September 12, 2019

The Honorable Richard Blumenthal
U.S. Senate
706 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Richard J. Durbin
U.S. Senate
711 Hart Senate Building
Washington, D.C. 20510

The Honorable Edward J. Markey
U.S. Senate
255 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senators Blumenthal, Durbin, and Markey:

We appreciate the letters you have written to the 50+ list of EdTech companies. We request that you consider adding the following companies to the list receiving a letter: Edsby (a Canvas competitor and Microsoft partner), Illuminate Education – School City, Horizon Software International – MyPaymentsPlus, Khan Academy, Buncee, Kahoot, and FlipGrid. Included in this letter is our personal story regarding student data privacy. The final two paragraphs of this letter provide recommendations for legislation.

Edsby's privacy policy appears to allow the transfer of data they collect and store as an asset in a merger or sale. Their data sharing agreement with our school district is concerning—its wording appears to place no limits on what can be collected on students. We also have concerns regarding how student intellectual property will be protected when it is shared or analyzed by third party EdTech vendors.

We have repeatedly requested our school district provide access to student record data shared, collected, and stored on our children with third party companies; to know the metadata associated with each data element collected, and to know all accounts (and passwords) the school district has created with third party companies using our children's identities. I have written Florida State Attorney General Moody, the Florida Department of Education Inspector General, Florida Department of Education Commissioners Stewart (with former Governor Scott on copy) and Corcoran (with State of Florida Representative Toledo and Senator Cruz on copy), and discussed with our Hillsborough County School Board representative, Dr. Hahn, and the Hillsborough County School District attorney, Mr. Gibson. We are consistently referred to the U.S. Department of Education or back our school district that has not provided the student data we have requested on our own children. We believe this student data is due to us under FERPA and Florida state law. The fact that we have not received this data from the school district, especially given the cybersecurity issues in the education sector, is shocking.

Even with state and federal laws protecting our rights to student data we have had no success exercising those rights. These laws seem unenforceable given the lengths we have gone to obtain this data. We have not been provided an inventory of accounts and passwords, or student data the school district shared or

allowed third parties to collect or create with analytics tools. As a result, we are unable to ensure our children's accounts are secured with strong passwords. We are unable to review complete student data for accuracy; a task that might be impossible given the number of data elements collected. When inaccurate quantitative or qualitative student data exists then risks to a child's future opportunities exist, especially if bad data were used for scoring in a university admissions or employment process.

In other areas of our lives we might consider these actions a form of identity theft, yet when schools perform these actions it is considered legitimate. I ask you, what rights effectively exist for parents to protect the identities and safety of their children when they cannot prevent the personal and private (and sometimes medical) information about their own children from being spread around to countless privately or publicly owned companies based in or out of country? Companies who may then share that student data (de-identified) with partners or researchers. In cases where that de-identified data is re-identified, one cannot reasonably assume the student data was protected at all.

One password created by our school district that we have seen (on an account we are aware of) was very weak and in violation of basic password security rules. Authentication policies appear insufficient, resulting in at least one teacher authenticating a student and creating another very weak student password. It appears the district fails to track or approve apps used in each classroom, creating more unknowns for parents who have a responsibility to protect our children and their identities. We discovered Alexa was pre-installed on devices in at least one classroom, and was inadvertently activated during a classroom discussion. How much data was collected on our child when Alexa was listening in the background? We do not allow Alexa or other voice activated devices in the home, why are our children subjected to this surveillance in public school when we diligently protect them at home?

We specifically requested the district provide our student data from two particular companies, Edsby and Curriculum Associates. Our requests to opt out of these platforms were denied. Our request to have our students' names removed from Edsby was denied. This process began over a year ago, and I have spent countless hours, nights and weekends educating myself on our rights, the law, making fruitless calls, and working to get this information from our school district. We have been forced into homeschooling to limit the access EdTech companies have to our children's data, and personally this has resulted in my having to turn down a part time job due to the time commitments of homeschooling.

The act of a district sharing our children's identities and personal data with third party companies that often collect additional unspecified personal information creates a security nightmare for parents. Even if we knew who all of these third parties are, we cannot possibly assess the security of each system and each company's policies and business practices to ensure our children and their personal data are well-protected. Rather than consolidating data in one place with one entity (the school district) to be secured, student data is being spread around to so many EdTech companies and cloud-based platforms that I cannot imagine how one school district could feasibly or practically inspect every one of these EdTech third parties for the security of their systems, software platforms, administrative procedures, partner sharing practices, de-identification (anonymization) procedures, etc.

Student data is attractive. A recent article out of the Omaha World-Herald, *NU faces 'very real' cyber threat: 9.94 million attacks blocked daily*, explains University of Nebraska blocks as many as 9.94 million cyberthreats daily. If one university faces this threat level what are each and every one of these EdTech companies facing in terms of daily cyberthreats, how secure is the student data, and do the countless companies with access to our childrens' student data even know each time they are breached?

It would not be irrational to assume our children's personally identifiable information (PII) is being siphoned off the grid and monetized somewhere amongst the plethora of EdTech companies that have been provided access to our children and their personal information without our consent.

The U.S. Department of Education must reinstitute the parental consent requirement in FERPA. It seems that relaxing the parental consent requirement allowed an industry of student data compilers to blossom and created a potential treasure trove of data on minors for hackers or those with monetary interests to misuse.

There is little knowledge or training in some school districts about FERPA, COPPA, or PPRA. There appears to be a lack of oversight regarding how contracts and agreements with third party EdTech companies are carried out and a lack of transparency regarding what is happening with student data. I believe this is putting children's privacy and safety at serious risk.

School districts that share student data with third parties, for any purpose, should be required to employ a full time credentialed CyberSecurity and Student Privacy Expert. Each state should have a Medical and Education CyberSecurity and Privacy Commissioner. School districts must be required to train all employees in FERPA, COPPA, and PPRA. Each state must have a complaint and resolution process for medical and student privacy violations, and an actionable process for data breach reporting from anonymous citizens. All data breaches, not only those above a *number of victims* threshold, should be reported expeditiously so those impacted can take appropriate steps to protect victims.

Finally, and most important, the parental consent requirement must be reinstated in FERPA, requiring parental consent prior to a school district sharing student data (regardless of third party designation as a school official or other like designation), giving parents back the ability to protect their own children. Without the parental consent requirement the individual privacy of our children looks bleak. When government or corporations know nearly everything personal about an individual, it becomes easy to manipulate and silence those citizens; this sort of environment does not work in the favor of freedom, the good, or the just.

Sincerely,

Cathryn Moering

CC:

The Honorable Ron DeSantis
Office of the Governor
State of Florida
The Capitol
400 S Monroe St
Tallahassee, FL 32399

The Honorable Rick Scott
U.S. Senate
716 Hart Senate Office Building
Washington, DC 20510

The Honorable Marco Rubio
U.S. Senate
284 Russell Senate Office Building
Washington, DC 20510