STATEMENT OF ALLYSON KNOX

DIRECTOR OF EDUCATION POLICY AND PROGRAMS

MICROSOFT CORPORATION

BEFORE THE

EDUCATION AND THE WORKFORCE COMMITTEE

SUBCOMMITTEE ON EARLY CHILDHOOD, ELEMENTARY, AND SECONDARY EDUCATION

UNITED STATES HOUSE OF REPRESENTATIVES

"HOW EMERGING TECHNOLOGY AFFECTS STUDENT PRIVACY"

FEBRUARY 12, 2015

Thank you, Chairman Rokita and Ranking Member Fudge, and all the Members of the Subcommittee for inviting me to testify today. My name is Allyson Knox. I am the Director of Education Policy and Programs at Microsoft Corporation.

I am pleased to have this opportunity to discuss student privacy. Specifically, I will discuss what technology companies such as Microsoft are doing to protect student privacy while providing services that help children learn; discuss why federal law is out of date; and suggest solutions that we believe should be considered by policymakers to better protect student privacy and encourage the use of safe and beneficial technologies in schools.

Over the past year, revelations of government surveillance, highly publicized data breaches, and other stories of personal data being used inappropriately have dominated the media. These stories have prompted many parents and students to think much harder about the data collected by schools, including the extent to which it is being gathered and protected. Parents have grown concerned that student data is being used to target advertising to students.

These concerns are reflected in a growing number of recent surveys of parents. For example, a survey by the Benenson Strategy Group on behalf of Common Sense Media found that 90 percent of respondents were "concerned about how private companies with non-educational interests are able to access and use students' personal information" and 77 percent support making it "illegal for schools and education technology companies to sell students' private information to advertisers."

With this in mind, companies like Microsoft that provide education technology continue to work to effectively meet both education objectives as well as privacy and safety expectations.[1]

[1] Microsoft's approach to the trustworthy cloud includes important investments in privacy that reinforce the principle that enterprises own their data, even when stored in the cloud.

For several years, schools have been increasingly bringing technology into the classroom because it transforms education, enables personalized instruction and helps children learn. Schools will save money and always have the latest technology if they use “cloud” based services rather than maintaining and updating their own on-site servers. Cloud computing takes advantage of massive and efficient data centers operated by third party providers. This means instead of storing all data on a local computer, teachers and students can log into their cloud services and access their documents and communications anywhere from almost any device. More importantly, cloud services offer benefits to help teachers and students be more efficient and more productive, and to enable learning anytime and anywhere.

Technology in the classroom has resulted in the creation and collection of much more data than ever before. For example, while previous generations relied solely on a paper report card to gauge student performance periodically during the year, today’s technology allows parents and teachers to monitor a student’s progress continuously on a password protected website throughout the school year. And while teachers in the past relied on in-person parent conferences to discuss sensitive issues such as learning disabilities or medical conditions, parents and educators today often discuss these issues via email.

As these examples illustrate, the use of technology and the collection of data about students presents tremendous opportunities to help evaluate student progress in real time and provide instruction that is tailored to a particular student’s unique strengths, weaknesses and learning style. However, it also raises serious privacy concerns, and it is important that appropriate safeguards are in place to protect the privacy of this information, and similarly, that some uses of that information, such as to target advertising to students, are appropriately limited. That is why it is so important that when technology companies are invited into the classroom and entrusted with sensitive information about schoolchildren, parents, educators and school leaders should have confidence that those same companies will act as responsible stewards of that information.

We believe that the new opportunities enabled by technology require thoughtful evaluation and responsible and comprehensive approaches that allow our children to learn with technology in an engaging, safe and respectful manner. Misleading, exploitative, or aggressive advertising practices simply do not belong in the classroom.

Microsoft was one of the first companies to recognize the need to treat sensitive student data in the same way that we treat other customer data, such as government, health or financial services data. Microsoft has long understood that in order for our customers to trust us with their sensitive information, be it health data, government data, financial services data or student data, they need to trust us to do the right thing. That is why from the start, we baked privacy as a core ingredient into our education products. With these products we have publicly committed to "not mine your data for advertising purposes."[2]

Federal Policy

Current Federal law does not adequately protect students from practices such as targeted advertising based on student data that is collected by, stored in or transmitted through most third party operated cloud services. This is because the primary federal law focused on protecting student privacy, the Family Educational Rights and Privacy Act or FERPA, no longer reflect the reality of today's education system and the explosion of new technologies that are being used.

That should come as no surprise since FERPA was enacted in 1974, when the Xerox machine and the electric typewriter were cutting edge technologies, pocket calculators were brand new, and the Internet, cell phones and laptops did not exist, to say nothing of cloud computing.

[2] *E.g.,* http://products.office.com/en-us/business/office-365-trust-center-cloud-computing-security

In 1974, student data was collected and stored the old fashioned way: A teacher sent a form home with the student. The parent filled out the form and sent it back to the school with the child. The student handed the form to their teacher. The teacher handed the form to the principal. The principal handed the form to an assistant. And the assistant put the form in a folder, which also might contain sensitive information about the student's grades and disciplinary actions. The folder was placed in a filing cabinet that might be locked and most likely never left the school office.

The world of information storage and sharing has certainly changed. In almost all schools, information about a student is stored digitally on PCs, tablets, servers or memory sticks. In most schools, information about the student can be accessed through the school district's intranet or through the open Internet. The data is portable and often is not deleted when the student graduates from high school. Furthermore, the data is oftentimes maintained by service providers far beyond the classroom walls.

Given these facts, it leads to the obvious question: how could a law written in 1974 meet the needs of today's students? The answer seems quite clear: it cannot. Specifically:

- FERPA has not kept pace with new technologies such as cloud email and storage, and many have questioned what may or may not be within FERPA's reach. As a result, some have concluded that FERPA applies to cloud-based email for faculty *but not students* and that FERPA doesn't apply to most third party online courses. FERPA would benefit from an update to reflect these new types of technologies that students and teachers use.

- FERPA was written such that its reach and primary sanction apply only to educational institutions and not private third party service providers. FERPA should also be updated to incorporate express limitations on third parties regarding certain uses of protected student information, such as the use to target advertising or to build profiles for use in advertising to students in the school setting or once they leave school.

- Use of FERPA by regulators to drive better practices in schools and among third party providers has also been challenging since FERPA's primary sanction is the denial of federal funds to schools. Many have suggested that this penalty is too draconian or schools and provides no incentive for third parties to improve data privacy practices.

The time has come to do the difficult work of revising this law to bring it into the 21st century.

State Policy

In the absence of Federal action to update FERPA, states have taken this issue into their own hands and are passing laws to provide safeguards to student data that is collected and maintained by third-party service providers.

The Data Quality Campaign (DQC), a non-profit which closely tracks state student privacy legislation, found that in 2014, 28 bills explicitly addressing the safeguarding of education data were passed in 20 states. This focus on privacy is not slowing down. DQC found that as of just last week, 102 privacy bills have already been introduced in 32 states this year.

Microsoft has also been aware of many of these state initiatives and has often provided comments and supportive feedback to state legislators. That said, we believe it would be beneficial to have uniform rules to protect the privacy of every student across the country, and consequently, we would support the creation of a single, uniform set of rules to address this issue.

Student Privacy Pledge

Microsoft and other technology companies have also moved forward on their own to set a higher standard for protecting student data. On October 7, 2014 Microsoft was among the 14

original signatories of a voluntary and comprehensive industry Pledge about how participating companies will protect student privacy. Today the Pledge has grown to over 100 signatories.

More specifically in the Student Privacy Pledge, school service providers promise 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
- Be transparent about collection and use of data

Microsoft and Partners Address Student Privacy Issues Together

The Pledge has been influential and beneficial, but Microsoft believes that more should be done. It is for this reason that Microsoft has worked closely with key national education associations to help inform and educate schools, parents and other key stakeholders about how to protect student data.

For example Microsoft co-published with the Consortium for School Networking (CoSN) a professional association for district technology leaders, the "Protecting Privacy in Collected Learning" online toolkit. The toolkit is an in-depth, step-by-step guide for school district leaders to navigate federal privacy issues and provide suggested practices for school IT administrators that reach beyond compliance to include checklists, examples, and key questions to ask.

Microsoft has also partnered with is the National School Boards Association's (NSBA) Council of Student Attorneys (COSA) and co-published the "Data in the Cloud: A Legal and Policy Guide for

School Boards on Student Data Privacy in the Cloud Computing Era." The guide responds to the numerous laws that potentially govern student data privacy and the guide helps district leaders to ask the right questions and understand potential problems.

Another key partner that Microsoft works closely with is the National Parent Teacher Association (NPTA) that is also providing testimony today. I have talked with many national and state PTA leaders about issues and concerns they have about student privacy from over twenty states. Last December the NPTA and Microsoft organized a two day training for a group of state PTA volunteer advocates to learn more about the complexity of protecting students' data. Our work with the PTA has shown us that this is an issue of vital importance to parents, and they have been leading the way at the state level to bring education privacy laws into the 21st century.

Conclusion

Again, I appreciate the opportunity to be here today and I look forward to working with you on this important issue.