ExcelinEd

MAY 2016

BUILDING A TRUSTED ENVIRONMENT FOR EDUCATION TECHNOLOGY PRODUCTS

ABOUT EXCELINED

Founded by former Florida Governor Jeb Bush, the Foundation for Excellence in Education is igniting a movement of reform, state by state, to transform education for the 21st century economy by working with lawmakers, policymakers, educators and parents to advance education reform across America. Learn more at ExcelinEd.org.

FOR MORE INFORMATION ON STUDENT DATA PRIVACY POLICY

Special thanks to Douglas Levin, Founder and President of EdTech Strategies, LLC for his research and writing for this paper. If you have any questions, need assistance or more information on developing a Student Data Privacy Policy in your state please contact Neil Campbell, Director, Next Generation Reforms.

EXCELINED.ORG

@EXCELINED

FACEBOOK.COM/EXCELINED

Table of Contents

EXECUTIVE SUMMARY

Data about learning, about teaching and about school operations helps to generate information that can and is being used to benefit students. This, in fact, is one of the key advances powering the dynamic movement to use technology in schools to support student learning. At the same time, not all parents and privacy advocates are equally comfortable with data and its many uses, and justifiably so when it involves personally identifiable information about students. To strike the right balance between the benefits and challenges associated with student data use, we must marshal the resources of parents, educators, schools and service providers in a shared effort to build expectations that lead to increased trust.

In the absence of consensus among all these parties, there remains significant risk that privacy advocacy results in the passage of well-intentioned but regressive policies that slow the adoption of technology in education, erect barriers to promising practices that help at-risk students and impede innovation. The long-term implications for providers, educators and students themselves are serious and profound.

Previous work by ExcelinEd examined the legal and regulatory context for student data privacy, particularly on the important roles states play. This paper focuses on the roles and responsibilities of service providers, including education and technology companies, with respect to student data privacy.

This paper highlights the reasons why companies should increase their engagement in student data privacy issues, and it suggests high-level tactics and best practices for how to do so. Insights and advice are derived from our research and a series of interviews conducted in early 2016 with leading privacy advocates, service providers and student data privacy experts.

While not every best practice identified in this paper is suitable for every company or solution, taken together these practices suggest a positive and productive high-level framework for school providers to build trust among parents and privacy advocates. These best practices for service providers include:

- Embracing the principles of privacy by design (primarily—though not exclusively—for new product development);
- Assessing the use cases and need for student data (to re-evaluate and minimize the need for managing personally identifiable information);
- Providing users with tools to manage data collected about students (including tools that involve parents, as appropriate);
- Strengthening student data security practices;
- Reviewing and upgrading privacy policies;
- Communicating a commitment to the privacy of student data; and

- Considering support of third-party privacy initiatives, including the Student Privacy Pledge.

The paper concludes by offering recommendations for those who are vital to establishing a trusted learning environment, such as investors in education and technology companies, school leaders and philanthropists. Every actor involved in supporting learning and success shares responsibility for establishing appropriate polices, deploying the right tools and maintaining good practices.

Coalescing around clear guidelines and expectations for how to make reasonable decisions about student data use will enable the field to find an acceptable balance that advances innovative digital learning opportunities for all students while safeguarding student privacy.

Expert Interviews in This Paper

- Tyler Bosmeny, CEO, Clever
- Alex Bradshaw, Bradshaw, Ron Plesser Fellow, Center for Democracy & Technology
- Brendan Desetti, Director of Education Policy, Software & Information Industry Association
- Bill Fitzgerald, Director of Privacy Initiative, Common Sense Media
- Marsali Hancock, President, iKeepSafe
- Andrew Joseph, Amazon Education
- Jules Polonetsky, CEO, Future of Privacy Forum
- Michael Walden, Partner, ReThink Education

BUILDING A TRUSTED ENVIRONMENT FOR EDUCATION TECHNOLOGY

Education data is critical to serving students and improving schools. Data provides valuable information to families and students on gaps in student understanding and opportunities to build upon student strengths and interests. Education data offers schools insight into the effectiveness of instructional programs and the unique needs of their student body. School service providers, including education and technology companies, use student data to help teachers to differentiate instruction and personalize student learning.

Parents express concerns about the collection of data about students that accompanies the use of new technology and software innovations.

Notwithstanding the many insights provided by data, not all parents are equally comfortable with its collection and many uses. For instance, polling commissioned in 2015 by ExcelinEd found that a sizeable proportion of parents (41 percent) express at least a general level of concern about the collection of data about students and student learning that accompanies the use of new technology and software innovations. Parents also reported having many questions about these data collections, including:

- Who has access to this student learning data?
- How is the data being protected and kept secure?
- What can companies use the data for?[i]

To strike the right balance between the benefits and challenges associated with data collection and use in education, we must aspire to build what the Aspen Institute Task Force on Learning and the Internet described as a "trusted environment for learning."[ii] A trusted environment is one that marshals the resources of parents, educators, schools and service providers (whether working for the school or directly for the student or family) to enhance student success, while ensuring student safety, security and privacy. Every actor involved in supporting learning and success, including service providers, shares responsibility for establishing appropriate polices, deploying the right tools and maintaining good practices.

Previous work by ExcelinEd shined an important light on the legal and regulatory context for student data privacy, particularly on the important roles that states can and are playing. This included the development of student data privacy principles; a snapshot of state laws on student data use, privacy and security; and a whitepaper, *Protecting K-12 Student Data Privacy in a Digital Age*, which identified strategies to address parental and public concerns about student data privacy, including via the passage of new state legislation.[iii]

This paper focuses in depth on one critical aspect of building a trusted environment for learning powered by data that has not yet received enough attention: the roles and responsibilities of service providers, including education and technology companies, with respect to student data privacy.

The insights and advice offered in the paper are derived from a series of interviews conducted in early 2016 with leading privacy advocates, service providers, and student data privacy experts. Without their generosity in sharing time and expertise, this work would not have been possible.[iv]

and strategies to address parent concerns, all grounded in new data commissioned for this paper by ExcelinEd on parent views about technology and student data privacy.

WHY EDUCATION COMPANIES SHOULD CARE ABOUT STUDENT DATA PRIVACY

Fairly or unfairly, some companies and organizations serving education have been singled out by policymakers and the media—often in high-profile ways—for questions about their student data privacy practices. The most prominent example in recent years is arguably that of the nonprofit InBloom, which sought to offer states and districts technical infrastructure services. After a sustained backlash and scrutiny, the effort—despite raising significant capital—failed to successfully launch and was wound down in 2014.

If InBloom's challenges related to student data privacy concerns were not enough to capture the education industry's attention, its demise was followed by—and may have contributed to—the introduction of hundreds of new legislative proposals in virtually every state in the nation, as well as at the federal level. Many of these bills and new laws were designed to circumscribe or limit the ability of schools and companies to collect, manage and share data about students, as well as to introduce new liabilities and penalties for non-compliance.

> "If there is a cloud over the data collection that some companies are doing, it will stifle innovation and slow down adoption."
>
> **Alex Bradshaw**
> Ron Plesser Fellow, Center for Democracy & Technology

For those associated with companies and organizations that have avoided the uncomfortable and politically-charged limelight focused on InBloom, the two-part question remains: first, why should my business care about student data privacy; and second, what benefit could there be for my company in making it a priority?

Jules Polonetsky, CEO of the Future of Privacy Forum, a D.C.-based think tank that seeks to advance responsible data practices, sees immediate and direct reasons for companies serving education to devote sufficient attention and resources to issues of student data privacy. He explained, "It is a risk issue. If you are on the wrong side of a privacy alarm, you find yourself banned from schools. People may not want to fund contracts with you. You could find yourself on the wrong side of a government enforcement action."

"It is a big deal," agreed Alex Bradshaw, the Ron Plesser Fellow at the Center for Democracy & Technology (CDT), a nonprofit organization dedicated to online civil liberties and human rights, including the right to privacy. "If there are concerns about some companies' data collection, it will stifle innovation and slow down adoption." Indeed, many experts interviewed for this paper recognized that policymakers—driven by fear of an unknown future or without due considerations to unintended consequences of their proposals—may "overcorrect" and limit some of the technology-enabled innovation occurring in the education market.[v] At the same time, many also echoed the sentiments of Michael Walden of Rethink Education, an investor in education startups (and a parent of school-aged children himself), who made a point to emphasize that student data privacy is a serious issue. "We understand," he said. "I don't think people are crazy for being concerned."

Defining Student Data

Not all types of student data are created equal, and it is important to understand the varying ways it is both collected and classified.

In general, data about students is generated in one of three ways: (1) it is provided directly by families and students to schools, sometimes at the direct request of schools and sometimes voluntarily; (2) it is generated by educators and other school officials in the course of their duties (such as by professional observation or by administering assessments); and (3) it is generated by service providers who maintain a relationship with the school or—in some cases—directly with the parents or student. Education and technology companies in the service provider role may collect data from students actively (e.g., by having students respond to questions or prompts) or passively (e.g., by tracking student interactions with their software in the form of mouse clicks and metadata).

The data that is collected about students is used for administrative purposes (to ensure the allocation of resources and compliance with regulations), for instructional purposes (primarily by teachers in the classroom), for education assessment and measurement uses (to evaluate education programs and ensure students are on track), and for other non-educational purposes (such as related to student transportation, meals, participation in sports or other extra-curricular activities, or research studies and evaluations).[1]

It is also important to note that personally identifiable information that may be collected about students can—and in many cases is—transformed to protect student identity in ways that allow schools, researchers and service providers to continue to perform necessary duties and functions. These transformations include "de-identifying" data collected about students, as well as aggregating data in those cases where the information needed is not pertinent to the experiences of any individual child or even school. The de-identification of data involves both the removal of any information that could be used to directly identify a student in a data file (such as name, address, telephone number, email address or social security number), as well as the application of scientific techniques to obscure data that could be combined or derived to identify an individual (even absent the direct identifiers described above).

While the varied legal and regulatory context for student data privacy and uncertain future represents a real challenge to companies seeking to serve the education sector, Bradshaw made a point to underscore the real-world trade off for students and families: “We believe in the potential for education technologies to enhance the classroom environment and long-term learning outcomes.” Walden agreed, saying, “We believe that technology has the opportunity to be create better outcomes…[and] better learning….We think technology has a role to play in that and we don’t want to overcorrect on this and stunt some of the opportunities it has to have an impact.”

UNDERSTANDING WHAT IS AT STAKE

Most observers intuitively understand that data about learning, about teaching and about school operations all help to generate insights that can benefit students. This, in fact, is one of the key advances powering the movement to use technology in schools and to support student learning. Based at least in part on analyses of data collected via technology, policymakers and administrators can encourage student success, facilitate more effective instruction and identify steps to ameliorate inequalities.[vi] Indeed, if we are going to be able to move the needle on student outcomes and equity, there is little argument that data needs to be an integral part of that process.

Looking forward, Marsali Hancock, president and CEO of iKeepSafe, a nonprofit dedicated to ensuring the health and safety of youth online, is excited about the emerging ways that technology and data enable not just insight, but personalization, such as by helping students to “better access and benefit from the specific information they need in ways that are engaging and relevant.” Andrew Joseph of Amazon Education, concurred, saying we “need to be able to differentiate teaching and learning for students.” Data generated with the aid of educational technology, Joseph further explained, will increasingly help classroom teachers to individualize instruction for all students, because “we can’t necessarily expect every teacher has the capacity or the time to intuitively (without data) understand where each of their students…are with every single thing they are doing [in the classroom] and to differentiate the learning so that the students get the content and interventions and support they need.”

Nonetheless, Common Sense Media’s Bill Fitzgerald, director of his organization’s privacy review program, noted, “right now, the conversations [about student data collection and use] are really heavily slanted toward the negative.” Why? There are a range of concerns expressed by privacy advocates: from the collection of sensitive data about students; to the alleged oversharing of that data with third parties, some of whom may seek to monetize that data via advertising or other activities; to questions about the ability of schools or their service providers to keep secure the data that they collect.

While each of these issues is concerning and worth being addressed, the biggest reservation expressed by the experts interviewed for this paper centered primarily on potential future uses of student data. Fitzgerald explained, “There are real and ongoing risks with current data practices. Information collected today may be used in ways that we can’t predict tomorrow. It is possible that information may be shared without the subject of the information being asked or even aware.” Hancock added, “If we get it wrong, the information that should be confidential about a student is in public and will

> “We need to be behaving and showing an interest and a concern for this that goes beyond what people expect of us. It is too big an issue.”
>
> **Michael Walden**
> Partner, ReThink Education

follow them forever…. Students could have individuals or organizations make decisions about them and for them, not in their best interests.”

Further confounding the issue, according to Fitzgerald, is that “a lot of people come out strong for student data privacy, because they are against other platforms for data use.” The Future of Privacy Forum’s Polonetsky explained, “There are folks who hate the notion that their kid’s data will be used for research or to better understand how teaching works, just as there are others who understand the incredible importance of being able to assess whether schools are functioning well, certain teachers are teaching well or whether their child is progressing.” As such, student data privacy issues can become proxies for disagreements about curricula and academic standards, classroom management practices, teaching and learning approaches, or even about the role and influence of technology and media in children’s lives.

How should companies and the industry respond? ReThink Education’s Walden offered some direct advice: “We need to be behaving and showing an interest and a concern for this that goes beyond what people expect of us. It is too big an issue. Unless we are having open discussion about this, people are going to assume things.” And, with no counterweight, should public and policymaker sentiment about student data privacy become more extreme and lead to significant new restrictions on data use practices and policies? Walden said it will “squash a lot of innovation and lot of the good that is going to come out of this industry.”

TOWARD CLARITY IN ENSURING STUDENT DATA PRIVACY

Perhaps the greatest challenge facing education and technology related to student data are the myriad, evolving expectations and regulations governing its protection, handling and use. Some of these expectations and regulations vary depending on the age of the student and the state in which they live. Add in the hundreds of legislative proposals considered by policymakers in the last few years, and the task can seem daunting.

“This is an area where the uncertainty has been the risk,” said the Future of Privacy Forum’s Polonetsky. “Most of the players in the space are not there to make money by selling data to data brokers. They are there because they see a mission of helping schools better serve kids.” iKeepSafe’s Hancock added, “In the education community there is not a clear set of guidelines and expectations between users and vendors [with respect to privacy]. There is not clarity yet.”

The solution? “The more we can help schools, companies, and parents see some clear guideposts so they can make reasonable decisions, the quicker we’ll have acceptance and answers for these technologies,” stressed Polonetsky. “The more that can be done to draw some lines that create some standards, it provides schools with the certainty they need.” Standards and rules provide comfort and build trust.

Tyler Bosmeny, CEO of Clever, a platform school districts use to securely manage data access to third-party education applications, sees a silver lining to the student data privacy challenge facing the industry. He said, “There are a lot of companies in the industry who want to push the ball forward on student data privacy. They’re committed to this, and are even looking for opportunities to affirm those commitments.” Bosmeny suggested embracing the opportunity, actively engaging with stakeholders and developing practical solutions that fit your company and customer’s needs.

> “There are a lot of companies in the industry who want to push the ball forward on student data privacy. They’re committed to this, and are even looking for opportunities to affirm those commitments.”
>
> **Tyler Bosmeny** | CEO, Clever

Many in the education and policymaking communities would welcome that sort of meaningful engagement. “All stakeholders need to be more solutions oriented…. and start working together to the extent we can on practical solutions that will work on a day-to-day basis in the classroom,” said CDT’s Bradshaw. Common Sense Media’s Fitzgerald agreed, “There are areas of common ground that we can all find that will make things a lot better for a lot of people. It is professionally irresponsible not to find those, and it is professionally irresponsible not to aggressively go after those.”

We expect that schools, advocates and service providers will welcome those sort of practical solutions. Ultimately, Hancock sees it as nothing less than a shared, mutual goal, saying “companies can build products without the hiccups that come from confusion about student data privacy expectations and…schools can experiment and try new connected technology without hiccups.”

PROMISING PRACTICES TO BUILD TRUST IN DIGITAL LEARNING SERVICES AND APPLICATIONS

Given the issues raised by student privacy advocates, the core question facing companies and organizations offering digital learning solutions to schools is how to build trust into relationships with educators and parents. As ReThink Education's Walden stated, "It is no longer an option. It is a demand. The parents, the districts, the government are going to demand that we address this. They are legislating that we address this. You can't pick and choose any more. You can't hide behind 'this is how we've always done it,' or 'nothing is going on here,' or 'we would never do it.' You've got to have polices and systems in place that address this, and you have to demonstrate that you are out in front of this."

The good news is that the experts interviewed for this paper identified numerous promising practices that leading companies are already implementing or intend to implement to successfully build trust among educators and parents with respect to the use of data about students. These are tactics other companies could adopt, and they include:

- Embracing the principles of privacy by design (primarily—though not exclusively—for new product development);
- Assessing your use cases and need for student data (to re-evaluate and minimize the need for managing personally identifiable information);
- Providing users with tools to manage data collected about students (including tools that include parents, as appropriate);
- Strengthening student data security practices;
- Reviewing and upgrading privacy policies;
- Communicating your commitment to the privacy of student data; and
- Considering support of third-party privacy initiatives, including the Student Data Privacy Pledge.

While not every tactic is suitable for every company or solution, together they suggest a positive and productive high-level framework for school providers to build trust among parents and privacy advocates in promising technology-based innovations in teaching, learning and school operations.

Embrace the Principles of Privacy by Design

“The time to think about privacy is when you build,” advised iKeepSafe’s Hancock. It is far better, she argues, to develop a tool the first time in a way that ensures a business model that can generate sufficient revenue consistent with applicable laws. Indeed, the concept of “privacy by design” was first developed in the 1990s by Ontario’s Information and Privacy Commissioner. Privacy by design is guided by seven foundational principles, including:

- Being proactive, not reactive; and being preventative, not remedial;
- Setting privacy as the default setting for all users, not as an option available to some;
- Ensuring privacy is embedded into the design of the product, not bolted on after the fact;
- Ensuring that full product functionality does not make false tradeoffs among innovation, privacy and security;
- Providing end-to-end security of data over the lifecycle of a user’s interaction with the product;
- A commitment to visibility and transparency of data collection, use and security practices, including a willingness to undergo independent verification of those practices; and
- A respect for user privacy by adopting a user-centric view on privacy defaults, user notifications and other user settings and options.[vii]

The Software & Information Industry Association’s director of education policy Brendan Desetti has seen the concept of privacy by design gain awareness and acceptance among the companies with whom he works. “It is really getting traction,” he said. “It’s important to build a culture of privacy within a company, as opposed to it being siloed in one place.”

Assess Your Use Cases and Need for Student Data

Experts interviewed for this paper underscored the importance of education companies maintaining an accurate and up-to-date understanding of the lifecycle of each of the data elements they collect about students in their products (including passively by tracking student actions through an application), as well as how each element is used to add value to a student’s experience. As CDT’s Bradshaw explained, “It is important for companies to be clear about their use case for data, to be able to describe the data they are collecting to run the platform and how the data serves the platform’s purpose.”

> “The time to think about privacy is when you build.”
>
> **Marsali Hancock**
> President & CEO, iKeepSafe

One key aspect of such an assessment is considering under what situations personally identifiable student data—including direct identifiers (such as name or email) and data that could be reasonably used alone or in combination to derive the identity of an individual student—may even be desirable or necessary to collect. To the extent that personally identifiable data is not necessary, it shouldn’t any longer be collected (or ever collected in the first place). “Data minimization is a no-brainer,” said Common Sense Media’s Fitzgerald. “That should be a starting point and not something you are thinking about three years into your build.”

Such a lifecycle evaluation also entails a consideration of the ongoing need for any collected data. To the degree that data is necessary to provide an educational service of a limited time period (such as for the provision of tutoring services within a school year), that data should be returned or destroyed, as appropriate, after its useful life. Should there be an ongoing business need to continue to maintain collected data, such as for longitudinal analyses of a program's impact or for product improvement purposes, an evaluation should be conducted to assess the desirability of de-identifying any personally identifiable data in order to minimize the risk of a privacy breach.

In the end, this assessment of the collection and use of data needs to be done with an eye toward transparency and "understanding that your use of data can be suspect," added the Future of Privacy Forum's Polonetsky. Any use (or over-collection) of data—beyond that needed for the explicit educational purpose addressed by the product and for product improvement purposes—is likely to be difficult to defend in public. As Polonetsky explained, to the degree you can "communicate and frame properly how you are using data on behalf of students, you are able to succeed at gaining acceptance for your technology or business model."

Resources for Education Startups

Every education startup faces similar challenges: time, capacity and resources to name a few. Nonetheless, that is no excuse for not giving issues related to student data privacy their due consideration. As iKeepSafe's Marsali Hancock explained, "The government regulates the market with respect to children's data privacy, so every company has to pay attention. To not do it right is to leave yourself open to costly fines and threats to your business." Brendan Desetti of the Software & Information Industry Association concurred, saying, "It is really important that you consider these privacy implications from the beginning." Experts interviewed for this paper suggested a number of organizations and sites as places to begin to learn more. These include:

- **Common Sense Media** is developing a system to evaluate the privacy policies, legal terms and basic security practices of education apps: Graphite.org/Privacy
- **Foundation for Excellence in Education (ExcelinEd)** offers resources on the federal and state policy context for student data privacy: ExcelinEd.org/Student-Data-Privacy
- **Future of Privacy Forum** has launched FERPA|SHERPA to provide service providers and other stakeholders easy access to those materials to help guide responsible uses of student's data: ferpasherpa.org
- **iKeepSafe** offers privacy assessments to provide vendors a method to demonstrate legal and regulatory compliance: iKeepSafe.org/Privacy
- **Privacy Technical Assistance Center (PTAC)** of the U.S. Department of Education serves as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student data: ptac.ed.gov/
- **Software & Information Industry Association**'s Education Technology Industry Network (ETIN) of the Software & Information Industry Association represents and supports developers of educational software applications, digital content, online learning services and related technologies across the K-20 sector: siia.net/Divisions/ETIN-Education-Technology-Industry-Network

Provide Users with Tools to Manage Student Data

While there are varied audiences for and users of educational products and services—educators, schools, parents and students themselves—many of the experts interviewed for this paper lamented the lack of settings that would allow responsible parties to directly manage the uses of data about students (and to do so in more fine-grained ways than completely opting out from participation). For his part, ensuring that there are appropriate controls and safeguards in handling student data is a priority for Clever's Bosmeny, who noted that "schools retain full ownership and control over their students data [in Clever].... Not enough companies are clear here. Schools own and control student data. Period."

CDT’s Bradshaw concurred, and in circumstances when it is appropriate encourages companies to extend the control of student data directly to parents. She said, “Sometimes it is more appropriate for a parent to have control. For example, for homework applications and other applications designed to be used outside of school. Being more thoughtful about how to implement parental controls would be really helpful.” Common Sense Media’s Fitzgerald would go even further, envisioning “vendors building into apps at the outset a student view to see data collected for and about them, so they could challenge and comment on it.” He continued, “Ironically, one of the things that is missing in the student data conversation is student voice… It is largely adults talking about student data but we tend to actually lose sight of the fact this is student’s information.”

Don’t Overlook the Security of Student Data in Your Products

Many would agree with Common Sense Media’s Fitzgerald who noted that the privacy and security risks that pertain to the collection and use of student data are often conflated. Still more would agree with him that “there is a very real risk that occurs when there is a data breach” and that it would be a mistake not to focus also on shoring up both the physical and technical security of educational products and services that handle student data.

While there is no shortage of advice and best practices available to those developing software applications and web services (beyond the education market), several high-profile media reports have specifically noted the insufficiency of the security features of online education products. As Natasha Singer of the *New York Times* explains in one 2015 article:

> *“While none of the security weaknesses appear to have been exploited by hackers, some technologists say they are symptomatic of widespread lapses in student data protection across the education technology sector. They warn that insecure learning sites, apps and messaging services could potentially expose students, many of them under 13, to hacking, identity theft, cyberbullying by their peers, or even unwanted contact from strangers.”*[viii]

Among the many aspects of what it takes to secure student data, Fitzgerald believes that greater use of encryption would be a huge step forward for many companies. “Just use SSL by default,” he offered. “It would be a huge win.” Even better, he suggested would be if the major app stores (such as those offered by Apple and Google) would “set a hard requirement that every app use a secure API [application program interface] to access and share data.” The ripple effect on the larger ecosystem—even beyond the products covered in those app stores—could be a significant step forward in ensuring the security of data collected about students.

Upgrade Your Privacy Policy

While it may be tempting to treat your privacy policy as a boilerplate compliance document that can be outsourced to devote more energy to product development, marketing and customer support, a company's privacy policy is fundamental to building trust with users and the public. As Clever's Bosmeny argued, "A privacy policy done well should be clear and reassuring. Done poorly it can be alarming to a lot of readers."

Experts interviewed for this paper described strong privacy policies as those that are clear and easily understandable ("not written for lawyers, but 'human readable'"), that highlight all of the ways in which a company ensures privacy of data is maintained, and that affirm a company's actual and routine (not aspirational) practices. As SIIA's Desetti explained, "What companies are doing needs to match their privacy policies. That is a big deal and companies need to be upfront about what their end users can expect with data collection and use." CDT's Bradshaw agreed, "Companies need to put themselves in their users' shoes and use common sense when deciding which policies to apply and when."

> "A privacy policy done well should be clear and reassuring. Done poorly it can be alarming to a lot of readers."
>
> **Tyler Bosmeny**
> CEO, Clever

Given that good products and services iterate over time based on success in the marketplace and user requests, including with respect to how they use student data, one of the challenges facing education companies is ensuring that their privacy policies remain up-to-date. One common strategy employed in privacy policies to cover this eventuality is a disclaimer that the policy may change at some point in the future. Such a disclaimer, while not uncommon, is hardly reassuring to some. "Think about that from a school's perspective," elaborated Bosmeny. "They select technology based on very specific privacy obligations. It makes no sense to ask that they agree to privacy practices that can change at a moment's notice." In response, Clever piloted an approach to making their privacy policy publicly available on a version control system (GitHub) that documents every change to their privacy policy over time. While this solution may not be suitable to every company serving education, nearly twenty companies have done so to date.[ix]

Communicate Your Commitment to Privacy of Student Data

The notion that parents and schools increasingly desire to see companies treat student data privacy as more than a compliance exercise is in and of itself a sign of changing times. That public communications, product marketing and customer support should also attend to data use and privacy practices, as the experts interviewed for this paper argued, reflects another aspect of how far the student data privacy issue has shifted over the last few years.

Why the calls for a better focus on communications? “When there is a lack of transparency, that is when people get nervous,” explained ReThink Education’s Walden. “It is always a good solution to create as much transparency about what your tool does and platform does.“ And, while many experts interviewed for this paper stressed that transparency was not a silver bullet solution for addressing privacy concerns, SIIA’s Desetti was quick to point out that “you can’t build trust on secrets.”

While communicating key information about the protections you have in place to protect student data is important, perhaps even more important is how that information is communicated. There is a need to focus first on helping educators and administrators understand how the use of student data can help schools better meet their students’ needs. “The companies that have been the most successful are ones where the use of data is perceived to be obvious and helpful to users,” explained Polonetsky of the Future of Privacy Forum. “If people are scouring your policy to understand what you are doing, you are already on the defensive.”

> “It is always a good solution to create as much transparency about what your tool does and platform does.”
>
> **Michael Walden**
> Partner, ReThink Education

Consider Signing the Student Privacy Pledge

“The [Student Data Privacy] pledge is part of what we believe is the most important strategy that companies can take in this privacy discussion, which is communication” said SIIA’s Desetti. Developed by the Future of Privacy Forum and SIIA to help effectively communicate with parents, teachers and education officials about how student information is used and safeguarded, the Student Privacy Pledge holds school service providers accountable to:

- Not sell student information;
- Not behaviorally target advertising;
- Use data for authorized education purposes only;
- Not change privacy policies without notice and choice;
- Enforce strict limits on data retention;
- Support parental access to, and correction of errors in, their children’s information;
- Provide comprehensive security standards; and,
- Be transparent about collection and use of data.

“This industry-led pledge to honor student data privacy is an important step in the right direction,” said Thomas Gentzel, executive director of the National School Boards Association. “Those vendors who opt to take the pledge are demonstrating their public commitment to responsible data practices in a manner that will help support school boards’ efforts to safeguard student privacy.” Over 250 companies have signed the pledge as of April 2016.[x]

Seek Out and Consider Supporting Other Third-Party Privacy Initiatives

While the Student Data Privacy Pledge is not the only third-party initiative to help companies to demonstrate and amplify their commitment to student data privacy, the Future of Privacy Forum’s Polonetsky noted there are “not a lot of efforts [overall] right now” compared to other sectors beyond education.

In addition to the aforementioned open-sourcing of privacy policies (championed by Clever and other like-minded companies), other notable efforts beyond the privacy pledge include those launched by iKeepSafe (which offers independent evaluations of company privacy policies and practices that result in an iKeepSafe designation as being ‘privacy approved’), Common Sense Media (which has begun working with school districts to pilot a standardized rubric for evaluating the privacy policies of education companies, including testing steps that schools can employ), and the Consortium for School Networking (which is working to help school districts communicate their commitment to student data privacy through the earning of a Trusted Learning Environment Seal).

Walden of ReThink Education agreed with Polonetsky, saying that “we are still at an early stage. The market just has to catch up to the access and innovations that are happening.” Nonetheless, he remains convinced that “the market will rise to meet the requirements.” When asked if he is worried that a focus on privacy competition might drive investors and companies away from the education market, he bluntly responded, “Education is a big enough market that folks will come and innovate.”

ROLES AND RESPONSIBILITIES FOR OTHERS IN BUILDING A TRUSTED LEARNING ENVIRONMENT

While education companies and service providers bear the primary responsibility for earning and maintaining the trust of educators, parents and students, it remains important to consider the roles and responsibilities of other actors in the ecosystem, such as investors, school districts themselves, and even philanthropists and foundations (which have undeniably played a role in shaping the marketplace and demand for new education tools and services). Indeed, the leadership of education service providers does not operate in a vacuum, and it would be a mistake to suggest that they alone can sufficiently address the range of issues surrounding the collection and use of student data.

Investors in Education Companies

Given the key role that private investors play in the education market—and especially in helping to bring new products and services to scale—they have the unique opportunity to play a constructive role in helping to address student data privacy issues. According to estimates by CB Insights, for instance, global education technology companies received investments of nearly $3 billion in 2015 alone across over 400 separate deals.[xi] This influx of investment dollars has helped to grow existing education companies and launch dozens of new, high profile ventures.

Two trends are driving the need for investor engagement in the issue.

First, the regulatory environment surrounding the collection and use of data about students is rapidly evolving and complex, with variations in regulations depending on the state in which companies do business and the age of students being served. Especially for those companies pursuing monetization strategies that are advertising-based or market direct to teachers as a free or "freemium" service, it is important to evaluate the degree of compliance with existing privacy regulations, as well as the potential future risk should new privacy-related laws or regulations be introduced.

> "In 2016, school districts care more than ever if the software [they are looking to purchase] will interoperate, how they approach privacy, and how they deal with security."
>
> **Tyler Bosmeny**
> CEO, Clever

Second, school districts—as purchasers of education products—are increasingly seeking information about how the companies they do business with handle student data privacy with the intent to factor that information into their purchasing plans. As Clever's Bosmeny notes, "In 2016, school districts care more than ever if the software [they are looking to purchase] will interoperate, how they approach privacy and how they deal with security. In the buyer's mind, these have gone from important to essential." SIIA's Desetti concurred, saying that privacy "should be at the top of investors' …lists. It is not going to go away [as an issue], and poor privacy practices and policies can lead to a poor reputation and a short lifespan for new companies. As technology is more integrated into the classroom, it will only become more important."

Experts interviewed for this paper suggested a number of productive steps investors could take in evaluating new deals or in supporting the leadership of companies in which they are already invested. Chief among these ideas is the notion that how a company treats student data privacy issues should be among the first considerations of any prospective investor. Walden of ReThink Education advised, "As an investor, know how your companies use data." By that, Walden means more than evaluating a company's privacy policies. "Hearing 'our lawyers built us one and we're good' doesn't make me feel good," he said.

Rather, Walden explained that it means learning about how the company "think[s] about it and how ingrained it is in how they work." This could mean evaluating data flows with company leadership, including understanding the need and use for personally identifiable data, as well as how data is secured.

Polonetsky of the Future of Privacy Forum suggested that investors ask company leadership to "put on the critic's hat and do an assessment from the point of view of someone who doesn't support it" to allay any potential concerns. While founders may not like the idea of seeing themselves questioned in that light, it is necessary should the company's commitment to privacy or security ever be questioned. Such assessments can be conducted by company leadership working with investors directly or by retaining third-party privacy and security experts hired by the investors to do such an assessment.

Educating company leadership on privacy and security issues, including the public policy context and perspectives of privacy advocates, is also a role that investors can and are playing. Why? "Startups don't have support on this," offered Walden, whose firm has run several privacy-focused "bootcamps" for emerging companies in partnership with the Future of Privacy Forum.

Should concern about how issues of privacy are handled in education give investors pause in making investments in the education market? Absolutely not, said many of the experts interviewed for this paper. While issues of privacy are challenging, Walden remains optimistic, in part because "most people are not in the education space, because it is the easiest place to get rich. People in this are really motivated by good things." And, as Bosmeny observed, there are "lots of exciting opportunities and no shortage of need."

School Leaders

While it may seem challenging in practice given the explosion of innovation in technology-based products and services to support teaching, learning and school operations, school leaders have the obligation to control access to data collected from and about their students' formal education activities. In so doing, schools and students should be protected from flagrant violations of privacy by providers (for instance, the unrestricted re-selling of data about the health status of young children to data brokers). At the same time, it is to be expected that schools will have different views and philosophies about what privacy needs their students have. "When it comes to areas where there is a legitimate range of views," explained the Future of Privacy Forum's Polonetsky,"[it]… should be the decision of parents and schools about how they want to implement."

School Capacity to Evaluate the Privacy of Education Technology Products

What responsibility should schools have to evaluate the privacy and security of the digital and online learning tools and services they offer or recommend to students? Many of the experts interviewed for this paper felt that a minority of schools were likely to have any sort of reasonable capacity to do so—regardless of what they feel their responsibility may be. "Given how thinly stretched our schools are, it may not make sense to always put decision making responsibilities on the school," explained the Center for Democracy & Technology's Bradshaw. "They may not always have the capacity to decide what EdTech privacy and security practices are acceptable." iKeepSafe's Hancock agreed, "It is hard for educators to see how they can fulfill their role. Schools are not equipped to do their own privacy assessments."

Compounding this issue is that many school districts grant teachers wide latitude in finding and using instructional tools to meet the needs of their students, including online tools and services. In so doing, school and district leadership may not necessarily be aware of every app or service being used with students. "How does the district or school building even know what the teachers are adopting?" Walden of ReThink Education asked. "Not having a good answer to this question feeds parent concerns."

While many of the practices and initiatives described in this paper will help schools to make informed choices about with whom to work, the Future of Privacy Forum's Polonetsky concluded that "the level of sophistication [in evaluating the privacy of online products and apps] is not there yet." As such, school leaders would benefit from good industry partners who take it upon themselves to proactively educate their customers (teachers and school leaders) about how they can play a productive role in protecting student data privacy.

School leaders would do well to have discussions with their educators and parents about the types of information and choices they would like to consider related to privacy when a new tool or app is considered for use in a school or recommended by an educator (including under what circumstances and how they can get further information). Ultimately, these discussions should lead to the development of privacy-related processes—reflecting local beliefs and values—that can be used in making procurement decisions and in communicating with potential service providers. Clever's Bosmeny noted that "2015 is when districts really started to step forward on this. We are hoping for broader adoption of these practices."

The development of new third-party privacy review sites and tools—such as those being developed, for instance, by Common Sense Media and iKeepSafe among others—offer to inform schools as they vet online tools and services. SIIA's Desetti agreed that such third-party reviews, especially those offering in-depth information to schools (as opposed to simple rankings), can be useful and are promising. At the same time, he emphasized that schools "can't outsource their responsibility" and that no one information source (whether a third-party review, the signing of the student data privacy pledge or the earning of a privacy seal) is likely to be wholly sufficient for school evaluation purposes.

Philanthropists

Experts interviewed for this paper suggested two primary ways in which foundations can play an important role in helping to build trust in the use of student data to improve teaching, learning and school operations: first, by supporting education and communication efforts related to privacy (both to the school and provider communities); and second, by establishing clear criteria for grantees—including researchers and program evaluators—for the use, privacy and security of student data.

Communications and education efforts—especially those undergirded by high-quality, balanced considerations of the privacy landscape—are vital. They can help build awareness and capacity among school district leaders, as well as among companies, concerning what guidelines exist and how best they can fulfill their respective roles. Such efforts could include the development of decision-making tools and rubrics, which also could be used to help educate parents about the positive examples of data use in schools that help to meet the individual needs of students.

In setting clear criteria for the use of student data by their grantees and in their own operations, foundations can serve to model the trust-building approaches that would help advance the sector. The Center for Democracy & Technology's Bradshaw sees value, if not also an obligation, for foundations to take this approach. She explained, "It is important for…[foundations] to articulate their standards and best practices regarding security and privacy as part of their investment decision." The Bill & Melinda Gates Foundation, Bradshaw noted, has articulated its data stewardship principles and applies those principles both to decision making in formulating grant investment decisions, as well as in decisions internal to foundation operations. [xii]

EMBRACE THE OPPORTUNITY

The pace of change we are experiencing at the intersection of technology innovation and education is staggering. "This is all very new," observed ReThink Education's Walden. "How we think about this is still evolving, and it is evolving much faster than anybody could have been prepared for." With such changes come opportunities to provide new and better services to support educators in helping students. The ability to personalize education to better meet the needs of individual students—and to empower students to pursue individual pathways uniquely suited to their strengths and interests—presents the chance to dramatically improve outcomes for large numbers of children and youth. The smart use of technology and data will help power this transformation.

At the same time, change also brings challenges, including building consensus for the guardrails and guidelines with respect to student data privacy. As such, there remains significant risk for service providers not working to build trust on issues of student data privacy. Chief among these risks is privacy advocacy that results in the passage of well-intentioned, but ham-handed policies that have the potential to slow the adoption of technology in education, erect barriers to promising practices that help at-risk students and impede innovation. The long-term implications for providers and education leaders are both serious and profound.

> "This is all very new. How we think about this is still evolving, and it is evolving much faster than anybody could have been prepared for."
>
> **Michael Walden**
> Partner, ReThink Education

As we move forward, it will be important for issues of school capacity to be addressed, but today putting too much control or responsibility solely in schools hands can be problematic. As the Center for Democracy & Technology's Bradshaw stated, "Companies need to take responsibility as well." Not only is this the right thing to do, Walden noted that companies are only "playing into paranoia if they don't engage." He continued, saying, "That is why a lot of the burden has to come back to us as investors and entrepreneurs. We have to take this seriously."

What is at risk is a new generation of valuable tools and services that can help students succeed, and the stakes are simply too high to remain seated on the sidelines.

NOTES

[i] Foundation for Excellence in Education, *Protecting K-12 Student Data Privacy in a Digital Age*. (Tallahassee, FL: Foundation for Excellence in Education, 2015). Available online at: http://www.excelined.org/student-data-privacy/

[ii] Aspen Institute Task Force on Learning and the Internet, *Learner at the Center of the Networked World*. (Washington, DC: The Aspen Institute, June 2014). Available online at: http://csreports.aspeninstitute.org/Task-Force-on-Learning-and-the-Internet

[iii] These and other ExcelinEd student data privacy resources can be found online at: http://www.excelined.org/student-data-privacy/

[iv] Experts interviewed for this paper include: Tyler Bosmeny (Clever), Alex Bradshaw (Center for Democracy & Technology), Brendan Desetti (Sofware & Information Industry Associaton), Bill Fitzgerald (Common Sense Media), Marsali Hancock (iKeepSafe), Andrew Joseph (Amazon Education), Jules Polonetsky (Future of Privacy Forum), and Michael Walden (ReThink Education).

[v] For context on current federal law and the unintended consequences of legislative proposals, see: *Protecting K-12 Student Data Privacy in a Digital Age*. (Tallahassee, FL: Foundation for Excellence in Education (ExcelinEd), 2015). Available online at: http://excelined.org/2015DataPrivacyWhitePaper/

[vi] Zeide, E., *19 Times Data Analysis Empowered Students and Schools: Which Students Succeed and Why?* (Washington, DC: The Future of Privacy Forum, March 2016). Available online at: https://fpf.org/2016/03/22/19-times-data-analysis-empowered-student-and-schools/

[vii] Cavoukian, A., *Privacy by Design: The 7 Foundational Principles*. (Ontario: Information and Privacy Commissioner of Ontario, 2011). Available online at: https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

[viii] Natsha Singer, "Discovering Security Flaws in Digital Education Products for Schoolchildren," *New York Times*, February 8, 2015. Available online at: http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html

[ix] See http://privacybychoice.github.io/ for an up-to-date list of companies who have open sourced their privacy policies, including links to each company's policy.

[x] See https://studentprivacypledge.org/ for more information on the Student Privacy Pledge, including endorsements and the current list of signatories.

[xi] See CB Insights, "Mega-Rounds Boost Global Ed Tech Funding To New Record," January 19, 2016. Available online at: https://www.cbinsights.com/blog/2015-global-ed-tech-funding/

[xii] See Bill & Melinda Gates Foundation, "Stewardship Principles to Protect Student Data Privacy." Retrieved on March 17, 2016 from: http://postsecondary.gatesfoundation.org/wp-content/uploads/2014/08/BMGF_DataStewardshipPrinciples_logo.pdf

ExcelinEd

Stay Connected

EXCELINED.ORG

FACEBOOK.COM/EXCELINED

@EXCELINED