input. For example, a decision about tech-driven school safety should include input from subject matter experts in school safety, privacy, and technology, which typically span multiple people and even divisions in school systems. If it is something that is being purchased, which it typically is in the case of tech-driven school safety, it will also require input from those responsible for procurement and budget. One of the most important steps that an organization can take is to identify the right people to provide input at the right time, especially on decisions that set the goals and direction for whether and how technology will be used.

With that said, a significant challenge that many school systems will face in putting together this multidisciplinary team is that they lack privacy capacity. 95% of data security incidents are a result of human error, which is largely due to a lack of capacity and training on privacy and security[22]. Education is no exception. A recent survey of school district chief information officers in the United States revealed that although their top concern is cybersecurity, staffing and resource constraints are limiting their ability to solve this issue[23]. Therefore, it is important to be realistic about the skill set that an organization has when identifying who will make these decisions. This is even more important when dealing with vendors as the education technology industry continues to grow rapidly, (e.g. EdTech companies have raised more money in this year than in all of 2019, especially with the shift to remote learning[24]), but school systems have not experienced that same level of growth and are largely organized in the same way that they have been for decades. As the education data and technology industry grows, an already under-resourced and underserved issue like student privacy is experiencing an even greater imbalance of power, knowledge, and skill. The good news is that capacity can be built, and there are a number of resources available to support this development as student privacy is not a new issue in education. Moreover, school systems are increasingly centralizing student privacy responsibilities by hiring chief privacy officers (or their equivalent under a different title) that coordinate and manage these efforts on behalf of the organization and will play a critical role in how decisions are governed[25].

In addition to determining who is involved internally in making these decisions, it is also important to consider who should be involved outside the education system. Privacy laws do not typically require the consultation of those whose opinion arguably matters the most: students and families. After all, it is their data that is being collected, analyzed, and shared, and yet they are rarely, as sung in the musical *Hamilton*, “in the room where it happens.” However, there are many examples of how this lack of involvement and consultation hurts tech-driven initiatives. For example, in the wake of the tragic school shooting in Parkland, Florida, the state legislature quickly passed the Marjory Stoneman Public High School Safety Act in 2018 that required the creation of a centralized repository of information on individual students that included information from multiple public agencies including law enforcement, juvenile justice, and children and family services, along with social media data on students[26]. The purpose of this repository is to integrate information about individual students, so that stakeholders can analyze it to determine who might pose a threat of committing an act of mass violence. However, as previously stated, there is no research that could predict who might perpetrate such an act, but there are well-documented examples of how this type of data sharing without a clear and achievable purpose can harm individuals, especially those from marginalized communities[27]. Some parents were in support of this law but many groups of parents were not consulted, so when awareness about this particular provision of law increased, the system was delayed significantly, experienced public pushback[28], and ultimately scaled down to where it is essentially useless[29]. Another tech-driven school safety initiative that experienced backlash occurred in St. Paul, Minnesota in which the local school district and law enforcement established a data sharing agreement aimed at decreasing arrests by predicting which students might commit a criminal act and intervening before something happened[30]. Similar to Florida, once parents and community members learned of this project, it galvanized the community, resulting in the dissolution of the agreement and loss of several years of work. A community leader said, “Data is not bad, but data without any kind of oversight that includes the community does not benefit us[31].”

As education is a public good, it is incumbent on leaders to prioritize engaging families in decisions about how data and technology are used while protecting their privacy and civil rights.

It is important to remember that parents are not a monolith and will have different opinions on what is appropriate and right for their children, and this extends to how data and technology are used to keep their children safe. As education is a public good, it is incumbent on leaders to prioritize engaging families in decisions about how data and technology are used while protecting their privacy and civil rights. Not only might it prevent the backlash that school districts have experienced, but it also ensures that well-meaning, tech-driven school safety initiatives are meeting their intended goals and reflecting the needs and concerns of the communities they serve.

Which issues need better governance?

In addition to identifying the right people to involve in decision-making, it is critical to identify which issues will be addressed and how they will be resolved. If well-designed, these processes are where governance is better suited to respond to evolving questions and demands, especially in an emerging area like tech-driven school safety. There are the typical technical governance issues related to data and technology including data standards, data definitions, platform specifications, and disclosure avoidance rules that need to be addressed[32], but there are frequently overlooked but equally important processes that would benefit from including data and technology expertise in their governance like identifying the problem to solve, budgeting and procurement, overseeing privacy, and issuing policies and regulations that will drive better practices.

Problem identification

To start, governance of data and technology should not only be responsible for technical issues but also strategic questions that will drive subsequent decisions, the most important of which is: what problem are we trying to solve? In the context of school safety, this question is critically important as it establishes the scope of the issue as well as whether technology can solve it. For example, it is very difficult, if not impossible, to predict who might perpetrate an act of mass violence, with or without technology. If that is what a school system is seeking to accomplish, facial recognition, social media monitoring, real-time access to cameras, and data sharing are unlikely to meet this goal[33]. Even worse, deploying these technologies could actually make students less safe as surveillance is known to disproportionately affect marginalized communities or further expose groups of students to law enforcement who already have more interactions with police than their peers. Too often school practitioners collect data or buy technology first and then ask how they can help when in fact it should start with their questions[34]. In determining whether technology is safe and for whom, using governance to identify the problem and determine whether data and technology might solve it is one of the most critical issues to address and from which all subsequent decisions should be made.

Budgeting and procurement

Another issue that has a significant impact on tech-driven school safety initiatives is budgeting and procurement. In a resource constrained environment, like exists in schools, governance can assist with making tough choices about the best use of resources, including purchasing new technologies. Ensuring that the governance of budgeting and purchasing decisions includes data, technology, and privacy expertise can make certain that a product is equipped to solve the problem that has been identified as well as meet the needs of students and families while not violating their rights. Without this, school systems might purchase a product that does more harm than good, has lax privacy controls, or poor security practices that jeopardize the well-being and rights of students and families. Having a multidisciplinary team to oversee these decisions is an important lever in governing how data and technology can support school safety.

Additionally, the budgeting and procurement process also provides an opportunity for the public to gain transparency into how schools are allocating funds and the specifics of the services they are seeking. Budgeting and procurement documents are typically public records, thus subject to freedom of information requests. Transparency is especially important regarding tech-driven school safety as schools are not obligated, and in many cases choose not to, communicate to families and communities about how they are using data and technology to keep schools and students safe. As stated earlier, it is a best practice and in the interest of schools to be more proactive and communicate; however, having a means through which the public can force this transparency is an important lever that is being used around this issue.

Student privacy

Just as overall governance requires a multidisciplinary team, effective and efficient privacy management does as well. It requires legal, policy, and technical expertise, in addition to understanding the programmatic goals which are set by other subject matter experts[35]. Anticipating and planning for a team to support privacy practices is also important. Everyone within a school system plays a role in keeping students safe and protecting their well-being, and that extends to protecting privacy and civil rights. Considering and planning for how different perspectives and input are needed to make these decisions is an important aspect of governance.

Policies and regulations

School systems have the authority to issue policies and regulations that can drive behavior among practitioners, so this is an important governance tool as well in managing data, technology, and privacy. Policies or regulations that address data or technology in some form (e.g. data collection, school accountability, public reporting, school finance, school assignment lotteries) provide an opportunity to reinforce the importance of privacy as well as specific steps that stakeholders can take to protect student privacy. To do this, the drafting and release of policies and regulations must go through an inclusive governance process that includes data, technology, and privacy expertise to ensure this perspective and skillset is incorporated. In some cases, public agencies can issue regulations that focus solely on student privacy and provide opportunity for public input and comment[36], further demonstrating that other forms of public governance can shape privacy practices and policies in a timely manner.

Data governance

In addition to the aforementioned issues, data governance can oversee the policy and implementation of data and technology for an agency. The aspect of governance that is perhaps the trickiest to balance is the structures through which people will engage, advise, and decide on the issues described above. Government is notorious for concocting overly complicated processes that become so cumbersome that they are merely tolerated or even avoided. Data governance is subject to the same risks if the structures are not well-conceived to be flexible, responsive, and have the right authority to move work forward at a speed that the work of serving students and families often demands.

Fortunately, quite a bit of work has been done on the best ways to structure data governance to accomplish business goals while effectively balancing data and technology with privacy considerations. When it comes to data governance, form should follow function, so taking an inclusive approach to governance likely entails governance at various levels of the system (starting with the executives with the most authority down to data stewards with technical expertise). *Figure 1* provides an example of a K-12 data governance structure, with multiple levels of input and stakeholders depending on the goals they are trying to accomplish.

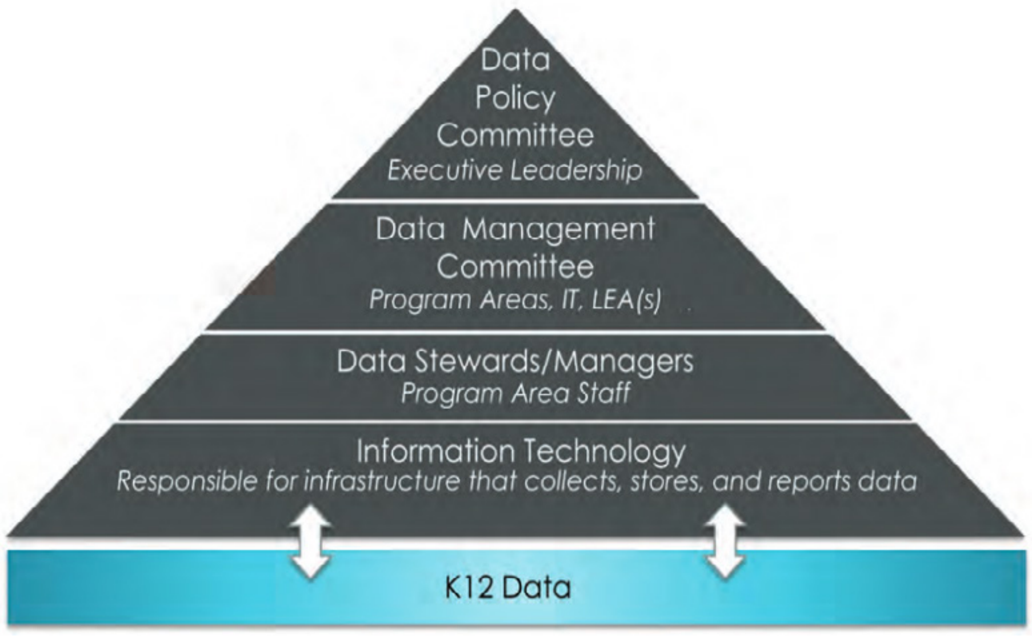

Figure 1: A traditional data governance structure for a single agency (a K-12 agency is used as an example)37

In the context of school safety, having a data governance structure in place will support informed decisions, but it is also important to incorporate data, technology, and privacy expertise into governance structures that are addressing related but separate issues that affect what is possible like policy, budget, procurement, and programmatic decisions. For example, school districts may have established cross-functional teams that lead and execute school safety initiatives, which like privacy also span multiple people and decisions, so it is important that those structures also include data, technology, and privacy expertise.

Looking Ahead: Tech-Driven COVID-19 Initiatives

In recent months, the classroom has moved from the school building to the home due to the global pandemic, which has created new privacy issues for schools to address. In particular, as schools look at reopening for in-person instruction, they are considering versions of the same technology that were used in the name of school safety[38]. In fact, protecting students and the adults that work with them from contracting or spreading COVID-19 is the latest priority issue within the school safety portfolio. It is important to understand the connection between these two initiatives and overlapping technologies as they share similar goals and limitations, which should be navigated through effective governance. The facial recognition technology that could be used to control who has a right to be on campus has been extended to include thermal imaging that can take an individual's temperature[39]. Social media monitoring could try to keep tabs on which students and families are complying with social distancing restrictions[40]. Mobile applications with varying levels of privacy protection could collect information from families about their children's health and that information could be shared with third parties (e.g. department of health) without parental consent or a way to opt out[41].

Similar to tech-driven school safety initiatives, schools are turning to data and technology to help them reopen schools in ways that keep students safe, in this case preventing students (and teachers) from contracting and spreading a life-threatening illness. However, it is in moments of crisis that individuals are most likely to sacrifice their rights, including privacy [42], so it is important that advances in technology and data do not compromise the rights of students and their families. There are several steps that education policymakers and practitioners should take to protect student privacy, the most important of which is to govern these choices in a deliberate, thoughtful, and inclusive manner. As previously discussed, this will include internal governance bodies that comprise the right people, discussing the right issues, and within the right structures to make optimal decisions. Additionally, engaging parents and community members is also important to prevent backlash as well as solicit input to ensure that tech-driven COVID-19 initiatives are meeting community needs and addressing concerns. If schools already have these structures in place, it would behoove them to utilize and adapt them rather than abandon them as they have experience and capacity in addressing some of these issues.

> However, it is in moments of crisis that individuals are most likely to sacrifice their rights, including privacy, so it is important that advances in technology and data do not compromise the rights of students and their families.

Conclusion

Assessing the benefits of data and technology against the potential risks and privacy violations can be an art, not a science, especially if schools go beyond legal compliance and center what is best for students and families. At the same time, technology and the problems that it is trying to solve are rapidly evolving, which presents challenges to address student privacy via legislation only. Therefore, if schools seek to address their ethical obligation to ensure that data and technology do not come at the expense of student's safety and well-being, governance of agency administrative and policy decisions is a critical component of achieving this objective. Moreover, that governance should be inclusive and extend beyond technical requirements to address important strategic issues and decisions that will drive technical implementation, like programmatic goals, budgeting, procurement, privacy management, and policies and regulations.

It is not enough to construct internal governance without considering how to collect and incorporate external feedback, especially from parents and community members. This is an important step to ensure that data and technology are used responsibly, meet community needs, and minimize potential backlash that might occur if communities are not consulted and do not agree with the direction that was chosen. Efforts around school safety, in particular preventing acts of mass violence and contracting and spreading COVID-19, are at risk of utilizing data and technology that is not effective, wastes resources, and actually makes certain students less safe by using unproven technologies to surveil students. These technologies are likely legal, so governance is perhaps the best approach to balancing emerging technologies with privacy and civil rights. Everyone in the school system has a responsibility to keep students and families safe, and that includes protecting their privacy and civil rights. Effective and efficient governance can help do just that.

Endnotes

[1] Benjamin Herold, “Schools Collect Tons of Student Information, Deleting It All Is A Major Challenge,” *Education Week*, March 15, 2019, https://blogs.edweek.org/edweek/DigitalEducation/2019/03/schools_data_deletion.html.

[2] Natasha Singer, “For Sale: Survey Data on Millions of Students,” *New York Times*, July 29, 2018, https://www.nytimes.com/2018/07/29/business/for-sale-survey-data-on-millions-of-high-school-students.html.

[3] Benjamin Herold, “inBloom to Shut Down Amid Data-Privacy Concerns,” *Education Week*, April 21, 2014, https://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html.

[4] “Education Data Legislation Review: 2019 State Activity,” *Data Quality Campaign*, August 1, 2019 https://dataqualitycampaign.org/wp-content/uploads/2019/10/DQC-Legislative-summary-02042020.pdf.

[5] *Final Report of the U.S. Department of Education Office of Inspector General Office of the Chief Privacy Officer’s Processing of Family Educational Rights and Privacy Act Complaints.*

[6] Claire Galligan, Hannah Rosenfeld, Molly Kleinman, and Shobita Parthasarathy, “Cameras in the Classroom: Facial Recognition Technology in Schools,” *University of Michigan Gerald R. Ford School of Public Policy Science, Technology, and Public Policy Program*, August 10, 2020, http://stpp.fordschool.umich.edu/sites/stpp.fordschool.umich.edu/files/file-assets/cameras_in_the_classroom_full_report.pdf.

[7] 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.

[8] Benjamin Herold, “Parkland Commission: Police Should Get Real-Time Access to School Security Cameras,” *Education Week*, December 13, 2018, https://blogs.edweek.org/edweek/DigitalEducation/2018/12/parkland_commission_police_school_cameras.html.

[9] Jessica Bakeman, “Florida Launches Controversial Database Of Student Information Aimed At Identifying Threats,” *WLRN*, September 15, 2019, https://wusfnews.wusf.usf.edu/2019-09-15/florida-launches-controversial-database-of-student-information-aimed-at-identifying-threats.

[10] Bethany Barnes, “Targeted: A Family and the Quest to Stop the Next School Shooter,” *The Oregonian*, August 29, 2019, https://www.oregonlive.com/news/erry-2018/06/75f0f464cb3367/targeted_a_family_and_the_ques.html.

[11] “Education Data Legislative Review: 2018 State Activity,” *Data Quality Campaign*, October 2018, https://dataqualitycampaign.org/wp-content/uploads/2018/09/2018-DQC-Legislative-Summary.pdf.

[12] Hannah Quay-de la Vallee and Natasha Duarte, “Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data,” *Center for Democracy and Technology*, August 2019, https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf.

[13] “Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns,” *Center for Democracy and Technology and Brennan Center for Justice*, October 17, 2019, https://cdt.org/wp-content/uploads/2019/10/CDT-Brennan-School-Social-Media-Monitoring.pdf.

[14] Quay-de la Vallee et al., “Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data.”

[15] "Technological School Safety Initiatives: Considerations to Protect All Students," *Center for Democracy and Technology and Brennan Center for Justice*, June 4, 2019, https://cdt.org/wp-content/uploads/2019/06/2019-05-24-School-safety-two-pager-Final.pdf.

[16] Maggie Koerth-Baker, "Mass Shootings Are a Bad Way to Understand Gun Violence," *FiveThirtyEight*, October 3, 2017, https://fivethirtyeight.com/features/mass-shootings-are-a-bad-way-to-understand-gun-violence/; "School Violence Myths," *University of Virginia Curry School of Education and Human Development*, July 26, 2015, https://curry.virginia.edu/faculty-research/centers-labs-projects/research-labs/youth-violence-project/violence-schools-and-5.

[17] Nora Gordon, "Disproportionality in Student Discipline: Connecting Policy to Research," *Brookings Institution*, January 18, 2018, https://www.brookings.edu/research/disproportionality-in-student-discipline-connecting-policy-to-research/.

[18] "We Came to Learn: A Call to Action for Police-Free Schools," *Advancement Project and the Alliance for Educational Justice*, https://advancementproject.org/wecametolearn/.

[19] Faiza Patel and Rachel Levinson-Waldman, "School Surveillance Zone," *Brennan Center for Justice*, April 30, 2019, https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone.

[20] Kyle Wiggers, "New York Bans Use of Facial Recognition in Schools Statewide," *VentureBeat*, July 22, 2020, https://venturebeat.com/2020/07/22/new-york-bans-use-of-facial-recognition-in-schools-statewide/.

[21] *Final Report of the Federal Commission on School Safety: Presented to the President of the United States.*

[22] "IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of Cyber Attack and Incident Data from IBM's Worldwide Security Operations," *IBM*, May 2014, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.

[23] "2020 State of EdTech Leadership," *Consortium for School Networking*, accessed September 14, 2020, https://www.cosn.org/focus-areas/leadership-vision/state-edtech-leadership.

[24] Marlene Givant Star, "EdTech Awash in Capital Amid Shift to Remote Learning," *Forbes*, September 2, 2020, https://www.forbes.com/sites/mergermarket/2020/09/02/edtech-awash-in-capital-amid-shift-to-remote-learning/#59cbfa3d7adc.

[25] Elizabeth Laird, "Chief Privacy Officers: Who They Are and Why Education Leaders Need Them," *Center for Democracy and Technology*, January 30, 2019, https://cdt.org/insights/chief-privacy-officers-who-they-are-and-why-education-leaders-need-them/; Emily Tate, "Chief Privacy Officers: The Unicorns of K-12 Education," *EdSurge*, February 25, 2019, https://www.edsurge.com/news/2019-02-25-chief-privacy-officers-the-unicorns-of-k-12-education; Kate Stringer, "Exclusive: Student Data Needs Protecting, New Report Says. Hiring a Chief Privacy Officer Can Help Schools and Districts Do Just That," *The 74 Million*, January 30, 2019, https://www.the74million.org/article/exclusive-student-data-needs-protecting-new-report-says-hiring-a-chief-privacy-officer-can-help-schools-and-districts-do-just-that/.

[26] *Marjory Stoneman Douglas Public High School Safety Act 2018*, S.B. 7026, (Florida) s. 1001.212 (6).

[27] 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-createstudent-profiles-based-on-risk-factors/85-e982ec3f-7e9a-481a-99d3-b8d3f21052de.

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

[29] Katya Schwenk, "Florida 'Student Safety' Database Fell Short, Commission Says," *EdScoop*, August 16, 2019, https://edscoop.com/florida-student-safety-database-public-safety-commission/.

[30] Frederick Melo, “St. Paul, Ramsey County to End Youth Data-Sharing Agreement After Withering Criticism,” *Twin Cities Pioneer Press*, January 28, 2019, https://www.twincities.com/2019/01/28/st-paul-ramsey-county-to-end-youth-data-sharing-agreement-after-withering-criticism/.

[31] Ibid.

[32] “Data Governance Toolkit: Implementation,” *National Center for Education Statistics Institute of Education Sciences Statewide Longitudinal Data Systems Grant Program*, accessed: September 14, 2020, https://slds.ed.gov/#program/data-governance-policies-and-processes.

[33] Faiza Patel and Rachel Levinson-Waldman, “Monitoring Kids’ Social Media Accounts Won’t Prevent the Next School Shooting,” *Washington Post*, March 5, 2018, https://beta.washingtonpost.com/news/posteverything/wp/2018/03/05/monitoring-kids-social-media-accounts-wontprevent-the-next-school-shooting/; Brian Resnick and Javier Zarracina, “This Cartoon Explains Why Predicting a Mass Shooting is Impossible,” *Vox*, August 5, 2019, https://www.vox.com/science-and-health/2018/2/22/17041080/predict-mass-shooting-warning-sign-research; Bruce Schneider, “Why Mass Surveillance Can’t, Won’t, and Never Has Stopped A Terrorist,” *Digg*, March 11, 2015, https://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist.

[34] Education Data 101: A Briefing Book for Policymakers,” *Data Quality Campaign*, accessed September 14, 2020, https://dataqualitycampaign.org/wp-content/uploads/2017/12/DQC-EducationData101.pdf.

[35] Laird, “Chief Privacy Officers: Who They Are and Why Education Leaders Need Them.”

[36] “State Education Department Proposes Regulations to Strengthen the Security of Personally Identifiable Information for Students and School Personnel,” *New York State Department of Education*, January 14, 2019, http://www.nysed.gov/news/2019/state-education-department-proposes-regulations-strengthen-security-personally.

[37] “P-20W Data Governance: Tips from the States,” *National Center for Education Statistics Institute of Education Sciences Statewide Longitudinal Data Systems Grant Program*, February 2017, https://slds.grads360.org/services/PDCService.svc/GetPDCDocumentFile?fileId=25962.

[38] Hannah Quay-de la Vallee and Cody Venzke, “Privacy and Equity in the New School Year: Steps for In-person, Remote, or Hybrid Learning,” *Center for Democracy and Technology*, July 2020, https://cdt.org/insights/report-privacy-and-equity-in-the-new-school-year/.

[39] Julie Jargon, “Back to School? Look Out for Covid-Tracking Surveillance Tech,” *Wall Street Journal*, August 11, 2020, https://www.wsj.com/articles/back-to-school-look-out-for-covid-tracking-surveillance-tech-11597150800.

[40] Kathleen Holder, “‘Sick Posts’ on Social Media Help Early Tracking of COVID-19,” *University of California, Davis*, April 16, 2020, https://www.ucdavis.edu/coronavirus/news/sick-posts-social-media-help-early-tracking-covid-19/.

[41] Zack Whittaker, “Fearing Coronavirus, a Michigan College is Tracking its Students with a Flawed App,” August 19, 2020, https://techcrunch.com/2020/08/19/coronavirus-albion-security-flaws-app/.

[42] “COVID-19 and Student Privacy: Do’s and Dont’s for State and Local Practitioners,” *Center for Democracy and Technology*, September 1, 2020, https://cdt.org/insights/covid-19-and-student-privacy-dos-and-donts-for-state-and-local-practitioners/.

Designed by Yasmeen Safaie

Centre *for* MEDIA, TECHNOLOGY *and* DEMOCRACY

McGill

MAX BELL SCHOOL *of* PUBLIC POLICY