Testimony and Statement for the Record of

Amelia Vance
Director of Education Privacy
Future of Privacy Forum

Hearing on "Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe"

Before the

House Committee on Education and the Workforce

May 17, 2018

The Future of Privacy Forum
1400 I St. NW Ste. 450
Washington, DC 20005

www.fpf.org

On behalf of the Future of Privacy Forum, thank you for inviting me to testify today. My name is Amelia Vance, and I am FPF's Director of Education Privacy. FPF commends Chairwoman Foxx, Ranking Member Scott, and this Committee for holding this hearing to examine how schools and states are working to ensure that data and technology can be used as tools to help students succeed while also protecting privacy.

FPF is a non-profit organization focused on consumer privacy issues, including issues impacting students, parents, teachers, and others with a stake in the protecting education data. We primarily equip and convene key stakeholders to find actionable solutions to the privacy concerns raised by the speed of technological development. FPF's education privacy project works to ensure student privacy while supporting the technology use and innovation in education that can help students succeed. Among other projects, FPF maintains FERPA|Sherpa,[1] a website compiling education privacy resources with sections for parents, schools, ed tech, and other stakeholders; and we are the co-founders - with the Software and Information Industry Association - and gatekeepers of the Student Privacy Pledge, a voluntary, legally enforceable code of conduct for ed tech companies.[2] Now with nearly 350 companies as signatories, the Pledge is designed to both raise awareness of best practices and facilitate their implementation.

In recent years, the day-to-day experience of students has dramatically shifted; in FPF's 2016 survey,[3] ninety percent of parents said their child is using school-provided technology. Numerous surveys indicate overwhelmingly parental support for the proposition that ed tech can and has improved how their child learns.[4] When properly used and implemented, technology and data in education can close learning gaps in the classroom and be a powerful tool in fulfilling the great promise of high quality education for every student in America. Often, ed tech companies are founded by parents or former educators who noticed a gap in their own child or former students' educational resources and want to provide a solution to achieve the goal of helping every student succeed.

Many classroom technologies rely on collecting and using data about students. Trust is therefore key for the adoption of innovative technology in the education space. A majority of parents in our survey said that they had security and privacy concerns, worrying about both potential breaches of information and ways that data could be used to narrow, rather than broaden, their child's opportunities.[5] Ed tech solutions cannot succeed if schools, teachers, and parents believe that technology vendors cannot be trusted to protect that information or are motivated by monetizing student data. Leading ed tech actors recognize the necessity of building trust with administrators and parents, and prioritize trust in how they build their products, and make their practices understandable and accessible. Schools and the companies that serve them are attempting to strike a balance: how to use data and technology tools to deliver the best educational experience for each and every child while ensuring that student privacy is protected. To complicate this balancing act, companies are not always

---

[1] FERPA|Sherpa, https://ferpasherpa.org/.
[2] Student Privacy Pledge, http://studentprivacypledge.org/.
[3] Parents Support School Tech and Data, But Want Privacy Assurances, Future of Privacy Forum, https://fpf.org/2016/12/08/2016-parent-survey/.
[4] Seventy-one percent of parents said that "school tech has improved the quality of education." *See* Grading Tech, Marketplace.org, http://cms.marketplace.org/sites/default/files/grading-tech-infographic-2.jpg; Eighty-eight percent of parents in the Learning Assembly's 2016 Annual Survey said that they believed ed tech could have a positive impact in helping their child learn. *See* Public School Parent Poll, Learning Assembly, https://innovationassembly.files.wordpress.com/2016/10/learning_assembly_national_survey_results.pdf.
[5] Beyond One Classroom: Parental Support for Technology and Data Use in Schools, Future of Privacy Forum, https://fpf.org/wp-content/uploads/2016/12/Beyond-One-Classroom.pdf at p.10.

equipped to understand the complex regulatory regime surrounding student privacy, which can strain their relationships with schools.

So what does this look like on the ground? There has been a monumental shift in the student privacy legal landscape. That shift has largely come in the states. Since 2013, 39 states have passed 119 bills surrounding student privacy.[6] Many of those laws go beyond FERPA's regulation of schools and states to also directly regulate ed tech companies.

The focus of my testimony today will be on innovative practices that help companies, schools, and states protect student privacy, as well as the challenges and opportunities that stakeholders face when supporting appropriate use of educational technologies while safeguarding privacy. There are still improvements that can be made and some companies - particularly new start-ups entering the space - may not be aware of student privacy laws and best practices. At the same time, many companies are going above and beyond to protect student privacy. Sometimes this occurs when companies work with states and districts to protect students' privacy is ways that go above and beyond legal compliance. Sometimes companies take measures to increase transparency and make it easier for parents, educators, and administrators to understand how they use and protect data. And many companies have adopted internal measures to ensure that their employees and subcontractors keep data safe.

Leading ed tech vendors routinely help schools and municipalities ensure compliance with new state laws. For example, LearnPlatform, an edtech management app based in North Carolina, is being used by school districts to inform teachers about which educational apps have been approved for classroom use and notifies parents as to what technology is being used in the classroom. States like Connecticut and Utah use LearnPlatform to ensure that parents, teachers, administrators, and students know which products and tools comply with state and federal student privacy laws.

Some state student privacy laws, such as the Florida[7] and New York[8] statutes, require districts to list all ed tech programs being used, which can be a challenging and often impractical task - after conducting compliance audits, some large districts have discovered that they are using more than 50,000 apps and websites. The start-up CatchOn allows those districts to monitor their networks to see not only which apps and websites are being used on every district owned device, but also how often they are used, so districts can make informed decisions about which apps to use or forbid. All of this scanning is done without CatchOn seeing identifiable student data.

Connecticut has one of the strictest state laws, requiring a written contract with mandatory terms between local boards of education and any company that receives student information.[9] Connecticut school districts have struggled to negotiate compliance with companies that, in some cases, may only be providing software to one or two special education students. In response, the Connecticut Commission for Educational Technology stepped up to help districts comply with the law and negotiate with companies. Just last week, Connecticut announced that two of its largest education vendors, Microsoft and PowerSchool, a learning management application, signed Connecticut's model privacy contract addendum, making it easier for districts to help their students succeed. Doug Casey, the leader of this initiative, in particular praised Microsoft, noting that they were "the first major

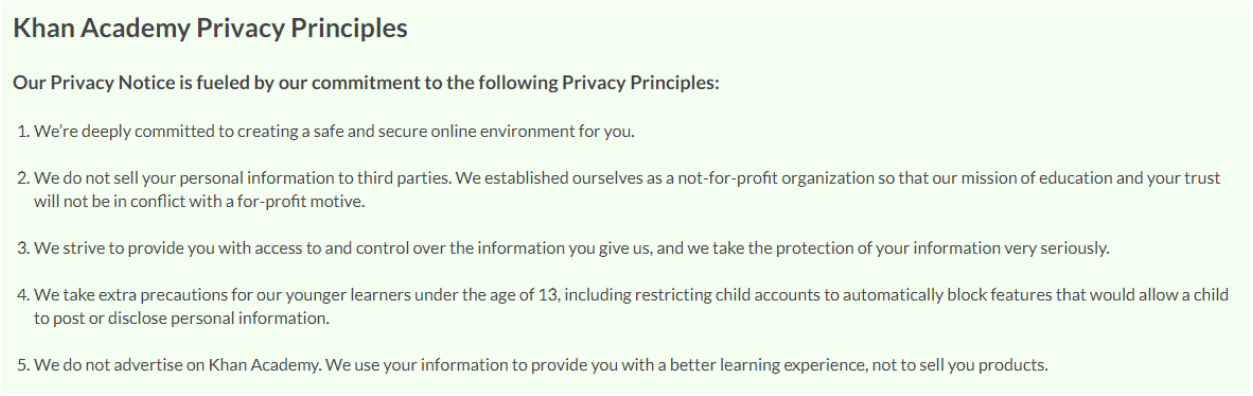
[6] State Student Privacy Laws 2013-2017, FERPA|Sherpa, https://ferpasherpa.org/state-laws/.
[7] Florida XLVIII § 1004.055, http://leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=1000-1099/1004/Sections/1004.055.html.
[8] New York EDN § 2d, https://codes.findlaw.com/ny/education-law/edn-sect-2-d.html.
[9] Connecticut § 10-234aa – dd, https://www.cga.ct.gov/2017/pub/chap_170.htm.

educational technology company to engage quickly with us. They went so far as to update their core Terms of Service to reflect our state's requirements, not just creat[ing a special privacy] addendum."[10]

These are not isolated examples: the Student Data Privacy Consortium,[11] founded by Cambridge Public Schools in Massachusetts and now present in seventeen states, has had over 600 companies sign the California Student Data Privacy Agreement.[12] A former district Educational Technology Specialist who helped form the California chapter of the Consortium told me that some companies have proactively reached out to negotiate and sign an agreement that all districts can then adopt. This has eased the administrative burden of California's student privacy law, which requires that districts vet and have signed student privacy agreements with ed tech companies.[13]

As I mentioned above, FPF reviews the relevant policies of each new company that applies to join the Student Privacy Pledge. One leading challenge is that privacy policies can be just as complicated for companies to write as they are for individuals to read. We often see cookie-cutter policies and standard legalese that is aimed at covering a company's liability rather than clearly communicating their data and privacy practices. These policies are commonly accompanied by statements, like "we reserve the right to change this policy at any time, and we will notify you by posting the date of revision at the top of this policy." Schools need to be able to quickly and easily evaluate a product's privacy policy, and some state student privacy laws require that companies have information on their websites about how they use and protect student data.

Leading companies have made this especially easy for schools. Khan Academy, an education video provider, has "Privacy Principles" at the top of their privacy policy so readers can quickly and easily understand the website's privacy protections and commitments (see Image 1[14]).



Khan Academy Privacy Principles

Our Privacy Notice is fueled by our commitment to the following Privacy Principles:

1. We're deeply committed to creating a safe and secure online environment for you.
2. We do not sell your personal information to third parties. We established ourselves as a not-for-profit organization so that our mission of education and your trust will not be in conflict with a for-profit motive.
3. We strive to provide you with access to and control over the information you give us, and we take the protection of your information very seriously.
4. We take extra precautions for our younger learners under the age of 13, including restricting child accounts to automatically block features that would allow a child to post or disclose personal information.
5. We do not advertise on Khan Academy. We use your information to provide you with a better learning experience, not to sell you products.

Image 1

ClassDojo, a classroom communication app, has a plain-English translation of their privacy policy, and also frames its policy as Q&A, making it easy for schools and parents to find answers to privacy questions (see Image 2[15]). ClassDojo also lists every sub-contractor they use, and a short description of why they use them.[16]

---

[10] Thank you to Doug Casey, Executive Director at the Connecticut Commission for Educational Technology, for sharing this example.
[11] Student Data Privacy Consortium, https://secure2.cpsd.us/a4l/.
[12] California Student Data Privacy Agreement, https://secure2.cpsd.us/cspa/agreements/CSDPA_Final_V1_Overview_022717.pdf.
[13] Thank you to Dana Greenspan, former Educational Technology Specialist for Ventura Office of Education and current contractor for the California Student Privacy Alliance, for sharing this example.
[14] Khan Academy Privacy Notice, https://www.khanacademy.org/about/privacy-policy.
[15] Privacy Policy, ClassDojo, https://www.classdojo.com/privacy/.
[16] Third Party Service Providers, ClassDojo, https://classdojo.zendesk.com/hc/en-us/articles/203732189.

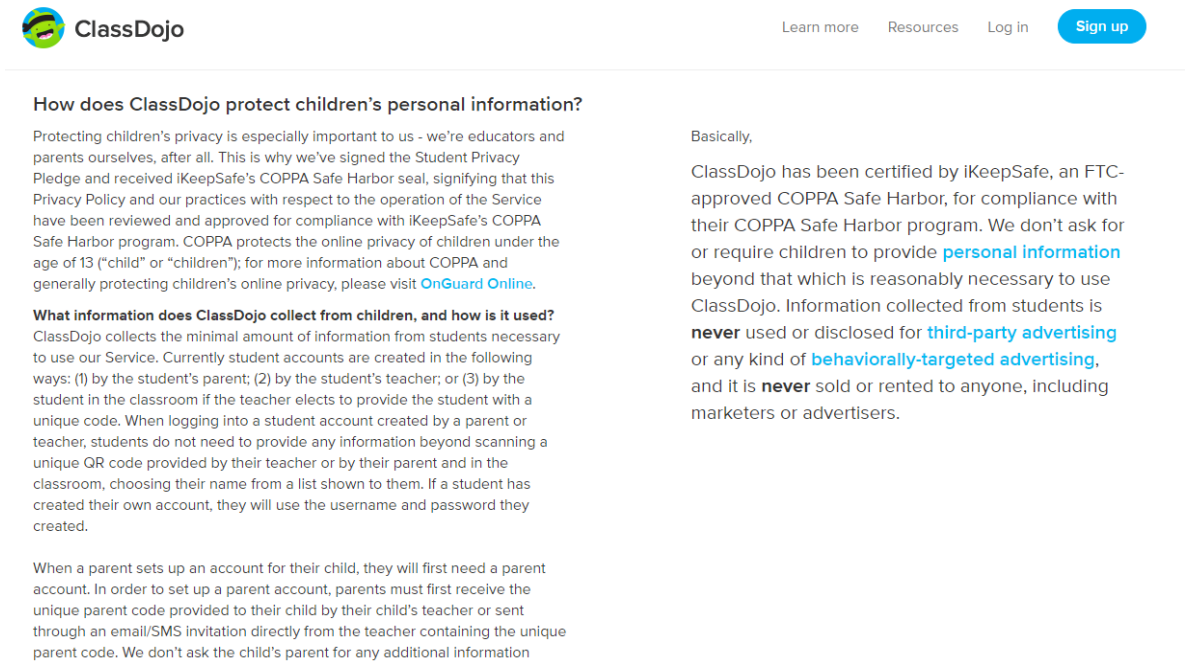


Image 2

Teachers and administrators need to be able to find, use, and explore the efficacy of technology that can help personalize learning, but students also need to have their data protected, and be given the freedom to intellectually explore. Leading companies have stepped up to aid schools in achieving this balance and building trust. For example, Apple's Classroom app, used to help teachers manage student iPad devices, has a number of privacy protections built in (see Image 3[17]). Teachers can only view a student's screen while the student is in their close proximity, and the student is alerted when their teacher is actively viewing their screen. Schools may also disable this feature completely if they determine it is unnecessary.

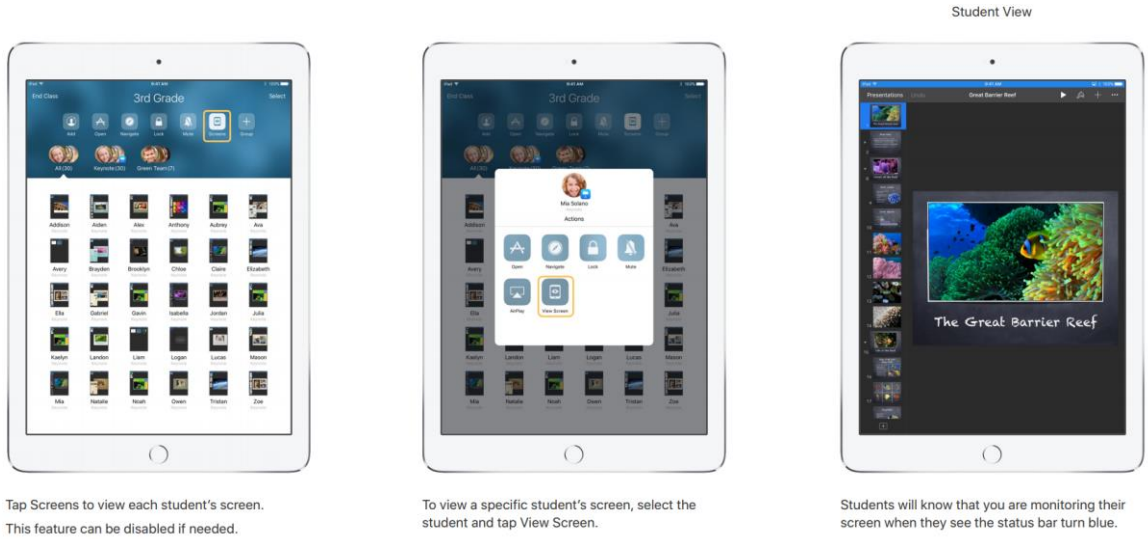


Image 3

[17] Getting Started With Classroom 2.0, A Teacher's Guide to the Classroom App for iPad, Apple, http://images.apple.com/education/docs/getting-started-with-classroom-2.0.pdf?linkId=36150220.

Leading companies - even when their products are not primarily directed at the education market - have stepped up to help districts address privacy concerns. AngelSense, a GPS tracking device marketed largely to parents of autistic children, has a "listen in" feature that allows parents to hear what is going on around their child. This obviously raises privacy concerns when the device is being used in school. AngelSense worked with a district in New Jersey to create an agreement disabling the "listen in" feature during school hours while still allowing parents retain the essential GPS capability. The company then allowed the district's lawyer to share their agreement with the more than 3000 members of the Council of School Attorneys, benefiting districts across the country.[18]

Finally, it is crucial that companies ensure their own internal practices enhance privacy. "Everyone who has access to students' personal information should be trained and know how to effectively and ethically use, protect, and secure it."[19] Both in districts and at companies, human error is the most like cause of security breaches and privacy violations.[20] To combat this, companies like eScholar, an education data management software provider, and the National Student Clearinghouse, an enrollment and degree verification service, have annual training for all of employees. Clever has implemented an annual audit of their privacy policy to ensure compliance with new developments in state and federal privacy law.

Leading companies have gone beyond industry security standards to implement technical measures to ensure data is kept safe, bolstering contractual and legal requirements. For example, Teachley, a math games app, routinely refreshes identifiers used in the company's games to ensure that, if information were breached or if authorized third parties attempted to use information for an unapproved purpose, users could not be tracked over time or across applications. Knewton, an adaptive learning platform employs unique identifiers to provide support to users while shielding user identity from tech support personnel; this safeguard would also mitigate the risk of reidentification of users if the information were ever breached. Other companies, like D2L, a cloud software company, have obtained internationally recognized security certifications.[21]

Despite these encouraging examples, there is still a lot of work to be done. Many companies are still struggling to understand and fulfill their privacy obligations. While none of the companies I highlighted above are perfect, all recognize the need to build trust and help schools and states through the difficulty of interpreting not only FERPA, but also brand new state privacy laws and district policies. In particular, while the U.S. Department of Education's Privacy Technical Assistance Center has provided incredible guidance and resources since its founding in 2011, more guidance and funding is needed to help reach all schools, states, and companies. Actions like holding this hearing helps elevate student privacy in the mind of every school leader and ed tech CEO, and I hope these conversations continue.

---

[18] Thank you to David Rubin, Attorney at Law, David B. Rubin, P.C., for sharing this story.
[19] Student Data Principles, http://studentdataprinciples.org/.
[20] According to Verizon, 63% of confirmed data breaches involve leveraging weak, default or stolen passwords. 2016 Data Breach Investigations Report, Verizon, http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf; A report by Baker Hostetler indicated that human error was involved in approximately 60% to 70% of data breaches. 2018 Data Security Incident Response Report, Baker Hostetler, https://f.datasrvr.com/fr1/518/85193/2018_BakerHostetler_Data_Security_Incident_Response_Report.pdf; Some observers have estimated that nearly three quarters of breaches are caused by human error. Data Breaches: Leading Cause & How to Avoid Them, Medium Corporation, https://medium.com/blue-bite/data-breaches-leading-causes-how-to-avoid-them-797e3d51b1b1. The conclusion was 73%.
[21] Security Certifications and Compliance, D2L, https://www.d2l.com/security/certifications/.