HOW EMERGING TECHNOLOGY AFFECTS STUDENT PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON EARLY CHILDHOOD, ELEMENTARY, AND SECONDARY EDUCATION

COMMITTEE ON EDUCATION AND THE WORKFORCE

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

HEARING HELD IN WASHINGTON, DC, FEBRUARY 12, 2015

Serial No. 114–2

Printed for the use of the Committee on Education and the Workforce

Available via the World Wide Web:
www.gpo.gov/fdsys/browse/committee.action?chamber=house&committee=education
or
Committee address: *http://edworkforce.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

93–208 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON EDUCATION AND THE WORKFORCE

JOHN KLINE, Minnesota, *Chairman*

Joe Wilson, South Carolina
Virginia Foxx, North Carolina
Duncan Hunter, California
David P. Roe, Tennessee
Glenn Thompson, Pennsylvania
Tim Walberg, Michigan
Matt Salmon, Arizona
Brett Guthrie, Kentucky
Todd Rokita, Indiana
Lou Barletta, Pennsylvania
Joseph J. Heck, Nevada
Luke Messer, Indiana
Bradley Byrne, Alabama
David Brat, Virginia
Buddy Carter, Georgia
Michael D. Bishop, Michigan
Glenn Grothman, Wisconsin
Steve Russell, Oklahoma
Carlos Curbelo, Florida
Elise Stefanik, New York
Rick Allen, Georgia

Robert C. "Bobby" Scott, Virginia
Ranking Member
Rubén Hinojosa, Texas
Susan A. Davis, California
Raúl M. Grijalva, Arizona
Joe Courtney, Connecticut
Marcia L. Fudge, Ohio
Jared Polis, Colorado
Gregorio Kilili Camacho Sablan,
Northern Mariana Islands
Frederica S. Wilson, Florida
Suzanne Bonamici, Oregon
Mark Pocan, Wisconsin
Mark Takano, California
Hakeem S. Jeffries, New York
Katherine M. Clark, Massachusetts
Alma S. Adams, North Carolina
Mark DeSaulnier, California

Juliane Sullivan, *Staff Director*
Denise Forte, *Minority Staff Director*

SUBCOMMITTEE ON EARLY CHILDHOOD, ELEMENTARY, AND SECONDARY EDUCATION

TODD ROKITA, Indiana, *Chairman*

Duncan Hunter, California
Glenn Thompson, Pennsylvania
Dave Brat, Virginia
Buddy Carter, Georgia
Michael D. Bishop, Michigan
Glenn Grothman, Wisconsin
Steve Russell, Oklahoma
Carlos Curbelo, Florida

Marcia L. Fudge, Ohio,
Ranking Minority Member
Susan A. Davis, California
Raúl M. Grijalva, Arizona
Gregorio Kilili Camacho Sablan,
Northern Mariana Islands
Suzanne Bonamici, Oregon
Mark Takano, California
Katherine M. Clark, Massachusetts

C O N T E N T S

HOW EMERGING TECHNOLOGY AFFECTS STUDENT PRIVACY

Thursday, February 12, 2015
House of Representatives,
Subcommittee on Early Childhood, Elementary,
and Secondary Education,
Committee on Education and the Workforce,
Washington, D.C.

The subcommittee met, pursuant to call, at 11:15 a.m., in Room 2175, Rayburn House Office Building, Hon. Todd Rokita [chairman of the subcommittee] presiding.

Present: Representatives Rokita, Thompson, Carter, Bishop, Grothman, Russell, Curbelo, Fudge, Davis, Bonamici, and Clark.

Also present: Representatives Kline, Messer, Scott, and Polis.

Staff present: Lauren Aronson, Press Secretary; Janelle Belland, Coalitions and Members Services Coordinator; Nancy Locke, Chief Clerk; Daniel Murner, Deputy Press Secretary; Krisann Pearce, General Counsel; Jenny Prescott, Legislative Assistant; Mandy Schaumburg, Education Deputy Director and Senior Counsel; Alissa Strawcutter, Deputy Clerk; Tylease Alli, Minority Clerk/Intern and Fellow Coordinator; Austin Barbera, Minority Staff Assistant; Jacque Chevalier, Minority Senior Education Policy Advisor; Eamonn Collins, Minority Education Policy Advisor; Denise Forte, Minority Staff Director; Melissa Greenberg, Minority Labor Policy Associate; Christian Haines, Minority Education Policy Counsel; Ashlyn Holeyfield, Minority Education Policy Fellow; and Brian Kennedy, Minority General Counsel.

Chairman ROKITA. Well, good morning. And welcome to the first hearing of the Subcommittee on Early Childhood, Elementary, and Secondary Education in the 114th Congress.

I would like to thank our witnesses for joining us today. We appreciate the opportunity to learn from you about how emerging technology in the classroom affects student privacy.

And Ms. Fudge, before we begin, I want to take a moment to congratulate you on being selected by your colleagues to be the ranking member of this subcommittee. I anticipate that we are gonna hear a lot from each other, work well together. And I look forward to doing that with you.

Ms. FUDGE. Thank you.

Chairman ROKITA. Forty years ago, Congress enacted the Family Educational Rights and Privacy Act, otherwise known around these parts as FERPA. It was meant to safeguard students' educational records and ensure parents had access to their children's information. The law established the circumstances under which the record could be shared, giving parents the peace of mind that with few exceptions, that their child's academic performance and other personally-identifiable information would be under their kid's school's lock and key.

As a father of two young boys, I can appreciate why parents may not have that same confidence today. Despite the advent of computers, the internet, wifi, cloud services, et cetera, the law has not been significantly updated since its introduction in 1974. As a result, student privacy—the very information FERPA was intended to protect—may be at risk.

As administrators, teachers, and students continue using emerging technology to track everything from test results to bookstore purchases, parents and students are vulnerable to the inappropriate use of student data, often without their knowledge or consent. New devices, platforms, programs, and services have enabled educators to better understand the behavioral and educational needs of each student and tailor individual learning plans accordingly. I think that is amazing progress.

They have assisted researchers in developing new solutions to improve class room reduction, and they have provided families with more educational options by facilitating distance and blended learning opportunities. Technology organizations and policymakers have taken steps to strengthen student privacy protections. And that is appreciated. However, these efforts have not addressed rules under which schools must operate as the guardians of student data.

So unless Congress updates FERPA and clarifies what information can be collected, how that information can be used, and if that information can even be shared, student privacy will not be properly protected. We welcome your thoughts on how this committee can update FERPA for the 21st Century, improve parental involvement, and hold bad actors accountable.

Modernizing student privacy protections without undermining opportunities to improve student achievement is no small task, as everyone here understands. But we owe it to our students and parents to work together to find that proper balance. So I look forward to hearing from you and from my colleagues on this important issue.

And with that, I welcome and recognize our subcommittee's ranking member, again, my colleague, Congresswoman Fudge, for her opening remarks.

[The statement of Chairman Rokita follows:]

Prepared Statement of Hon. Todd Rokita, Chairman, Subcommittee on Early Childhood, Elementary, and Secondary Education

Good morning, and welcome to the first hearing of the Subcommittee on Early Childhood, Elementary, and Secondary Education in the 114th Congress. I'd like to thank our witnesses for joining us today. We appreciate the opportunity to learn from you about how emerging technology in the classroom affects student privacy.

Ms. Fudge, before we begin, I want to take a moment to congratulate you on being selected by your colleagues to serve as ranking member of this subcommittee. I anticipate we will have many robust conversations on key issues, and I am looking forward to working together on policies that will help our children succeed in school and in life.

Forty years ago, Congress enacted the Family Educational Rights and Privacy Act, or FERPA, to safeguard students' educational records and ensure parents had access to their children's information. The law established the circumstances under which the records could be shared, giving parents the peace of mind that, with few exceptions, their child's academic performance and other personally identifiable information would be under the school's lock and key.

As a father of two young boys, I can appreciate why parents may not have that same confidence today. Despite the advent of computers, the Internet, Wi-Fi, and cloud services, the law has not been significantly updated since its introduction in 1974. As a result, student privacy, the very information FERPA was intended to protect, may be at risk.

As administrators, teachers, and students use emerging technology to track everything from test results to bookstore purchases, parents and students are vulnerable to the inappropriate use of student data – often without their knowledge or consent.

New devices, platforms, programs, and services have enabled educators to better understand the behavioral and educational needs of each student and tailor individual learning plans accordingly. They have assisted researchers in developing new solutions to improve classroom instruction. And they have provided families with more educational options by facilitating distance and blended learning opportunities.

Technology organizations and policymakers have taken steps to strengthen student privacy protections. However, these efforts have not addressed rules under which schools must operate as the guardians of student data. Unless Congress updates FERPA and clarifies what information can be collected, how that information can be used, and if that information can be shared, student privacy will not be properly protected.

We welcome your thoughts on how this committee can update FERPA for the 21st century, improve parental involvement, and hold bad actors accountable. Modernizing student privacy protections without undermining opportunities to improve student achievement is no small task, but we owe it to students and parents to work together to find the proper balance. I look forward to hearing from you and from my colleagues on this important issue.

With that, I will now recognize the ranking member, Congresswoman Fudge, for her opening remarks.

Ms. FUDGE. Thank you very much, Mr. Chairman. And I thank all of you for being here today. Look forward to hearing your testimony.

I certainly want to recognize the ranking member of the full committee who has joined us, Representative Scott, from Virginia.

And I want to say to the chairman, indeed I do hope that we can have some very productive meetings and discussions. This is a very timely topic. I thank you for calling this hearing.

I do though find it unfortunate that it is our first hearing after we had a 10-hour mark up yesterday on ESEA. And with that, to you, more than ever before, technology does play an essential role in educating our nation's children, enhancing learning and empowering educators with more and better information to meet the individual needs of their students.

Gone are the days when education was supported by flashcards and workbooks. Today's students use electronic tablets and smartphone apps, online study tools, and various other technological resources to aid them in their studies. Teachers have the ability to extend learning beyond the classroom using online learning platforms to share multimedia resources and engage parents in their children's learning.

New educational technology generates information that can be instrumental in improving a student's learning experience. The data from these tools allow teachers to more accurately assess student progress and provide interventions to ensure children are learning.

Data can also assist schools in making district strategy and curriculum decisions. Many states now use longitudinal data systems to link student achievement data from pre-K through grade 12, or even through entrance into the workforce, enabling district and state leaders to make informed, data-driven policy decisions.

While the use of technology in education continues to expand, we must take the necessary steps to protect the privacy and the data of students and their families. The Family Educational Rights and Privacy Act was enacted 40 years ago to address concerns about privacy in a time of paper student records. Innovative new educational technology tools capture large amounts of student data. And many districts now contract with private vendors to use online, cloud-based storage for students. I see some of those very vendors here today.

Congress must ensure student data is being used only for defined educational purposes and cannot be sold or used for private companies' financial gain. Parents should know who has access to student data and how it is being used and protected. And teachers and school leaders need to understand how to properly protect student information while taking advantage of the powerful digital learning tools at their disposal.

As we examine FERPA, we need to balance privacy and innovation. Students, teachers, and parents need to feel comfortable that student data is protected. At the same time, we need to be careful not to limit the advancement of new educational technologies, restrain educators' ability to accurately assess student learning, or stifle research and development of effective instruction tools.

I look forward to hearing from our witnesses. Mr. Chairman, I yield back.

Prepared Statement of Hon. Marcia L. Fudge, Ranking Member, Subcommittee on Early Childhood, Elementary, and Secondary Education

More than ever before, technology plays an essential role in educating our nation's children, enhancing learning and empowering educators with better information to meet the individual needs of their students.

Gone are the days when education was supported by flashcards and workbooks. Today's students use electronic tablets and smartphone apps, online study tools, and various other technological resources to aid them in their studies. Teachers have the ability to extend learning beyond the classroom, using online learning platforms to share multimedia resources and engage parents in their children's learning.

New educational technology generates information that can be instrumental in improving a student's learning experience. The data from these tools allow teachers to more accurately assess student progress and provide interventions to ensure children are learning.

Data can also assist schools in making district strategy and curriculum decisions. Many states now use longitudinal data systems to link student achievement data from pre-k through grade 12, or even through entrance into the workforce, enabling district and state leaders to make informed, data-driven policy decisions.

While the use of technology in education continues to expand, we must take the necessary steps to protect the privacy and the data of students and their families.

The Family Educational Rights and Privacy Act (FERPA) was enacted 40 years ago to address concerns about privacy in a time of paper student records. Innovative new educational technology tools capture large amounts of student data and many

districts now contract with private vendors to use online cloud-based storage for student data.

Congress must ensure student data, is being used only for defined educational purposes, and cannot be sold or used for private companies' financial gain. Parents should know who has access to student data and how it is being used and protected. And teachers and school leaders need to understand how to properly protect student information while taking advantage of the powerful digital learning tools at their disposal.

As we examine FEPRA, we need to balance privacy and innovation. Students, teachers, and parents need to feel confident that student data is protected. At the same time, we need to be careful not to limit the advancement of new educational technologies, restrain educators' ability to accurately access student learning, or stifle research and development of effective instructional tools.

I look forward to hearing from our witnesses. Thank you.

Chairman ROKITA. Thank the gentlelady. Pursuant to Committee Rule 7(c), all members will be permitted to submit written statements to be included in the permanent hearing record. And without objection, the hearing record will remain open for 14 days to allow such statements and other extraneous material referenced during the hearing to be submitted for the official hearing record.

It is now my pleasure to introduce our distinguished witnesses for today. First we have Shannon Sevier. All right. Not off to a good start. Sevier. Shannon Sevier—thank you—has been a PTA member for 14 years. As vice president for advocacy, she needs advocacy efforts for the national PTA positions at federal, state, and local levels. Welcome.

Next, we have Allyson Knox, who is the director of education policy and programs at Microsoft. In her 10 years at Microsoft, she has focused on stem, computer science, education and technology, and student privacy issues. Welcome to you, as well.

Next, we have Sheryl Abshire, who is the chief technology officer for the Calcasieu Parish Public Schools in Lake Charles, Louisiana. For over 40 years, Dr. Abshire has worked as a chief technology officer, school principal, K through 5 teacher, a library media specialist, classroom teacher, and university professor. She was the first teacher inducted into the National Teacher's Hall of Fame. Thank you for being here.

Next, we have Joel Reidenberg. He is the Stanely D. and Nikki Waxberg Chair in law and professor of law at Fordham University, where he directs the center on law and information policy. Reidenberg publishes regularly on both information privacy and on information technology law and policy. Mr. Reidenberg, welcome back. I understand this is at least your third time testifying.

Mr. REIDENBERG. Thank you.

Chairman ROKITA. I will now, in conformance with our rules, ask our witnesses to stand and raise your right hand.

[Witnesses sworn.]

Let the record reflect that the witnesses answered in the affirmative.

And before I recognize each of you to provide your testimony, let me briefly explain our lighting system. You will each have 5 minutes to present your testimony. During the first 4 minutes of that, the light will be green. The last minute it will be yellow. And then if it turns red, I will be forced to use the gavel, which we have never had to do. At all. Ever. So I am sure it won't happen today.

So with that being said and understood, Ms. Sevier, you are recognized for 5 minutes.

TESTIMONY OF MS. SHANNON SEVIER, VICE PRESIDENT FOR ADVOCACY, NATIONAL PARENT TEACHER ASSOCIATION, SAN ANTONIO, TEXAS

Ms. SEVIER. National PTA thanks Chairman Rokita and Ranking Member Fudge for the opportunity to submit testimony to the Committee on Education and the Workforce. On behalf of the National Parent Teacher Association, I express my appreciation for holding a hearing to discuss emerging technology and student data privacy.

My name is Shannon Sevier, vice president of advocacy for the National PTA, past European PTA president, and proud mother to Ryley, MacKenzie, Meraleigh, Ryan, and Hanna.

Founded in 1897, PTA is the oldest and largest volunteer child advocacy association in the United States. For more than 118 years, we have worked side by side with policymakers at every level to improve the lives of our nation's children. With more than 4 million members and 22,000 local units in every U.S. state, D.C., Puerto Rico, the Virgin Islands, and Europe, PTA continues to be a powerful voice by advocating for federal policies to improve educational equity and opportunity for all children.

With access to so many families, PTA also recognizes our responsibility to our membership to approach changes in education policy through engagement and outreach and to recognize that true advocacy is achieved through stakeholder consensus and collaboration. National PTA has long been a vocal advocate of keeping kids safe; safe at school, safe at home, and same online.

The National PTA's position statement on technology safety clearly states National PTA opposes the practice of collecting, compiling, selling, or using children's personal information without giving parents notification or choice with respect to whether and how their children's personal information is collected and used.

The National PTA takes student data privacy seriously and believes we should strive to guarantee the effective use of students' information, while keeping that information protected. While student data management has changed, parents' and students' expectation of privacy has not. And as such, National PTA has made safeguarding student data a key pillar of our overall policy agenda.

The Administration has also called attention to this issue, announcing its support of what it calls the Student Digital Privacy Act, which would build upon the basic language of record management release and review offered by the Family Educational Rights and Privacy Act, or FERPA. This law was written in 1974 with the intent to protect the privacy of student educational records and includes a parental consent provision.

Over the past 40 years, however, the concept of privacy has evolved from the right of direct control to an individual's right to control the information they have entrusted to others. This wrinkle in control requires subsequent change to student data privacy policy.

Entities collecting educational data should seek to provide value back to the people on whom data are being collected. Our children's data, our children's privacy, should not be treated as a product or

commodity. Until now, the collection and use of student data could not be feasibly used to target advertising or mass profiles by third party vendors. The use of student data for other than educational purposes was not contemplated on a large commercial scale. FERPA provisions must be updated to address the privacy concerns presented through such use.

In addition, we are seeing this data collected and stored in a different fashion heretofore not addressed by FERPA. State by state, we see the construction of longitudinal data systems that hold hundreds or even thousands of pieces of data related to individual students. Typically, demographic, enrollment, curriculum choice, test performance, and grade information. The extent to which this information constitutes a student's legal educational record is unclear, as are the policies for protecting student data through cloud-based computing.

Current policy also begs the questions, who owns the data and who is responsible for the management of the data? Has the data been selected ethically with full consent and notification? And what constitutes sufficient notice in the case of breaches or unauthorized releases of data?

Parents, as their child's first educator, play a unique role in education reform. Whether big or small, reform will be unsustainable without the buy-in of these key stakeholders.

National PTA remains committed to engaging parents, to guaranteeing students have safe and secure access to technology in the classroom, and committed to supporting policies that ensure responsible management of student records, digital or otherwise.

National PTA commends the committee for holding this hearing and highlighted the need for sound federal policy that balances the promise of educational technologies with student data, privacy, and security.

Thank you.

[The testimony of Ms. Sevier follows:]

National PTA®
everychild.onevoice.™

Testimony of Shannon Sevier, Vice President of Advocacy
National Parent Teacher Association

Before the United States House of Representatives
House Committee on Education and the Workforce
Subcommittee on Early Childhood, Elementary and Secondary Education

Hearing on How Emerging Technology Affects Student Privacy

February 12, 2015

National PTA thanks Chairman Rokita and Ranking Member Fudge for the opportunity to submit testimony to the Committee on Education and the Workforce. On behalf of the National Parent Teacher Association, I express my appreciation for holding a hearing to discuss emerging technology and its impacts on student data privacy.

My name is Shannon Sevier. Vice President of Advocacy for the National PTA, past European PTA President and proud mother to Ryley, McKenzie, Meraleigh, Ryan and Hanna.

Founded in 1897, PTA is the oldest and largest volunteer child advocacy association in the United States. For more than 118 years, we have worked side by side with policymakers at every level to improve the lives of our nation's children, including the passage of child labor laws, providing nutritious lunches in school, improvements to the unfair and punitive treatment of children in the justice system, and overall increased education opportunities for all children.

With more than four million members and 22,000 local units in every U.S. state, the District of Columbia, Puerto Rico, the Virgin Islands, and Europe, PTA continues to be a powerful voice by advocating for federal policies to improve educational equity and opportunity for all children and their families. With access to so many families PTA also recognizes our responsibility to our membership to approach changes in education policy through engagement and outreach, and to recognize that true advocacy is achieved through stakeholder consensus and collaboration.

With regard to today's hearing, National PTA has long been a vocal advocate of keeping kids safe: safe at school, safe at home, and safe online. National PTA believes that our children's schools should provide safe and nurturing environments for both teaching and learning. This includes ensuring that all student data is safe and secure.

The National PTA's position statement on technology safety clearly states: *National PTA opposes the practice of collecting, compiling, selling or using children's personal information without giving parents notification or choice with respect to whether and how their children's personal information is collected and used. The National PTA takes student data privacy seriously, and believes we should strive to guarantee the effective use of students' information, while keeping that information protected.*

National PTA
every child. one voice.

While student data management has changed, parents' and students' expectation of privacy has not, and as such National PTA has made safeguarding student data a key pillar of our overall policy agenda. In order to demonstrate our commitment to this critically important issue, PTA has taken steps to encourage action by supporting common sense approaches and informing our parents about the importance of keeping their children's data safe.

The Administration has also called attention to this issue, announcing its support of what it calls, The Student Digital Privacy Act, which would build upon the basic language of record management, release and review offered by the Family Educational Rights and Privacy Act, or FERPA. This law was written in 1974 with the intent to protect the privacy of student educational records and includes a parental consent provision. Over the past 40 years, however, the concept of privacy has evolved from the right of direct control, to an individual's right to control the information they have entrusted to others. This wrinkle in control requires subsequent change to student data privacy policy.

As a general rule of thumb entities collecting educational data should seek to provide value back to the people on whom data are being collected. Our children's data, our children's privacy, should not be treated as a product or commodity. Until now the collection and use of student data could not be feasibly used to target advertising or amass profiles by third party vendors. The use of student data for other than educational purposes was not contemplated on a large commercial scale. Now that it is, FERPA provisions must be updated to address the privacy concerns presented through such use.

In addition to the diversified use of student data, we are seeing this data collected and stored in a different fashion heretofore not addressed by FERPA. State by state we see the construction of longitudinal data systems that hold hundreds or even thousands of pieces of data related to individual students – typically demographic, enrollment, curriculum choice, test-performance and grade information. The extent to which this information constitutes a student's legal "educational record" is unclear as are the policies for protecting student data through cloud-based computing.

Current policy also begs the questions: who owns the data and who is responsible for the management of the data; has the data been collected ethically, with full consent and notification; and what constitutes sufficient notice in the case of breeches or unauthorized release of data?

Parents, as their child's first educator, play a unique role in education reform. Whether big or small, reform will be unsustainable without the buy-in of these key stakeholders. National PTA remains committed to engaging parents, to guaranteeing students have safe and secure access to technology in the classroom, and committed to supporting policies that ensure responsible management of student records, digital or otherwise. We respectfully ask this Committee and this Congress to work together to find the best way forward to protect student data privacy and ensure student data security. National PTA commends the committee for holding this hearing, and highlighting the need for sound federal policy that balances the promise of educational technologies with student data privacy and security.

ROKITA. Thank you for your testimony.
Ms. Knox, you are recognized for 5 minutes.

TESTOMONY OF MS. ALLYSON KNOX, DIRECTOR OF EDUCATION POLICY AND PROGRAMS, MICROSOFT, WASHINGTON, D.C.

Ms. KNOX. Thank you, Chairman Rokita, Ranking Member Fudge, and members of the subcommittee for inviting me to testify today. My name is Allyson Knox. For 10 years I worked in the fields of education, workforce development, and economic development at the local, regional, and state levels in Michigan. I have worked at Microsoft for 10 years, and currently serve as the director of education policy. I am pleased to be here today to discuss this important issue of student privacy.

Microsoft believes students must be protected. Student data belongs to students and their parents. And students are not commodities to be monetized through advertising. 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. Microsoft, a provider of education technology, continues to balance education objectives, as well as privacy and safety expectations.

For many years, schools have been increasing the use of technology in the classroom because it transforms education. It enables personalized instruction, and it helps students learn. Schools that use cloud-based services rather than maintaining and updating their own on-site servers, they save money and can access the latest technology. Cloud computing allows teachers and students to access their documents and communications, such as email, anywhere from almost any device, enabling learning any time and anywhere.

We have seen great changes on the technology side. But the primary federal law focused on protecting student privacy, the Family Educational Rights and Privacy Act, or FERPA passed in 1974 has not kept pace with these changes.

Think back to a classroom in 1974. I think we can all remember student data being collected and stored in an old-fashioned way on paper forms sent home with kids and stored in school filing cabinets.

The world of information storage and sharing has certainly changed. In almost all schools, information about a student is stored digitally, and it can be accessed through the school's internet or the open internet. The data is portable and often not deleted when the student graduates from high school.

There are obvious difficulties with the law that is 4 decades old. And there are three areas to consider. First, it is questionable whether FERPA covers email stored in a cloud. As a result, some interpretations are that FERPA applies to cloud-based email for faculty, but not for 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.

Second, FERPA was written to apply only to educational institutions. It should be updated to prohibit third parties from using

data for targeted advertising or for building profiles to advertise to students after they leave school.

And third, FERPA's primary sanction is the denial of federal funds to school. This all-or-nothing enforcement penalty is so draconian that it has never been used. As a result, FERPA provides no real incentive for technology providers to improve data privacy practices. The time has come to do the difficult work of revising this law to bring it to the 21st Century.

And in the absence of federal action to update FERPA, states have taken this issue into their own hands. This year, already over 100 student privacy bills have been introduced in 32 states. It is becoming more and more difficult to interpret and comply with the patchwork of federal and state laws on this issue, even for a company of our size.

Microsoft and other technology companies have also moved forward on their own to set a higher standard for protecting student data. Last October, Microsoft was one of the 14 original signatories of a detailed and voluntary industry pledge, led by Representatives Messer and Polis, about how to protect student privacy. Today, the pledge has over 100 signatories.

Under the student privacy pledge, school service providers promised to not sell student information, not target advertise to students, use data for authorized education purposes only; and there are 5 other points, but I am running out of time. The pledge has been influential and beneficial, but Microsoft believes that signing it is only part of what must be done to help inform schools and parents on how to protect student data. It is for this reason that Microsoft has worked closely with key lawmakers and national education associations to help inform and educate stakeholders about the student privacy issue.

Again, I thank you for this opportunity to come before you today to discuss these important issues, and I look forward to answering any questions.

[The testimony of Ms. Knox follows:]

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.

Chairman ROKITA. Thank you for your testimony.
Dr. Abshire, you are recognized for 5 minutes.

TESTIMONY OF DR. SHERYL R. ABSHIRE, CHIEF TECHNOLOGY OFFICER, CALCASIEU PARISH PUBLIC SCHOOLS, LAKE CHARLES, LOUISIANA

Ms. ABSHIRE. Yes, sir. Thank you, Chairman Rokita, Ranking Member Fudge, and members of the subcommittee for inviting me to testify about technology's impact on student privacy and confidentiality.

For over 40 years, I have served the Louisiana Public Schools as a teacher, school librarian, principal, and technology leader. I now serve as the chief technology officer of the Calcasieu Parish schools in Lake Charles, Louisiana. And I am also a member of the Consortium for School Networking, CoSN, the national professional organization for school tech leaders.

I appreciate this opportunity to discuss how our district uses technology to support teaching and learning and to share our strategy for balancing effective technology and data use with strong student data privacy protections.

Technology and data use plays a central role in our district's strategy for supporting teaching and learning, as well as in improving the system's planning, evaluation, and continual improvement. Equipped with the right technology, high-quality professional development, and appropriate data, our teachers tailor individualized instruction, engage students, and deliver rich digital resources. Our district also equips parent and guardians with the data they need to monitor, understand, and support their children's educational progress.

Using technology to provide the right people with the right data at the right time is critical to effective decision making at the classroom, school district, and state levels. We believe robust data sharing, however, must be complemented by well-designed strategies and practices to protect student privacy and ensure confidentiality.

Our district has taken an aggressive and comprehensive approach to assuring student privacy. We have created extensive data-sharing training materials, and all employees in the district have participated in training sessions. Upon completion of this required training every year, each district employee signs a statement of assurances. This process is based on CoSN's protecting privacy in a connected learning toolkit that we produced in partnership with the Harvard Law School. And the best part, it is free to all school districts.

The Calcasieu Parish Public Schools strongly emphasize both appropriate technology and secure and safe data use, including using this data to develop a greater understanding of student needs, and then tailoring instruction delivery of resources to help them succeed. Over the past 3 years, our district has developed a leading edge data warehouse and data dashboard to provide our teachers and school leaders with timely, targeted information; the information they need to support improving learning.

Based on my experience in the Calcasieu Parish Schools, I urge Congress to proceed very cautiously with new federal privacy re-

quirements. We want to ensure that any contemplated legislation doesn't impede this type of powerful instructional data use.

We also work with all of our vendor partners that use any student data as part of learning or assessment. We require them to certify their compliance with our data usage policy. And our state law reasonably addresses data sharing with vendors and requires them to sign contracts specifying the limited purposes for which the student information can be used.

Our district believes that our teachers and school leaders and parents must be equipped with the right technology and the knowledge about how to use the student data and protect—to use it with fidelity to implement best practices. We provide this regularly-targeted professional development designed to equip our educators and school leaders with this knowledge they need to use to, most importantly, improve student outcomes, and including training them with privacy and security practices.

However, additional federal investments in technology and student-focused privacy professional development, including the Enhancing Education Through Technology program is urgently needed. I would encourage Congress to support the President's fiscal year 2016 request. Unfortunately, for school districts, this program hasn't been funded since 2011.

Our district also prioritizes communicating with stakeholders to convey the value of this data in teaching, learning, and decision making. All of this information is made readily available to parents and the entire community on our district web page. Transparency builds trust with our communities. And that is why I hope Congress will consider strategies that encourage districts to promote data use transparency, including describing the who, what, where, and when of their technology practices.

Protecting student data is not a one-time event. Educators' data needs are evolving. Security threats are constantly changing, and professional development need are ongoing. I hope Congress would encourage districts to implement security practices that meet the mature technical, physical, and administrative standards.

While federal state and privacy policy is critically important, there is no doubt in my mind that school districts and schools must lead these efforts to protect student data privacy. And any effort by Congress to update laws to protect students, FERPA and COPPA, should support, not burden school district and state data use to improve instruction and decision making.

Appropriate data sharing must be served to strengthen the potential of technology to transform and improve education. I urge Congress, please do not overreach as you address this important issue. But instead, take a thoughtful, balanced approach focused on supporting schools and district leaders.

I thank the members of the Committee for this opportunity to share a realistic view of the issue from the perspective of a school district that is engaged in this work. And I am happy to answer any questions.

[The testimony of Dr. Abshire follows:]

HOUSE EDUCATION AND THE WORKFORCE COMMITTEE
SUBCOMMITTEE ON EARLY CHILDHOOD, ELEMENTARY AND SECONDARY EDUCATION

"HOW EMERGING TECHNOLOGY AFFECTS STUDENT PRIVACY"
FEBRUARY 12, 2015

TESTIMONY OF SHERYL ABSHIRE
CHIEF TECHNOLOGY OFFICER
CALCASIEU PARISH PUBLIC SCHOOLS
LAKE CHARLES, LOUSIANA

Introduction

Thank you, Chairman Rokita, Ranking Member Fudge, and members of the subcommittee, for inviting me to testify about technology's impact on student privacy and confidentiality. For over 40 years, I have served Louisiana Public Schools as a teacher, school librarian, principal, and technology leader. I now serve as the Chief Technology Officer of the Calcasieu Parish Public Schools in Lake Charles, Louisiana, and I am also a member of the Board of Directors for the Consortium for School Networking (CoSN), a national professional organization for school district technology leaders.

Framing the Issue

I appreciate this opportunity to discuss how our district uses technology to support teaching and learning and to share our strategy for balancing effective technology and data use with strong student data privacy protections. Technology and data use play a central role in our district's strategy for supporting teaching and learning, as well as in improving the system's planning, evaluation, and continual improvement. Equipped with the right technology, high quality professional development, and appropriate data, our teachers can tailor and individualize instruction, engage students, and deliver rich digital resources. Our district also equips parents and guardians with the data they need to monitor, understand and support their children's educational progress; grants school and district leaders with data to identify and address program performance gaps and make better management decisions; and provides state leaders with aggregate data to better assess the effectiveness of important state college and career readiness education reforms. Finally, we are on the cusp of providing real-time data to our students to enable feedback that deepens their learning and helps them go deeper, learn faster, and understand areas needing improvement.

Using technology to provide the right people, with the right data, at the right time is critical to effective decision-making at the classroom, school, district and state levels. We believe robust data sharing, however, must be complemented by well-designed strategies and practices to protect student privacy and ensure confidentiality. In our district, these protections include equipping our schools with well-designed privacy policies; ensuring implementation of technical, physical and administrative safeguards; and strengthening our educator, school leader and staff capacity to effectively use and protect personally identifiable data. We also take steps to continually educate our parents and other stakeholder groups about our district's technology, data use, and privacy strategies, so that the "what, where, and when" of our practices are understood and broadly supported by the community.

District Vision and Practice

Our district has taken an aggressive and comprehensive approach to assuring student privacy. We have created extensive data sharing training materials and all employees in the district, from the school custodians, bus drivers, to teachers and principals, have participated in the training sessions outlining the permissible uses of student data sharing. Upon completion of the required training, each year, every district employee signs a statement of assurances to acknowledge their understanding and compliance with student data sharing polices and laws of the district and state. This process is based on the CoSN Protecting Privacy in Connected Learning Toolkit produced in partnership with Harvard Law School's Cyberlaw Clinic and is free to all school systems.

Calcasieu Parish Schools strongly emphasize both appropriate technology and secure and safe data use, including using data to develop a greater understanding of student needs and then tailoring instruction and delivery of resources to help them succeed. Over the past three years, our district developed a leading-edge data warehouse and data dashboard to provide our teachers and school leaders with the timely, targeted information they need to support learning. Our system provides every school leaders and teachers in the Calcasieu Parish Schools with rich diagnostic information – including formative and summative results and other indicators – about each learner and their progress toward achieving Louisiana's college and career ready standards. This monitoring enables us to keep students on track for graduation, including identifying warning signs that might signal serious problems such as a greater likelihood to fall behind grade level or drop out. Based on my experiences in Calcasieu Parish, I urge Congress to proceed cautiously with new federal privacy requirements. We want to be sure that any contemplated legislation does not impede this type of powerful instructional data use.

Community-based organizations, researchers and private partners play an important role in supporting our district's efforts to meet the needs of every student. Collaborating with partners, including appropriately and lawfully sharing student information with them to improve teaching and learning, and to support school and district decision-making, greatly enhances our ability to improve student outcomes and efficiently run our district. For example, we work with all of our vendor partners that use any student data as part of a learning or assessment system. We require them to certify their compliance with our data usage policy. Our state law reasonably addresses such sharing by requiring all vendors to sign contracts securing their commitment to protect student data, specifying the limited purposes for which the student information may be used, and, as required by FERPA, ensuring that sensitive data always remains under the control of the district. CoSN's Security Questions to Ask of an Online Service Provider has been helpful in identifying the key elements we expect of companies.

Congress must carefully avoid overreaching in ways that might create unintended consequences for educationally appropriate data sharing, including avoiding legal prescriptions that disrupt suitable private partnerships, research, evaluation and other activities designed to support district administration and related policymaking or stifle the use of innovative and effective web-based technology resources.

Our district prioritizes teacher and school leader staff development. We believe successful data use, including ensuring best in class privacy protections, not only requires sounds policies and practices, but also meaningful attention to building the capacity of our school leaders,

teachers and other staff. Teachers and school leaders must be equipped with the right technology and the knowledge about how to use and protect student data with fidelity to implement best practices. As a result, we support successful implementation of our data systems and practices with regularly targeted professional development designed to equip our educators and school leaders with the knowledge they need to use data to improve student outcomes, including training them in privacy and security best practices. Additional federal investments in technology and student privacy focused professional development, including through the Enhancing Education through Technology Program, would contribute significantly to helping districts protect student data privacy by ensuring they have access to leading-edge security protections and equipping education professionals with the knowledge they need to successfully implement privacy policies and protocols. I encourage Congress to support the President's FY 2016 request to fund this important program. Unfortunately this program has not received funding since 2011.

Our district prioritizes communicating with stakeholders to convey the value of data to teaching, learning, and decision-making. With this goal in mind, we work to ensure that our parents and communities find value in the data that is collected and understand the "who, what, where, and when" of data collection and use. We also established a clearly understandable data inventory and description of the data we use. All of this information is made readily available to our parents and community on our district webpage. This step not only builds trust and understanding in our community, but also forces our district to reflect on our data use practices and ensure that we are not unnecessarily collecting student information. Informed communities become allies in both effective data use and privacy protection and recruiting them begins with efforts to promote transparency. CoSN and the National School Public Relations Association have produced a helpful infographic which school districts can use with their parents / guardians to convey why we collect data and how we protect it. This type of transparency is key to building trust with our communities. Congress should consider strategies that encourage districts to promote data use transparency, including describing the "who, what, where, and when" of their technology and data practices.

Finally, our district strives to routinely review and update our privacy, technology and data use policies, so that they reflect our educational needs and evolving privacy best practices. Protecting student data is not a one-time event. Educators' data needs evolve, security threats are constantly changing, and professional development needs are ongoing. We work to ensure that our policies reflect this dynamic environment so that we can meet our professional's needs and anticipate and address policy or practice gaps that might compromise the privacy of our students. Congress should encourage districts to implement security practices that meet mature technical, physical and administrative standards. Congress should also encourage districts to continually examine and update their privacy and security policies and practices and provide the resources needed to ensure our schools remain on the leading edge of privacy protections.

Conclusion

While federal and state privacy policy is critically important, school districts and schools must lead efforts to protect student data privacy. Any effort by Congress to update federal privacy laws to better protect students, including improvements to FERPA and Children's Online Privacy Protect Act (COPPA), should support, not burden school, district and state data use to improve instruction and decision making. Appropriate data sharing with researchers, evaluators and

private partners engaged in supporting educational and administrative activities must be preserved to strengthen the potential of technology to transform and improve education.

Although they have some weaknesses, FERPA and COPPA already provide a strong foundation for local privacy leadership and decision-making. Any new federal law should concentrate on addressing clear gaps in the present system, including the absence of a focus on ensuring technical, physical and administrative protocols and especially the lack of sufficient resources for professional development targeting educators, school leaders and staff.

I urge Congress not to overreach as it addresses this important issue, but instead to take a thoughtful, balanced approach focused on supporting district and school leadership.

I thank the members of the Committee for the opportunity to share a realistic view of this issue from the perspective of a school district. I will be happy to answer any questions the Committee might have.

ADDENDUM

CoSN's *Protecting Privacy in Connected Learning Initiative*

This CoSN-led effort provides school leaders and stakeholders with a suite of resources to help them navigate the four major federal privacy laws and address key questions about protecting student privacy.

The resources offered through the initiative include an in-depth, step-by-step toolkit; infographics to empower schools leaders to clearly discuss the issue; and additional complementary, standalone tools.

The resources can be downloaded for free at: cosn.org/privacy.

Chairman ROKITA. Thank you, Dr. Abshire. Appreciate it.
Mr. Reidenberg, you are recognized for 5 minutes.

TESTIMONY OF MR. JOEL R. REIDENBERG, STANLEY D. AND NIKKI WAXBERG CHAIR AND PROFESSOR OF LAW, FOUNDING ACADEMIC DIRECTOR, CENTER ON LAW AND INFORMATION POLICY, FORDHAM LAW SCHOOL, NEW YORK, NEW YORK

Mr. REIDENBERG. Thank you, Mr. Chairman. And good morning. Good morning, Ranking Member, and distinguished remembers of the committee. I very much appreciate the opportunity to testify today.

I studied and written on privacy technology for over 25 years. And I focused the last 5 or 6 years on student privacy issues, including several national studies that have been presented previously to this subcommittee. On a personal level, I served on a school board for 5 years. So it is an issue that is actually quite close to my heart.

I am testifying today though on my own behalf, I am not representing any organization with which I am affiliated. I have submitted a longer witness statement, but I am just gonna summarize that during the 5 minutes.

Educational technologies and the use of data today is transforming American education. We see tremendous opportunities to improve education. And at the same time, we see the scope of data collection has now become massive. And our privacy laws simply aren't working to protect children's privacy when that information is coming from schools.

We have three statutes in our federal privacy law; FERPA, the Protection of Pupil Rights Amendment from the 1970s, and COPPA. The Pupil Rights Amendment Act and COPPA are really addressing very narrow issues. One focuses on surveys in schools. The other focuses on directly collecting data from children.

So the main privacy legislation that addresses student information is FERPA. And FERPA desperately needs to be updated for the 21st Century. We have heard—you know, 40 years ago when it was enacted, data was kept—the records were kept in file cabinets. It worked then, but schools had no computers and the internet wasn't anyone's dream in the school systems in those days.

There are really three areas that I think we need to address in modernizing FERPA. The first is that the coverage of FERPA is outdated. FERPA governs educational records. Well, today, student and educational records are narrowly defined. Today, the kind of information will range from grades to metadata about reading habits. Much of the data that comes from learning tools is outside the scope of FERPA.

FERPA is a financing statute. It applies to institutions receiving federal funds, and only those institutions. That means the vendor community—those supplying many of these services—have no direct statutory obligations. Schools have them. But schools are often in a very difficult position to be able to work—deal with—contract with the vendors.

We have so many schools across the country that don't have legal council, don't have sufficient technology expertise to even know what they are looking at when they see a vendor agreement.

The privacy pledge that we heard about this morning is a tremendous initiative, but it is not a substitute for strong legal protections. And then FERPA misses very important elements. FERPA saying nothing about data security, saying nothing about breach notification, has nothing on the transparency of how vendors might be using and sharing information. So these are elements the coverage of FERPA just doesn't match what is going on today.

The approach—the secondary, the approach of FERPA itself, is outdated. FERPA's focus was on confidentiality and parental access. Today, the critical issues are about permissible educational uses of student data. What is the use; right? We have other statutes, like the Fair Credit Reporting Act, is a permissible purpose statute. That works in the modern world. FERPA doesn't. FERPA needs to look toward that model, identify what are truly educational uses. Those are fine. Everything else is prohibited wthout parental consent.

Data mining, homework assignments, teacher interactions, all of these things today, are they appropriate uses for the students' data? As a parent, a former board member, I don't think our children should be required to subsidize private commercial gain to get an education through their information being monitored and used.

Lastly, the third area is enforcement and remedies. FERPA is essentially unenforceable. The one existing remedy is a nuclear option. It has never been used by the department of education. It is total withdrawal of federal funds.

The victims have no redress. If you or your family's information is compromised, there is no redress under FERPA. FERPA needs to have graduated sanctions, fines, various abilities to enforce through the Department of Education. I think the State's attorney general ought to have enforcement authority. We see that again in the consumer credit reporting area. And I think it would be very important to have private enforcement options so that families have redress.

It would be helpful for Congress, I think, to encourage the States to have chief privacy officers in their state departments of education to assist the local schools. Because it is very difficult for local school to understand how to navigate this territory.

So my conclusion is that Congress can no longer wait. If we want the innovation that educational technologies and data uses offer us, if we want that to be accepted by schools and parents, Congress has to update FERPA so that it matches what will be happening in the school communities. Otherwise, parents will not have trust, and there will be a constant struggle between the communities and the schools and the educators and national education policy.

Thank you.

[The testimony of Mr. Reidenberg follows:]

United States House of Representatives
114th Congress, 1st Session

Committee on Education and the Workforce
Subcommittee on Early Childhood, Elementary and Secondary Education

Hearing on
"How Emerging Technology Affects Student Privacy"
February 12, 2015

Statement of Joel R. Reidenberg
Stanley D. and Nikki Waxberg Chair and Professor of Law
Founding Academic Director, Center on Law and Information Policy
Fordham University
New York, NY

Good morning Chairman Rokita, Ranking Member Fudge and distinguished members of the Committee. I would like to thank you for the opportunity to testify today on emerging education technologies and their effects on the privacy of our nation's school children.

My name is Joel Reidenberg. I am a law professor at Fordham University where I hold the Stanley D. and Nikki Waxberg Chair in Law and a visiting lecturer at Princeton. I am also the founder and director of the Fordham Center on Law and Information Policy ("Fordham CLIP"). As an academic, I have written and lectured extensively on data privacy law and policy and am a member of the American Law Institute where I serve as an Adviser to the *Restatement of the Law Third on Information Privacy Principles*. Of particular relevance to today's hearing, I directed the Fordham CLIP research studies on *Privacy and Cloud Computing in Public Schools*" (Dec. 12, 2013) http://law.fordham.edu/k12cloudprivacy, and on *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems* (October 2009) http://law.fordham.edu/childrensprivacy/. I also supervised the Fordham CLIP *Privacy Handbook for Student Information Online: A Toolkit for Schools and Parents,* http://law.fordham.edu/center-on-law-and-information-policy/34710.htm that was just released last week. On a direct practical level, I served for five years as an elected member of my local school board where I chaired the Board's Program Committee.

In appearing today, I am testifying on my own behalf as an academic expert and my views should not be attributed to any organization with which I am affiliated.

I would like to focus my testimony on the need to modernize federal educational privacy law to meet the challenges of today's educational technologies. I will place a particularly emphasis on the Family Educational Rights and Privacy Act of 1974[1] ("FERPA").

Education Technology, Schools and Data Use

Today, local schools are uniformly transferring vast amounts of student information to state educational agencies and to online third parties for many varied purposes.

At the state level, the enactment of *No Child Left Behind* established new school reporting obligations that increased data collections about individual children by state education departments. Over the ensuing years, the states created longitudinal databases known as State Longitudinal Data Systems ("SLDS") to track educational progress and often relied on private education technology vendors to provide hosting and analytic services. These SLDS collect and process extensive information about individual children and are designed using common data standards so that links can be made between state systems.[2]

At the local level, school districts across the country are rapidly embracing evolving online technologies to meet data-driven educational goals, satisfy their reporting obligations, realize information technology cost-savings, and take advantage of new instructional opportunities. These educational technologies serve many different functions including data analytics, student performance reporting, classroom and learning support, career guidance support, school bus route planning, and server hosting.[3] These online educational services involve the collection and transfer of enormous quantities of student information to third party commercial organizations including school records, homework essays, fitness profiles, and even lunchroom purchases. In essence, most schools across the country outsource their children's data.

Outdated Education Privacy Law

Federal educational privacy law has failed to keep up with the developments in the use of student data and fails to protect the privacy of student information in a range of commercial computing services used by states and schools.

---

[1] 20 U.S.C. § 1232g

[2] See Joel R. Reidenberg, Jamela Debelak, et al. *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems* (Fordham CLIP: Oct. 28 2009) http://law.fordham.edu/childrensprivacy/ [hereinafter "Fordham CLIP 2009 Study"]

[3] Joel R. Reidenberg, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier & Daniella Alvarado, *Privacy and Cloud Computing in Public Schools*" (Fordham CLIP: Dec. 12, 2013) http://law.fordham.edu/k12cloudprivacy, [hereinafter "Fordham CLIP 2013 Study"], at pp. 17-18

Three federal privacy statutes address student information that may be collected by and from schools: FERPA, the Children's Online Privacy Protection Act[4] ("COPPA") and the Protection of Pupil Rights Amendment[5] ("PPRA").

FERPA is the oldest and best-known educational privacy statute. FERPA was enacted over forty years ago when student records were confined to file cabinets in the principal's office. The statute is essentially a confidentiality law that was designed to protect students' paper files. When FERPA became law in 1974, computers did not exist in schools and internet access was decades away. Consequently, FERPA does not function as a complete fair information practice statute for student information.

COPPA focuses on one particular issue: the online collection of personal information directly from children younger than 13 years old without parental consent. And, the PPRA primarily addresses the use of certain types of data collected from in-school surveys as well as some marketing activities.

Collectively, these three statutes miss the wide-ranging scope and scale of the use of student information through emerging educational technologies. As a result of high profile data sharing programs such as those proposed through inBloom[6] and revelations about the use of school data in commercial products such as the Google Apps for Education,[7] many states have explored new privacy requirements for student information. These requirements generally focus on prohibitions related to advertising and marketing uses of information gathered about school children. Many other concerns remain such as parental access and consent to the use of children's data, the legitimacy of non-marketing commercial uses of school data, data security and the sheer volume of data gathering programs.

Modernizing FERPA to meet today's needs

Without an adequate set of privacy protections for student information online, our children's privacy will be compromised and innovative education technologies and programs will face justifiable parental skepticism and opposition. We have already seen these effects with the dissolution of inBloom as a result of strong opposition related to

---

[4] 15 U.S.C. §§ 6501-6506

[5] 20 U.S.C. § 1232h

[6] See Benjamin Herold, inBloom to shut down amid growing privacy concerns, Eduation Week, Apr. 21, 2014 http://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html

[7] See Michele Molnar, Google Abandons Scanning of Student Email, Education Week, Apr. 20, 2014, http://blogs.edweek.org/edweek/marketplacek12/2014/04/google_abandons_scanning_of_student_email_accounts.html

privacy[8] and with the failure of ConnectEdu to respect the conditions of student privacy in its bankruptcy proceeding.[9]

FERPA desperately needs to be updated in order to assure student privacy in the 21st Century and to enable the development of robust educational programs that take full advantage of educational technologies.

Five areas in FERPA need to be addressed:

1. Update the definition of "Educational Record"

FERPA covers "educational records" in a very narrow sense and contemplated only those records that were originally kept in central administration files such as transcripts.[10] The statute also specifically carves out an exemption for "directory information" including a student's name, address, date of birth, telephone number, age, sex, and weight.

The 1974 definition and the directory information exclusion no longer make sense in 2015. Much of the data gathered and used in the context of online services will be outside the scope of the existing definition. For example, metadata gathered from a learning app used by a child in school that was then compiled to create a profile of the child for content delivery would not be an "educational record" and would fall outside the bounds of FERPA. Similarly, information developed by a school's transportation company identifying the street corners where 6th graders wait to take the school bus would fall outside FERPA and could be disclosed for advertising purposes and even possibly disclosed to non-custodial parents. Likewise, a child's homework assignment saved or shared with a teacher on a third-party service would not be an "educational record" and would not protected by FERPA.

For meaningful protection of student privacy in this environment, FERPA needs to encompass any information gathered about children for educational and school related uses. This would include profiles, whether or not identified to specific students, if those profiles will have an effect on the child's education or school related services.

2. Update FERPA to apply to vendors

Currently, FERPA does not apply directly to vendors. By its terms, FERPA only applies to educational agencies and institutions that are recipients of federal funds.[11] When schools and state agencies use third-party vendors, the schools and agencies have compliance obligations, but the vendors do not. The vendor's only legal obligations

---

[8] See Herold, *supra note* 6.

[9] See Michelle Molnar, Millions of Student Records Sold in Bankruptcy, Education Week, Dec. 10, 2014, http://www.edweek.org/ew/articles/2014/12/10/millions-of-student-records-sold-in-bankruptcy.html

[10] See Owasso Independent School District v. Falvo, 534 U.S. 426 (2002)

[11] 20 U.S.C. § 1232g(a)

derive from their contracts with those schools and agencies.[12] Fordham CLIP's research demonstrated that typical contracts and SLDS programs have not adequately protected student information and, at the local level, schools are poorly equipped to address the vendor contracts.[13] While many responsible vendors are committing to protect student privacy through the Future of Privacy Forum's K-12 Student Privacy Pledge[14], the pledge is not an adequate substitute for meaningful legal protection applicable to all industry participants.

If FERPA is to cover adequately the ecosystem of student information, the statue must apply to all participants. The importance of this direct applicability is illustrated by a new trend among some ed tech companies to market products directly to teachers such as online gradebooks.[15] These marketing efforts are designed to bypass school administrators. As a result, these vendors are, in effect, soliciting teachers to violate FERPA because the teachers will generally not have the legal authority to enter into contracts for the transfer of the district's student data. While the Federal Trade Commission might be able to bring a deceptive practice claim, as a policy matter FERPA should address vendors directly.

3. Update FERPA to address "educational uses"

FERPA's original focus was on confidentiality and parental access to educational records. Now that student information is more extensive and the analysis of that data is more critical to the development of innovative learning tools, FERPA needs to provide clear parameters for legitimate educational uses of student information. FERPA should define permissible "educational uses" or "educational purposes" for student information and prohibit other uses without parental consent.

This approach is not new in American privacy law. The Fair Credit Reporting Act ("FCRA"), for example, is a permissible purpose statute. The law limits the use of consumer reports without consent to specifically defined purposes.[16] The FCRA's approach was very successful and has been widely recognized as a key factor in the development of a robust and fairer consumer credit market in the United States. For the education sector, there now needs to be a conscious public choice about the legitimacy of how information is gathered and used when the data comes from children in school.

---

[12] While under FERPA the Department of Education may bar a school from using federal funds to contract with a particular vendor, this indirect applicability is rare and cumbersome. See 20 U.S.C. 1232g(b)(4)(B).

[13] *See* Fordham CLIP 2013 Study, *supra note* 3; Fordham CLIP 2009 Study, *supra note* 2.

[14] See Future of Privacy Forum K-12 Student Privacy Pledge, http://studentprivacypledge.org/ (109 companies have signed the pledge as of Feb. 9, 2015)

[15] Stephanie Simon, Data mining your children, Politico, May 15, 2014 http://www.politico.com/story/2014/05/data-mining-your-children-106676.html

[16]

As a parent and former school board member, I do not believe that public schools should be used to gather students' information for private commercial gain or used to barter their children's information as products for third-party gain. Google, for example, has waived using student information mined from Google Apps for Education for advertising purposes.[17] But, what about data mining students' homework assignments or teacher interactions to profile the students and then use or sell those profiles to skew search engine results or modify delivered content? I believe that such types of commercial practices are not legitimate educational uses of student information and should be proscribed.

For educational privacy to be protected effectively by FERPA, the statute needs to specify that student information gathered online may only be used to provide direct educational benefits to the child whose information is used. Because the educational legitimacy of particular data collections and uses will often be contextually driven, FERPA also needs to have a safe harbor mechanism that will enable the Department of Education, state agencies and local schools to define the educational appropriateness of particular types of online practices.

By specifically enumerating legitimate educational uses and creating a safe harbor mechanism, I believe many of the complex issues related to the status of a data recipient such as whether a third party qualifies as a "school official" can be streamlined and resolved.

4. Expand FERPA to cover additional key information practices

FERPA includes important transparency requirements for student information. Parents have a right of access to their children's educational records held by educational agencies and institutions. This transparency needs to extend to any organization processing student information. Like the credit reporting system, families should be able to know who has their children's data and they should have the right to seek correction of inaccurate information.

In connection with transparency, processors of student information should be accountable to families regarding the identity of organizations to whom student information was disclosed. Credit reporting agencies must disclose to the consumer the identities of recipients of the consumer's credit report. Families deserve the same transparency for their children's information.

Another key information practice is data security. FERPA does not include any data security or breach notification obligation and a disturbingly large number of school

[17] Google, Protecting students with Google Apps for Education, Apr. 30, 2014 http://googleenterprise.blogspot.com/2014/04/protecting-students-with-google-apps.html

contracts with vendors fail to include security obligations or requirements.[18] With major security breaches occurring on an almost daily basis and with reported failures by education technology services to implement even minimal security,[19] student information needs legal protection that includes security and breach notification obligations.

5. Update FERPA enforcement remedies and oversight

The only sanction available under FERPA is the denial of federal educational funds by the Department of Education. This is a "nuclear option" and, to date, the Department has never issued such an order. FERPA needs to have a graduated range of remedies and broader enforcement capabilities, including fines and enforcement by the Federal Trade Commission and the state attorneys general along with the Department of Education.

The lack of a private right of action under FERPA means that victims and their families have no redress or remedy for the violation of a child's privacy.[20] For basic fairness, families should have a direct means of redress when their children's privacy is violated.

Lastly, FERPA confers guidance and oversight to the Department of Education that has a poorly funded office by comparison to the Office of Civil Rights in the Department of Health and Human Services where the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) are enforced.[21] FERPA can be more effective if Congress enhances the Department of Education's capacity to provide guidance and oversight. Likewise, educational privacy would be better served under FERPA if Congress were to encourage the states to create Chief Privacy Officer roles to provide local guidance through the respective state departments of education.

Recommendation

Congress can no longer wait to reform federal educational privacy rights. Congress should modernize FERPA to:

---

[18] In 2013, a Fordham CLIP study found that 40% of school data hosting agreements failed to require any data security and in other categories of services 33% or more of the agreements failed to require the deletion of student information at contract termination. See Fordham CLIP 2013 Study, *supra note 3*, Executive Summary, pp. 1-2.

[19] See Natasha Singer, Uncovering security flaws in digital education products for school children, NY Times, Feb. 9, 2015, p. B1 www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html

[20] Gonzaga Univ. v. Doe, 536 U.S. 273 (2002)

[21] For an interesting discussion of government agency privacy oversight activity, *see* Robert M. Gellman, *Who is the more active privacy enforcer: FTC or OCR?*, Concurring Opinions, Aug. 23, 2013, http://concurringopinions.com/archives/2013/08/who-is-the-more-active-privacy-enforcer-ftc-or-ocr.html

- **Protect all student information and not just "educational records" as conceived in 1974**
- **Apply directly to vendors**
- **Authorize the use of student information for specified educational uses and prohibit non-educational uses of student information**
- **Expand transparency obligations and add data security requirements**
- **Provide a range of enforcement remedies**
- **Encourage states to create Chief Privacy Officers**

Thank you again for the opportunity to participate in this hearing and for your consideration of my testimony.

Biography

Joel R. Reidenberg holds the Stanley D. and Nikki Waxberg Chair at Fordham University where he is a professor of law and the Founding Director of the Center on Law and Information Policy ("Fordham CLIP").

Professor Reidenberg is an expert on information technology law and policy. He is an elected member of the American Law Institute and serves as an Adviser to the *ALI Restatement of the Law Third on Information Privacy Principles* His published books and articles explore both information privacy law as well as the regulation of the internet. He teaches courses in Information Privacy Law, Information Technology Law, and Intellectual Property Law. He has taught as the inaugural Microsoft Visiting Professor of Information Technology Policy at Princeton University and has held appointments as a visiting professor at the Université de Paris 1 (Panthéon-Sorbonne), at the Université de Paris V (René Descartes), Sciences Po-Paris and at AT&T Laboratories - Public Policy Research .

Professor Reidenberg has served as an expert adviser on data privacy matters for the U.S. Congress, the Federal Trade Commission and the European Commission. He also served as a Special Assistant Attorney General for the State of Washington in connection with privacy litigation. Reidenberg has chaired the Section on Defamation and Privacy of the Association of American Law Schools (the academic society for American law professors) and is a former chair of the association's Section on Law and Computers.

Prior to coming to Fordham, Reidenberg practiced law in Washington, DC, with the international telecommunications group of the firm Debevoise & Plimpton.

Professor Reidenberg received an A.B. degree from Dartmouth College, a J.D. from Columbia University, and both a D.E.A. droit international économique and a Ph.D in law from the Université de Paris -Sorbonne. He is admitted to the Bars of New York and the District of Columbia.

Protecting Privacy
in Connected Learning
A CoSN Leadership Initiative

Ten Steps Every District Should Take Today

With so much uncertainty about what districts can or should be doing to help ensure the privacy of student data, it would be easy to lose sight of some very concrete steps that can be taken today.

1. **Designate a Privacy Official**—A senior district administrator needs to be designated as the person responsible for ensuring accountability for privacy laws and policies. This is a "divide and conquer" issue, but someone needs to be in-charge.

2. **Seek Legal Counsel**—Make sure that the legal counsel your district has access to understands education privacy laws and how they are applied to technology services. Do not wait until there is a pressing issue that needs to be addressed.

3. **Know the Laws**—Many organizations have and will be publishing privacy guidance for schools, such as the toolkit CoSN toolkit available at http://www.cosn.org/privacy. The US Department of Education's Privacy Technical Assistance Center is a must-know resource at http://ptac.ed.gov/.

4. **Adopt School Community Norms & Policies**—Beyond the privacy laws, what does the school community really expect when it comes to privacy? Seek consensus regarding collecting, using and sharing student data.

5. **Implement Workable Processes**—There must processes for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to processes. Once enacted, the processes should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws and policies.

6. **Leverage Procurement**—Every bid or contract has standard language around a wide range of legal issues. By adopting standard language related to privacy and security you will make your task much easier. Unfortunately, many online services are offered via "click-wrap" agreements that are "take it or leave it." You may have to look for alternatives solutions if the privacy provisions of those services do not align with your expectations.

7. **Provide Training**—Staff need training so they will know what to do or why it is important. Annual training should be required of any school employee that is handling student data, adopting online education apps and contracting with service providers. Privacy laws represent legal requirements that need to be taken seriously.

8. **Inform Parents**—Parents should be involved in the development of privacy norms and policies. Just as schools provide information about online safety and appropriate use, they need to put significant effort into making sure that parents understand the measures taken to protect student privacy.

9. **Make Security a Priority**—Privacy starts with security. Secure the device, the network and the data center. Toughen password policies. Have regular security audits conducted by a third party expert.

10. **Review and Adjust**—Interpretations of privacy laws are changing and new laws may be added. School policies and practices will need updating and adjusted so that they reflect legal requirements. Processes can become burdensomand when that happens, some people may want to skirt the process.

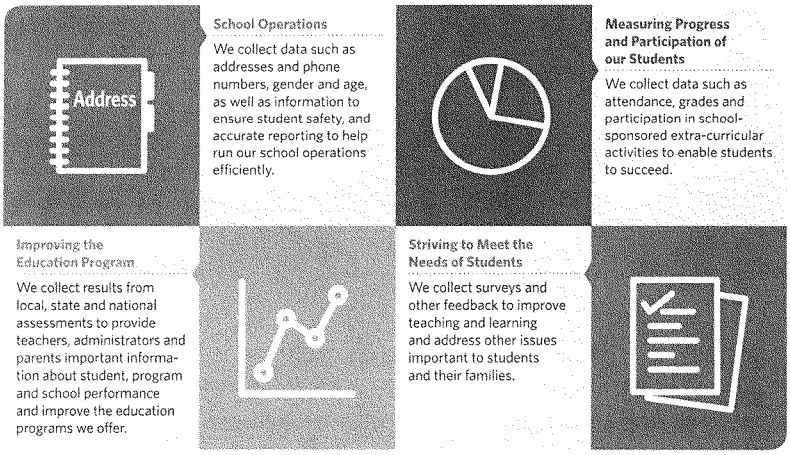
Excerpted from Making Sense of Student Data Privacy (May 2014), authored by Bob Moore, Founder, RJM Strategies LLC and supported by Intel. The full report can be found at http://www.k12blueprint.com/privacy.

CoSN
LEADING EDUCATION INNOVATION
COSN.ORG/PRIVACY

Parents and guardians want assurances that personal information and data about their children are secure and protected by our school system. These questions are rising as we use the Internet, mobile apps, cloud computing, online learning and new technologies to deliver exciting new education services.

At our school we strive to be clear about what data we collect, how data supports your child's education and the safeguards in place to protect that data.

What Data do We Collect and Why?



How Education Data Supports Student Success and School Improvement

data=success!

TEACHERS need data to understand when students are thriving and when they need more support in learning specific concepts.

PARENTS and guardians need access to their child's educational data to help them succeed.

STUDENTS need feedback on their progress so they can make good decisions about program choices and prepare for success.

SCHOOL OFFICIALS and community members need to understand school performance and know if scarce education resources are being allocated fairly and effectively.

How is Education Data Protected?

We follow federal and state education privacy laws and adhere to privacy and security policies.

» For example, the Family Education Rights & Privacy Act (FERPA) gives parents rights related to their children's education records and personally identifiable information. Additional information is available in our annual notice to parents of their rights under FERPA and from the U.S. Department of Education at http://familypolicy.ed.gov/.

When we use an online service provider to process or store data, they also must adhere to certain federal and state and privacy laws. We also expect them to use current security protocols and technology.

» Additionally, the federal Children's Online Privacy Protection Act (COPPA) prevents child-directed websites and apps from collecting certain personal information from anyone under 13 years of age without parental permission. Our school system may consent on behalf of parents in the education context when student information is collected for the school's exclusive use and benefit and for no other commercial purpose.

» Under FERPA, our vendors cannot use the education records we provide in any way that is not authorized by the school district. They cannot sell this data or allow others to access it except as we permit in accordance with federal and state education privacy laws.

Our Commitment

We are working to improve your children's education by ensuring it meets their unique needs. It would be very difficult to accomplish this goal without the ability to capture important information about your child's progress. Protecting personal information in secure and responsible ways is at the heart of our efforts to provide a richer and more dynamic learning experience for all students.

LEARN MORE about the rights of parents and guardians at **dataqualitycampaign.org/pta** or **PTA.org/Parents** or **commonsensemedia.org**

Protecting Privacy
in Connected Learning

Security Questions to Ask of An Online Service Provider

It is important to understand your provider's security practices to ensure that data shared with and collected by the provider remain private and protected. You should work with your School System's security point of contact to determine whether the security practices of the provider comply both with School System policies and applicable laws. While neither FERPA nor COPPA prescribes specific security standards, school systems should look to industry suggested practices when assessing an online service provider.

The following is a non-exhaustive list of key security questions to discuss with your provider. A service level agreement (SLA) should include as many of these considerations as possible.

Data Collection

- What data does the provider collect?
- What, if any, data is collected by 3rd parties (e.g., via cookies, plug-ins, ad networks, web beacons etc.)?

Network Operations Center Management and Security

- Does the provider perform regular penetration testing, vulnerability management, and intrusion prevention?
- Are all network devices located in secure facilities and under controlled circumstances (e.g. ID cards, entry logs)?
- Are backups performed and tested regularly and stored off-site?
- How are these backups secured? Disposed of?
- Are software vulnerabilities patched routinely or automatically on all servers?

Data Storage and Data Access

- Where will the information be stored and how is data "at rest" protected (i.e. data in the data center)?
  - Will any data be stored outside the United States?
  - Is all or some data at rest encrypted (e.g. just passwords, passwords and sensitive data, all data) and what encryption method is used?
- How will the information be stored? If the cloud application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers?
  - FERPA requires that records for a school be maintained separately, and not be mingled with data from other school systems or users.
- Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- How does the provider protect data in transit? e.g. SSL, hashing?
- Who has access to information stored or processed by the provider?
  - Under FERPA, individuals employed by the provider may only access school records when necessary to provide the service to the School System.
  - Does the provider perform background checks on personnel with administrative access to servers, applications and customer data?
  - Does the provider subcontract any functions, such as analytics?
  - What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?
- If student or other sensitive data is transferred/uploaded to the provider, are all uploads via SFTP or HTPPS?

Data and Metadata Retention

- How does the provider assure the proper management and disposal of data?
  - The provider should only keep data as long as necessary to perform the services to the School.
- How will the provider delete data?
  - Is data deleted on a specific schedule or only on termination of contract? Can your School request that information be deleted? What is the protocol for such a request?
- You should be able to request a copy of the information maintained by the provider at any time.
- All data disclosed to the provider or collected by the provider must be disposed of by reasonable means to protect against unauthorized access or use.
- Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession.

Development and Change Management Process

- Does the provider follow standardized and documented procedures for coding, configuration management, patch installation, and change management for all servers involved in delivery of contracted services?
- Are practices regularly audited?
- Does the provider notify the School System about any changes that will affect the security, storage, usage, or disposal of any information received or collected directly from the School?

Availability

- Does the provider offer a guaranteed service level?
- What is the backup-and-restore process in case of a disaster?
- What is the provider's protection against denial-of-service attack?

Audits and Standards

- Does the provider provide the School System the ability to audit the security and privacy of records?
- Have the provider's security operations been reviewed or audited by an outside group?
- Does the provider comply with a security standard such as the International Organization for Standardization (ISO), the Payment Card Industry Data Security Standards (PCI DSS)?

Test and Development Environments

- Will "live" student data be used in non-production (e.g. test or development, training) environment?
- Are these environments secure to the same standard as production data?

Data Breach, Incident Investigation and Response

- What happens if your online service provider has a data breach?
- Do you have the ability to perform security incident investigations or e-discovery? If not, will the provider assist you? For example, does the provider log end user, administrative and maintenance activity and are these logs available to the School System for incident investigation?

Suggested Contract Terms

After your School System chooses an online service provider, it is important to draft a contract that specifies how the provider will comply with your School System's security requirements. Drafting a contract should be done under the guidance of your School System's legal counsel; however, the following suggested contractual terms identify key components to consider including.

The contract should specify the services to be provided and the provider's obligations, including the following:

1. **Contract Scope**. Identify all elements that comprise the agreement and what order of precedence is followed in the event of a contradiction in terms. Identify any contract terms that are incorporated by reference (e.g. URL).

2. **Purpose.** If you have determined that the provider qualifies as a "school official" under FERPA and you will use the school officials exception as the vehicle for disclosing FERPA protected information to a provider, specify: (i) that the provider is considered a school official, (ii) the legitimate educational interest that the provider is fulfilling, (iii) the nature of the data collected, and (iv) the purpose for which any FERPA protected information is being disclosed.

3. **Data Collection, Use and Transmission.** Specify how the provider may use or collect data from the School System and your students, and any restrictions that may apply to the provider's use of that data and ensure that you bind the provider to those uses and restrictions. At a minimum, you should address the following:
   - Specify that the provider should only be permitted to use any information stored, processed, or collected as necessary to perform the services for the School System. Include a specific restriction on the use of student information by the provider for advertising or marketing purposes, or the sale or disclosure of student information by providers.
   - Specify any metadata the provider will collect (e.g. logs, cookies, web beacons, etc.).
   - Specify any data and metadata any 3rd party will collect (e.g. analytics, etc.) as a function of the use of the provider's service.
   - Specify that the provider should be restricted from accessing, collecting, storing, processing or using any school records, and student or parent information, for any reason other than as necessary to provide the contracted services to your School.
   - Specify when and how the provider may disclose information it maintains to other third parties. Under FERPA, providers may not disclose education records provided by your School System to third parties unless specified in your contract.
   - Specify whether the School System and/or parents (or eligible students) will be permitted to access the data (and if so, which data) and explain the process for obtaining access. Consider if the contract needs to specify whose responsibility it is (the provider or the School System) to obtain parental consent and facilitate parent's request to access student educational records.

- Specify that data collected belongs to the School System (and/or its users) and that the provider acquires no rights or licenses to use the data for purposes other than for the delivery of the service.
- Specify that a provider must disclose if it will de-identify any of the FERPA protected data that it will have access to and if so, require that the provider supply details of its de-identification process. When appropriate, you may want to retain rights to approve such a process prior to the provider using or sharing de-identified data in ways that are beyond the purpose for which any FERPA protected information is disclosed.

4. **Data Security.** Specify any security requirements that the provider must follow to the extent that it maintains, processes, or stores any information on behalf of the School System. At a minimum, the contract should address the following:
   - The provider must securely maintain all records or data either received from the School System or collected directly from the school, teachers, students, or parents in accordance with the security standards designated by the School.
   - Information, content and other data collected and stored from and on behalf of the School System and the students should be stored and maintained separately from the information of any other customer, school, or user.
   - The provider should restrict access to your School System's information to only those individuals that need to access the data in order for the provider to perform the agreed-upon services.
   - The agreement should identify what happens if the provider has a data breach. The agreement should identify the provider's responsibilities including the School System's point of contact, required notification time, and any obligations for end user notification and mitigation.
   - You should have the right to audit the security and privacy of your School System's or students' records or data.
   - Require the provider to notify you in writing about any changes that will affect the availability, security, storage, usage or disposal of any information.
5. **Data Retention and Disposal.** Assure the proper management and disposal of data or information pertaining to the School or its students. All data disclosed to the provider, or collected by the provider, must be disposed of by secure means to ensure that it is protected from unauthorized access or use.
6. **Bankruptcy or Acquisition.** Specify what happens to the data if the provider goes out of business or is acquired by another firm. Is there a source code or data escrow provision?
7. **Service Levels and Support**.
   - Specify the service levels the provider must meet and any credits you receive for any failure by the provider to meet these service levels.
   - Require the provider to supply the School with all the technical assistance you may need to use the services.

8. **Governing law and jurisdiction.** Typically a provider's default contract will specify that it is governed by the law of the provider's home state. Public institutions generally have significant restrictions on their ability to consent to such provisions under the School System's local state laws.
   - Check with your legal counsel about what law can govern contracts entered into by your School in light of your School's state laws.

9. **Modification, Duration, and Termination Provisions.** Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider. Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession, including archives and/or backups.

10. **Liability**. The provider should be liable for the activities of its staff and subcontractors.
    - The provider should generally have an obligation to comply with all applicable laws, including privacy laws.
    - If the provider will be collecting data from children under the age of 13, the provider should comply with COPPA.
    - The provider should be liable for any breaches in security or unauthorized third party access arising out of the provider's breach of its contract obligations.
    - The provider should be liable to the School System for any claims or damages that arise as a result of the provider's failure to comply with its obligations as a Cloud Service Provider under COPPA, FERPA, or other applicable laws.
    - Limits of liability should be consistent with market-tested commercial practices and should appropriately allocate risk between the Vendor as a Cloud Service Provider and the Customer as the owner of its Data.
    - The School System may wish to identify through negotiation specific categories of direct damages that would be excluded from traditional definitions of consequential damages.

*Endorsed by **The Association of School Business Officials International.***

Chairman ROKITA. Thank you for your testimony.

The way this usually works is the subcommittee chairman usually asks out with asking his questions. But I find out that my life goes smoother when I defer to the full committee chairman when he is in the room.

Sir, thank you for your leadership. You are recognized for 5 minutes.

Mr. KLINE. Yes, that won't work. Okay. Thank you, Mr. Chairman. This is a good hearing. Thanks for yielding to me to ask a question. I really want to thank the witnesses. You are an excellent panel. Years of expertise.

When we look at data and data privacy in the large, we as Americans ought to be concerned. We have seen spectacular reaches, big retail firms where all of their customers' information was made available to whoever was doing the hacking. Because these cyber attacks are not just a matter of rhetoric, they are a matter of fact. And so whenever you have data that is compiled, today, we have to be somewhat concerned that data will be made available. So as we look at this, we need to keep that in mind.

And I am also concerned that when we are dealing with technology—we, the Congress—we, the government. But we, the Congress, particularly—there is a great danger that we will be trundling along here years behind. In the House we move slowly. In the Senate they hardly move at all. And so it is a little troubling that we could be developing policy that by the time it is enacted is already outdated.

So I could probably start anywhere, but I am going to go to Ms. Knox to—I would like for you to get at the issue of the amount of technology that there is in the classrooms. It is not a simple question of the paper file drawer now being on a flash drive somewhere. There is all kinds of stuff. We have got hardware, software, apps, tablets, kids with cell—we have all kinds of things going on there.

So can you help us understand some common principles or ideas that we should be looking at when we are trying to update FERPA that will not get in the way of supporting technology in the classroom, but which can provide some privacy and something that won't be outdated tomorrow or in a week or something like that? Just give it your best shot.

Ms. KNOX. Sure, sure. I think starting with a commitment to trust is important. I know that at our company, we have principles and policies in place about establishing trust with customers. So starting with a commitment is always important. And then, you know, knowing what it is you believe. For example, in our company, we believe that people own their own data; right? So the student and the parent—the student's data belongs to them. So being clear on those pieces sort of guide, then, action and belief.

So then how does that translate? At least, again, where I work, that translates into making sure that privacy is in the design of any product that we put on the product. So if we design a product, there is always a privacy expert with the product developer. That means you are baking it in to who it is and what it is you are going.

And then, you know, wherever we go, we try to be extremely transparent about the data. So I know that the question has to do

with schools and there are all these different devices and how do you make sure that data stays secure. The cloud, you know, unites them, right, brings them all together. And it is a service of—in a remote data center, basically—and educating and becoming clear and being very transparent. Whoever that third-party provider is needs to articulate in the clearest terms how that data flows in and out, who has—if anyone have access.

And we have an entire center called the trust center. We have a trustworthy computing initiative. This morning I actually watched a couple of videos of some software engineers who took me on a virtual tour of our data centers. And I could see physical, you know, protections. I could see software protections. I could see a blue team and a red team identifying good and bad use. I mean, being transparent helps inform, but it also decreases fear. Because we believe data is critical in the age of 21st Century education, just like everybody else does.

And then two other points is, you know, in general, always committing, putting something in place where improvement continues. So whatever the law ends up doing—you know, whatever direction it goes in, there should be a piece in there that says we will constantly improve our practices based on the times and the opportunities that come available.

We do that at the company, as well. So that is, again, part of the way that we approach our work, the way that we, you know, commit to it, believe in it, act on it, create products. And I think that can be translated into the way that society sort of behaves when designing laws for students and their privacy.

Mr. KLINE. Thank you. I see my time is expired, Mr. Chairman. Thank you.

Chairman ROKITA. Gentleman's time is expired. And I see that this subcommittee's ranking member believes in a similar philosophy as I do. So Ranking Member Scott, you are recognized for 5 minutes.

Mr. SCOTT. Nice try. Thank you. And I want to thank all of our panelists. They have provided really good information. Let me just ask some general questions.

When you talk about personal data, is there anything in the discussion that will hurt us in trying to find growth models or trends, demographic trends, that in general we could use for educational purposes? Is there anything that—nonpersonal information, nonpersonally-identifiable information, is that at risk if—in any of our discussion? In other words, boys do better than girls in some areas, some pedagogy works better with some groups other than others. Are we gonna lose our ability to evaluate along those lines?

Mr. REIDENBERG. Yes, can I respond, Congressman? I don't think so. Because if the focus of FERPA is looking at using data appropriately for educational uses, that is going to be a very important educational use to understand how individual children learn, how cohorts of children learn, and how to deliver the most effective educational programs for them.

Mr. SCOTT. I just wanted to make sure that is not at risk.

Mr. Reidenberg, you indicated the problem with sanctions. We have got a problem with classified information. If a reporter gets classified information illegally, meaning somebody illegally has

classified information, gives it to a reporter, there is apparently no prohibition against the reporter just sticking it in the newspaper.

What about republication of data and other kinds of breaches? You alluded to the fact that we need the graduated sanctions so there will be some sanction. If there is a breach, would there be any prohibition against the rebroadcast or republication of the data? Is that part of FERPA?

Mr. REIDENBERG. You are talking about, say—take an example. Nashville, Tennessee a number of years ago had all of the information on all of the cities' students and their families openly available on the internet. A case like that, if you are talking about a newspaper publishing information from it, well, the First Amendment rights would address what the scope of the newspaper's authority to do that.

But if you are talking about a third-party organization taking all that data and then using it for various commercial purposes, I think that would be wrong and should be interdicted.

Mr. SCOTT. One of the questions is what is an educational record. Is homework, grades on quizes, exams, final grades, disciplinary records, financial records, are all those educational data that needs to be protected? Computer use, if you are using the library computer?

Mr. REIDENBERG. Those I do not believe are currently covered by the definition in FERPA. The Supreme Court has interpreted the educational record specification quite narrowly. So homework assignments, for example, would generally not be. A family's financial status; so if the child is on a reduced lunch program, for example, that is not going to be considered necessarily part of the educational record. How a child uses an app in school, the metadata generated from that app will be outside the scope of protection from FERPA.

And I think it should be. I think when you are dealing with data that is gathered about, by, or for kids in school, we should be treating that as custodians of our children's privacy, and we should be very careful with how that information gets used.

Mr. SCOTT. So stuff like that is not now covered, but should be covered?

Mr. REIDENBERG. I believe that is correct.

Mr. SCOTT. And part of the discussion is how long should the information be held? Somebody has graduated from high school, should the high school still have their stuff on some computer that somebody can get to?

Mr. REIDENBERG. I think it is going to depend on what the purpose is for the high school archiving it. Should the high school, for example, or the high school's vendor be storing the seventh grade home work assignment that Johnny or Sally wrote when they are 35 years old? I think the answer to that is probably no.

Mr. SCOTT. Let me ask you just another quick question. How do the marketers get this information? I mean, I think we would all agree you shouldn't be marketing people. How do they get the information to begin with?

Mr. REIDENBERG. If you ask me the question in a couple of months, I should be able to give you a specific answer. We are in the midst of doing a study right now in my research center that

is trying to understand the circulation of the student information in the commercial student marketplace. And I don't have an answer for you at this point.

Ms. KNOX. So your question is how does student data end up in the hands of marketing people. If the students are using certain cloud infrastructures and it is held by a third party and that third party's contract terms aren't clear, it is possible for them to trend through the data that flows. So emails, forms that the school district is completing. I am sure Dr. Abshire may have some specific examples of maybe situations.

But when it is flowing through the data center, it is possible to, you know, take a peek at it and find trends and put it kind of on the market to other businesses who want to advertise to those students. And then certain targeted ads then would flow back to the students. And when again they are emailing, low and behold, what they were talking about maybe in an email 6 months ago, there is an advertisement for it.

So this idea of trust and understanding where the data is flowing and committing to not using data for noneducational purposes becomes critically important in this information.

Chairman ROKITA. Thank you very much. The gentleman's time is expired.

I now recognize myself for 5 minutes. And in the first 20 seconds give Dr. Abshire a chance to respond to that last question, if she would like.

Ms. ABSHIRE. I guess I would just comment that the comment around trust I think is critically important. Also, the comment I would make is about how we at the district level should anonymize data. If you think about all that we collect about children—there was some earlier comment about large-scale demographic data. That data coming out of a school district usually is and should be anonymized so that it is reported in a way that it is not PII, it is not personally identifiable information. It indicates trends. It allows researchers and states to look at those trends and make solid educational decisions.

The other piece is the use of role-based data. In other words, depending what your role is in the school district or an organization, that limits your access to certain pieces of information. We have been very successful with that, and we are working on that in the—

Chairman ROKITA. And does that work in a cloud situation?

Ms. ABSHIRE. Absolutely.

Chairman ROKITA. Okay.

Ms. ABSHIRE. The pending and the agreements that are in place with our providers allow for that data to be—

Chairman ROKITA. And who writes your agreements? Who writes your agreements? You have outside counsel?

Ms. ABSHIRE. We work on that with counsel in the district and with our state department. Yes, sir.

Chairman ROKITA. Okay. Thank you. Very interested in all your testimony. So many questions, so little time.

I am going to start with Ms. Knox. You rightly praised the pledge that you signed. And now we have 100 other signatories to it. Good stuff. Where is the enforcement mechanism in the pledge?

Ms. KNOX. I know—

Chairman ROKITA. Assuming it was codified.

Ms. KNOX. Right. Oh, assuming—well, the existing penalty would be, you know, misleading. And if you actually do different activities than you said you would do in the pledge, then the FTC can fine you.

Chairman ROKITA. Okay. And then you also mentioned that FERPA, you mentioned correctly, does not include third parties.

Ms. KNOX. Right.

Chairman ROKITA. Should it?

Ms. KNOX. Yes.

Chairman ROKITA. Thank you. Mr. Reidenberg, same question. You mentioned the same thing.

Mr. REIDENBERG. Yes. I Think FERPA should absolutely apply to all participants in this space, which would include the third-party vendors. I—

Chairman ROKITA. Can you give some more specificity of what that would look like in an updated FERPA—

Mr. REIDENBERG. Sure.

Chairman ROKITA.—environment?

Mr. REIDENBERG. What FERPA should—what I think FERPA should be doing is specifying the kinds of uses that are permitted for student information. And uses that don't fall within that category would require consent. And that requirement of only using for admissible purposes would apply whether it is the school, whether it is a data analytics firm, whether it is some other cloud service provider offering services to the school.

Chairman ROKITA. So as long as there is some contractual relationship between the government jurisdiction or school element and the service provider, that would extend FERPA?

Mr. REIDENBERG. It would—there would always be that contractual arrangement where the school is using third-party services.

Chairman ROKITA. Right. Ms. Knox, you wanted to add something?

Ms. KNOX. Just really quickly, one of the things I really liked about Dr. Abshire's written and what you mentioned in your oral is she talked about not overburdening schools with more regulation. And I can't agree more. And I think that was part of the brilliance of the Student Privacy Pledge. And I just want to thank Representative Polis for his leadership there. The idea of industry standing up and raising our hand and taking a pledge and saying these are the kinds of things we think we should be doing and we will do them when it comes to students, I think it is important, and I think it does help with schools.

Chairman ROKITA. I thank you. But the question was on FERPA; right?

Ms. KNOX. Right. But I think it could translate right into FERPA. I mean, not word for word. But the same principles. There could be a new piece of FERPA that developed that looks at third party or business—

Chairman ROKITA. Absolutely. Absolutely. Thank you.

And with the time remaining at 1 minute, Ms. Sevier, what do you think about what has been said so far? Do you have comment to add?

Ms. SEVIER. I do. It sounds like we are all speaking on behalf of student privacy. And I just wanted to bring up the parent engagement aspect. If parents are not able to review digital records and if digital records are not included in the definition of a child's educational record, then that kind of relegates the parents to being a bystander in the process, and not a participant. And I think we need parents as participants. We need them involved.

Chairman ROKITA. Absolutely. They are the first guardians of all this. Literally.

Ms. SEVIER. Yes. We need them to be involved. If a digital profile is going to guide my children's opportunities, whether they graduate, whether they are eligible for services, I want to review that. I want to be involved. I want know how those determinations were made. And right now, unless I am in her school district, I don't necessarily have that opportunity.

Chairman ROKITA. Thank you all again.

Ranking Member Fudge, you are recognized for 5 minutes.

Ms. FUDGE. Thank you very much, Mr. Chairman. And again, thank you all for your testimony.

Let me start with you, Dr. Abshire. You have kind of been talking around it. But can you just give me some specifics about what you believe we can do or how FERPA can be modified to reflect the change in technological climate, while still ensuring that children's data is protected?

I mean, I understand, you know, that you don't want us to put more onerous restrictions. And I understand that too. But my priority is children. And so if—you know, maybe it is a little much and we can work on it. But how can we protect these children? What do we need to do with FERPA?

Ms. ABSHIRE. Well, thank you, Congressman Fudge. I appreciate that question.

I think the comments of my colleagues here at the table this morning have kind of encompassed that; that the revisions do need to be made with an eye towards a balanced approach. I would come down strongly on the side of ensuring parental engagement and involvement. In our district it is called "informed consent." Our parents are allowed to consent and opt in and out on different pieces of data around their children's educational records.

So they know that when they give informed consent, that student data around discipline, student data around a children's progress on formative and summative assessment results are gonna be used within the district with privacy with the educational experts that need access to make good decisions about that child's educational progress.

They also know that it is gonna be sent to the state to be able to assimilate that information and look at how our district performs against other peer groups in the state and on national levels. They also know that information will be anonymized for certain requests and it will not leave the district. It will not go out into the cloud and be available for potential data breaches.

So I think the strongest piece that I can bring to the table around that issue, Congresswoman, is the piece of informed consent; that it is, I think as Chairman Rokita said, the parents are the first guardians. And the culture of a community in Louisiana—

Ms. FUDGE. I don't want to cut you off, but I have got some other questions I must ask, so—

Ms. ABSHIRE. I am sorry—

Ms. FUDGE. So parental consent. Ms. Knox, what has Microsoft actually done to protect the data?

Ms. KNOX. Well, great for us we have some lead amazing products. And I feel lucky that I get to go out into classrooms and talk to actual teachers who use them. Office 365 being in the classroom. And these are specifically designed so that students don't receive any unwanted advertisement. And so they—a teacher can—as one teacher told me, no more in my classroom can anybody come back from doing their homework and say their dog ate their home work. Because everything is now stored in the cloud. And there is more productivity. Kids are really engaged. This office 365 product has really inspired him to do new things with technology; collect data, do analytics on which equation he is teaching about, you know, students struggled with the most at night and didn't struggle as much on this equation, so he changes his teaching strategy.

So all these things are great. But at the same time, we need to make sure that they are—that the student is protected and they are safe. And that is what these products do. It is possible to strike the balance that Dr. Abshire keeps talking about.

Ms. FUDGE. Thank you very much.

Dr. Abshire, can you give me an example of how your district uses this data dashboard to effect curriculum decisions and to provide interventions for struggling students?

Ms. ABSHIRE. Yes, Congresswoman. Thank you.

Teachers regularly meet in our district in what we call PLCs, professional learning communities. And those communities are focused on looking at how students are performing. And in the past it was a set of folders. It was stacks of information that people could not cross tabulate the data and, again, look for trends and look for specificity in what skills and standards are students not able to make.

Now in our direct, our teachers sit in conference rooms with the fourth grade team or a group of math teachers at the high school level and pull on a computer screen all the trends for the students in their classrooms, drilling down to a specific skill that don't know. So they are able to pull out students into groups, reteach that specific skill, and allow other students to move on.

What that data warehouse for us has created is efficiencies in learning and efficiencies in teaching.

Ms. FUDGE. Thank you very much, thank you very, very much. I yield back, Mr. Chairman.

Chairman ROKITA. Thank the gentlelady.

I would now like to recognize a new member of the committee and subcommittee who has served on school boards in Florida.

Mr. Curbelo, you are recognized for 5 minutes.

Mr. CURBELO. Thank you, Mr. Chairman, for this opportunity to discuss what is a topic that is increasingly on the minds of parents and students and teachers.

I wanted to delve further into the issue with penalties related to FERPA violations. Mr. Reidenberg mentioned that we should perhaps consider developing a graduated penalty system. Could you go

into that, expound what would something like that look like and how could it be most effective?

Mr. REIDENBERG. Thank you. I think my reference to graduated penalties, what I have in mind, are range of levels of fine depending on egregiousness of violation. So you would not want to see a school district or a state subject to crippling penalties for what are small technical violations.

On the other hand, we need to have some mechanism to insure that FERPA is, in fact, effectively enforced in local schools across the country. I think—so on the one hand, those are the publically-assessed fines. I think it is important that families have an ability to get redress if their information is compromised and their student's privacy rights are violated and they are harmed. Right now, we have no mechanism for that in FERPA. It is one of the few areas in American privacy law where we have no way of addressing redress.

Mr. CURBELO. Now, I also heard a conversation about expanding FERPA to cover third-party vendors—

Mr. REIDENBERG. Yes.

Mr. CURBELO.—for example, how ould those groups be penalized? Same way?

Mr. REIDENBERG. Same way. Same way. If FERPA is authorizing use for a defined educational purpose and the third-party vendor does something else; something else being using it for advising purposes, using it to profile a student to skew search results or to deliver content that is unrelated to the educational purpose for which the data was gathered. In an instance like that, the third-party vendor should be subject to a fine.

Mr. CURBELO. And a question for Ms. Sevier.

It is obvious that these types of breaches occur every day. Obviously, most of them do not rise to the level where they would get attention from the media. But how much do parents know about these beaches? Do you get the sense that schools are open and transparent about data breaches, or is there a lot that parents and even we don't even know?

Ms. SEVIER. That is an interesting question. And I think that there are layers of misunderstanding, depending on how involved the parent is in the landscape. But I also think that the reason that question is most interesting is because the way that the law is written right now, there is release of information that is not considered a breach. Does that make sense? And I think that is really the focus of revising FERPA and kind of shoring up those areas; really looking at the digital information that is being collected and stored, informing parents not just how it is being collected and stored and who is using it, but how it is legitimately being applied within the school, and then allowing them to review that.

And I would say that dialogue at that level is not happening, but that we are taking first steps with partners, like Microsoft, to get information out to parents so that they play more of an active role in shaping policy, at least at the district level.

Mr. CURBELO. Thank you.

Ms. Knox, I think you wanted to weigh in?

Ms. KNOX. Just in terms of the confusion that parents may find. We hosted last month—or in December—approximately 30 state

PTA leaders in our office. And we conducted a 2-day training on student privacy. Everything from personalized learning to what is cloud computing to—I mean, I can't—what is data-driven instruction.

But one of the most interesting moments, I think, for all of us was none of the adults had actually experienced personalized learning. And so they had never—I mean, those were words and terms. And so once they felt the power of oh, my gosh, I get to move on quicker based on the data because I am actually learning quicker than this person, but this person might come and help me, they got really excited once they experienced it.

But then they also thought where is all this data going? And then breaking down the cloud and how that works. And it was just a fascinating—I don't know if you want to mention—or comment. But it was good.

Mr. CURBELO. Please.

Ms. SEVIER. It was fascinating. And it enabled our state leaders to go back to their states and kind of mimic that same behavior with their constituents so they were informed advocates around the issue. And it decreased the amount of hyperbole. And I think it makes us better decision makers.

Mr. CURBELO. Thank you all very much.

Thank you, Mr. Chairman. My time is expired.

Chairman ROKITA. Thank the gentleman.

Ms. Bonamici, you are recognized for 5 minutes.

Ms. BONAMICI. Thank you very much, Chairman Rokita and Ranking Member Fudge, for holding this very important hearing.

Thank you to the witnesses. This is an important issue. And I hear a lot from many constituents in Oregon who are as concerned as I am about the gaps in protection.

There is always a problem in legislating around technology. Because as was recognized earlier, the technology changes much faster than policy changes. And trying to find that right balance to make sure that we aren't inhibiting innovation and the beneficial uses of technology while still finding protections is a critical balance. But it is past time for us to address that issue.

I want to talk with you, Professor Reidenberg, and say thank you for your excellent recommendations on the changes that are needed to update FERPA. When I think back to—I think you said in your testimony it was 1974. Things were a little different in 1974. And we have come a long way. But the law needs to definitely be updated.

You talked about an analogy to the Fair Credit Reporting Act, permissible purposes provisions, when you talked about educational use. But what about remedies? You said in your written testimony that right now, the denial of education funds by the Department of Education is the remedy.

But what happens, say for example, if a family finds out that there is erroneous information in a database about their student? What can they do? Is there way for them—analogous to the correction of errors provision in the Fair Credit Reporting Act, is there a way for them to correct erroneous information?

Mr. REIDENBERG. Yes. FERPA gives the parents the right to access and request the school district make changes to data that is

incorrect. If a school district does not do that, the parent has no recourse.

The second thing is that doesn't apply to all of the third parties holding that data. So all the educational app providers that are profiling individual children to serve them content or games or learning tools, the parents don't have a legal right to access what those profiles are. And to suggest that the profile really doesn't adequately or accurately describe the child, there is no mechanism for the parent to have it changed.

Ms. BONAMICI. An important issue to address.

And I want to follow up on Chairman Rokita's questioning about the Student Privacy Pledge, which I applaud. That is a great first step. However, I am concerned also about the voluntary nature of it; that it is something that doesn't have adequate enforcement if there is a problem. And again, being voluntary.

So I am also concerned about the issue of conflict. When schools are essentially acting in loco parentis, they are, playing the parent role, in fact, when our students are in their schools. So are schools really equipped to be a go-between in this kind of issue where parents and vendors and school district may have conflicts? How can schools adapt to serve that role?

Mr. REIDENBERG. So if I could address the pledge first, and then the second portion. I mean, I think the pledge is a terrific initiative. I think there are very serious questions about its enforceability; whether if a company signs up for it and does not adhere to it but then presents Dr. Abshire with a contract that is inconsistent with the pledge, and she has had her legal counsel review it, I think it is going to be very hard to claim it is a deceptive practice on behalf of the vendor.

So I think that relying on unfair and deceptive practices as an enforcement tool I think may be difficult. It also means the FTC is the principal enforcer for that. And their staff is simply not equipped to go after that many organizations that might not be following. It is great that there are 100 leading companies that are standing up, but there are thousands and thousands of companies across the country doing these sorts of practices.

Ms. BONAMICI. And as you know, the FTC doesn't represent individuals to begin with. So it would have to be a widespread practice.

Dr. Abshire, did you want to weigh in on this?

Ms. ABSHIRE. Just a quick addition. I think we should make no mistake about the fact that schools are painfully aware of this issue today. None of us is—can ignore, I think as Congressman Kline mentioned, the data breaches that have happened with public information and different companies and people's credit cards.

So we are all aware of this. And at the heart of our role as school district officials, principals, and superintendents and school boards, is the interest of the child. I think the chairman said it quite eloquently. Our role is to educate, protect, and take care of our nation's children.

And so in this area of privacy and security, we have not ignored this. Every meeting I go to around the country there are conversations about this. I am gonna be in California in a couple of weeks speaking to district CTOs from around the country about this issue. And if we find an issue, I don't know of an educational agen-

cy that would say we will not correct the record, that we will not do the right thing by the child; and that if a contract is violated, we have easy recourse. We quit doing business with them.

Ms. BONAMICI. My time is expired. I yield back. Thank you, Mr. Chairman.

Chairman ROKITA. I thank the gentlelady. And I would like to recognize another new member of the subcommittee and committee. Glad to have him, as well.

Mr. Carter, from Georgia. 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman.

And thank you y'all for being here. We appreciate what you do. Nothing more important than our children, and especially their education.

Let me ask you, when we are talking about this information, are we talking about specific information to a specific child? Or are we just talking about general information? Are we talking about, you know, at this school, 40 percent finished in this percentile?

Ms. KNOX. I mean, the way I think about the answer to that question is there is data that is collected in a classroom, right, that informs instruction. Then there is about classroom. Then there is data at the school level. Then there is data at the county level. And then it goes to the state.

And so you are right; there is all these different layers and there are policies that sort of try to blend together and weave together. I keep looking over at Dr. Abshire because she lives this. And so the answer to your question is it is like a fabric or a quilt that needs to kind of work all in the same direction. But there are many different buckets of data at play in the education system.

Mr. CARTER. Are you more concerned with the—I suspect that you are more concerned with the personal data on the specific student than you are about the general data.

Ms. KNOX. I mean, from my point of view, the personal data, why—I am very concerned. I don't want to see kids get viruses that penetrate their system. I don't want them to be—you know, to have data loss or have their passwords exposed. I don't want to have their data sold for inappropriate or un-educational purposes. All those types of things more on the micro or the personal level. But then data can being aggregated and there can—people can look for trends. And then there can be some unwanted advertising that is targeted towards the student or groups of students based on clicks and searches and ways they interact with the technology.

There are lots of ways for data to inform the technology that has been used. And sort of what does the company decide to do with the data that they are collecting? Is it for the purpose of improving the business, or is it actually to be monetized and sold and be making money off the whole process?

Mr. CARTER. Dr. Abshire, when your school system gives the information to a company, do you sell it? Do you get a price? Do you get paid for it?

Ms. ABSHIRE. Well, we don't give information about a student to a company. That data—we have been working on this for a little while. Let me say that. And as we look at PII, personally identifiable information, we have begun to ferret out systems where in

earlier contracts and earlier provisions, we used a lot of PII. And we are anonymizing that data now by using student IDs.

Information is power in this new technology, economy, and educational arena. And if we know that this information has the potential, as Ms. Knox said, to be misused or to be exploited in some way, then it is our responsibility as—it is the responsibility at the school district level to be able to restrict that PII in such ways that these children cannot be identified.

Only within our own discreet systems with the educator or the researcher or the evaluator that needs to use it in a direct line of correlation between that child and their educational records.

So as I said before, this is evolving. It is not an easy issue. Because obviously, the use of technology and information systems in schools is evolving. And it is complex. But it is our opportunity, I think, as a community of policymakers, of parents, of companies, and educators to look at this in a comprehensive way that holistically evaluates what are we doing, what should we be doing, what should happen if we don't do what we are supposed to be doing. And then look at ways that we can support the use of data to inform instruction.

Because I think as all the panelists said, the powerful learning opportunities that this technology provides to advance, remediate, enrich children's learning in ways that didn't happen 40 years ago when I started is the way we would transform schools and create competitive educational environments so our kids can compete within those safeguards. Does that help?

Mr. CARTER. That helps. One last question.

Are there any physical characteristics including in this information? You know, male, female, gender—

Mr. REIDENBERG. Yes. It will be in the metadata. It will be in some of the specific characteristics the child signs up for. An app in school that has an avatar and they are supposed to choose their sex, it will be predictable based on certain patterns that a child engages in school. So the third party can identify those characteristics, even if the child hasn't given the name.

I think it is important though, just giving an ID rather than a student's name is not satisfactory today, given the state of computer science. The computer scientists are able to show you can reverse engineer identity. If you give me several characteristics about an individual that are purportedly anonymized, I can reverse engineer who that child is.

And we see today that in our research we found approximately 25 percent of the school contracts in—I think it was in the classroom function area—were not paid with by cash; they were paid with using their students' privacy. They were giving the vendors information in exchange for the services.

Chairman ROKITA. Gentleman's time is expired.

Mr. CARTER. Thank you all again.

Chairman ROKITA. Thank the gentlemen.

Now I would like to recognize another new remember to the committee, very much welcomed as well. Mr. Russell, you are recognized for 5 minutes.

Mr. RUSSELL. Thank you, Mr. Chairman.

And thank you, panel, for being here today.

FERPA was changed under the leadership of Secretary Duncan, allowing anyone that has even a mild interest in education to see personal records. Would you support the elimination of access by third-party vendors? And that is for whoever would like to take that on.

Mr. REIDENBERG. I am happy to jump in and say no. I mean, third-party vendors serve an important and useful function for the schools. And our schools today would not be able to develop and enhance their educational programs if they couldn't use third-party vendors. So if you cut off access to the information, the schools would have tremendous difficulty delivering education and improving the outcomes for their kids. But that is not to say what those vendors do has to be careful and closely circumscribed.

Mr. RUSSELL. Okay. As a follow on to that, you know, Mr. Reidenberg, you have correctly pointed out in your previous comments about these unique identifiers that are attached that never go away. They are attached to personal level student data. It follows the data no matter where it goes. So disaggregated data is really a myth. So how do you protect that?

And then you are also willing to give it to third-party vendors, because it is all for the children. Well what about the Fourth Amendment of the Constitution of the United States that says we have a right to privacy of our papers? What do we do with that? And I would like to hear someone from the panel address those issues.

Ms. KNOX. I mean, from the company—from Microsoft's point of view, we can operate as a third-party vendor. But our belief system, what we adhere to, our principles and policies, is your data that we are gonna put in a data center offsite, you own that data. We don't own that data, and we will not access it. And so we have that in our contract. And that is, I think, a way of addressing and—well, addressing the issue, but increasing trust among all these stakeholders who could access the function—

Mr. RUSSELL. Well, and to that point—and I agree with that. But take the Federal government, for example. They are asking for data from states to fill out such initiatives as the prevention and intervention programs for at-risk youth. They provide grants for the SLDS, the longitudinal data system. Do you think that data from the National Assessment Educational—you know, NAP, do you think that would provide the very things that they are asking for with less specificity on individual students? Why does the Federal government need to drill down to that level?

Ms. KNOX. I think there are lots of ways probably to respond to that question. My big—my general response about the NAPE and the data that is collected, as a general education system as a country, we are trying to constantly improve it. So we are collecting, you know, aggregated data to make good, informed decisions so that we can improve our systems.

Mr. REIDENBERG. Congressman, there is a well-known principle in data privacy which is called "data minimization." And I think the question you are asking is really going to that point; what is the minimum level of data necessary to make the decision that we are seeking? And I think with—and we have done some research

on the SLDSs. And I think there are many questions about the scope and extensiveness.

In fact, it was approximately 4 or 5 years ago I testified before this subcommittee on a study that we did. And the example that I used came from the state of Louisiana. I was just telling Mr. Abshire this before the testimony. Louisiana requires its school districts to report whether children curse in school. And it seems to—because when you look at the disciplinary codes, one of the codes is using—the child is disciplined for using profane language.

And you have to ask the question, is that level of detail necessary? I think in many cases, we will increasingly conclude no.

Mr. RUSSELL. Well, and I appreciates that. And my last question, I mean, if FERPA no longer protects personal student data and we can give no assurances that we can't reverse engineer and find privacy factors, and yet we are still willing to give it to third parties, what makes any of you on the panel believe that the Federal government has a right to do that instead of states?

Local schools, local communities owned by their school boards, their parents, their teachers. Sure, we all accept that.

What gives the Federal government this right that none of you today by your statements, you realize that there are ways around all of this and it can be breached. So why should the—

Mr. RUSSELL.—federal government—

Chairman ROKITA. The gentleman's time is expired. So we will have to get those answers perhaps from the witnesses in writing.

Mr. RUSSELL. That would be great if I could. Thank you, Mr. Chairman.

Chairman ROKITA. Thank the gentleman.

Next, another new member of the subcommittee and committee. Mr. Grothman from Wisconsin, you are recognized for 5 minutes.

Mr. GROTHMAN. Thanks much. I have been concerned about this issue for a long time. And the more the government collects data of any sort—you know, we have seen every agency. Eventually, it is going to get out somewhere. And this is supposed to be confidential data. So it is a scary thing.

But Mr. Reidenberg just said something kind of shocking. And I want you to repeat for me, because I almost fainted, so I didn't hear the whole thing.

The percentage of vendors who are getting, apparently partly in compensation for what they are doing, are sending out data? Could you elaborate on that a little bit?

Mr. REIDENBERG. Yes. The school districts that are getting a service for which they are not paying cash. So the quintessential example is Google apps for education. The school districts aren't paying for it with cash. But what is Google getting? Google is getting the personal information of all of the district's children.

Mr. GROTHMAN. Can you give me an example of that information they are getting?

Mr. REIDENBERG. Home work assignments, communications between teachers and students, presentations that kids are working on in school, if they are working from school, the search items that are being used.

Mr. GROTHMAN. So in other words, if Google wants to sell a product and my niece is working on something on who knows what,

they are gonna know what she has chosen for her, whatever, middle school project or something?

Mr. REIDENBERG. Yes. But Google has now said that they won't use that data to market or advertise to the children. They haven't said whether they would not use that data to develop the product, to create the content for the product.

Mr. GROTHMAN. What else would they be doing with it?

Mr. REIDENBERG. That is a very good question. It is nontransparent. One of the difficulties is what the vendors do, how they are using this information, it is not transparent. It is not stated often in the contracts. If you look at the contracts that school districts have with their vendors—and we have done that. We have analyzed those contracts—it is very difficult to figure out exactly what they are doing.

Mr. GROTHMAN. And so these people, in addition to the garden variety government employees—well, Ms. Sevier, do you want to—

Ms. SEVIER. Thank you. The situation that you bring up is interesting to me. Because with this relationship that Google has with the district—and this goes even to some online apps that are used in a classroom—parents and students do have an expectation of privacy, but they don't always realize when they are opting out of it.

And so part of engagement and information-sharing would be to educate teachers, administrators, parents and students, when they are opting out of privacy; for them to understand that by participating in something—by using Google or one of those platforms, that they are giving their information up—

Mr. GROTHMAN. I am gonna—

Chairman ROKITA. Five minutes is—

Mr. GROTHMAN. Okay. Well, we will—I have got a broader question.

Ms. ABSHIRE. Just very quickly. Back to our earlier comments. This information, this concept of transparency and trust; that within our communities, it is school districts' responsibilities and states' responsibilities to inform and educate parents so they can make informed decisions. We cannot do this in isolation. I don't think we can do it with legislation, with policy, or with practice. It has got to be a partnership between companies, school districts, parents, and students so that they are informed when they make these decisions and we can use that power of technology.

I fear a world where we can not use the technology to transform learning. But I also fear a world where our students' privacy is jeopardized. But I think we can balance that. And I hope that we will. Because I think that the potential is transformative.

Mr. GROTHMAN. Well, I am 59 years old. I grew up without all this stuff, and I don't feel like I missed anything. But be that as it may, maybe I did. Maybe I would be so much better off if they had a big data bank to peruse.

Mr. Reidenberg, one quick question. By the time I am—let's say I go graduate school, so we got all this stuff. Or like I did, I went to law school. And this stuff was in place from the time I was 3 years old in day care to 25 years old in law school. What all—could you give us like a 1-minute summary of all the stuff that would be

in one place that somebody could fine out about me? You know, that we all have to have, the program has to be of?

Mr. REIDENBERG. Well, probably the easiest way to do that in a minute is just think George Orwell and take it to the Nth degree, and that is probably what would be available. I mean, we are in an environment of ubiquitous surveillance, essentially. So the data from all sorts of devices can be captured and synthesized in enormous number of places.

And as we see emerging between what children do in the classroom, what they do at home outside the classroom, I think we are gonna see a lot of pressure to have data from each of these places; what is done in the privacy of the home with what is done in school being merged together. And it will just be an extraordinarily-rich data set of your life.

Chairman ROKITA. Gentleman's time is expired. Thank the gentleman.

And I am also pleased to see that we have members from off the subcommittee interested in this issue. I would like to recognize the gentleman from Colorado for 5 minutes.

Mr. POLIS. Thank you, Mr. Chairman. And I appreciate the opportunity to join the subcommittee today.

I think it was very valuable the way that Ms. Bonamici has sort of framed this issue and why this has strong democratic and republican agreement about, you know, parental rights and privacy issues. It is really—as we know, schools function with a certain degree of ability to in loco parentis operate in lieu of the parents.

And the question is when it comes to kids' personal information, do the schools and the government own it and can they sell it? And the answer should be without the parent's consent, no, they don't have that ability.

But because of the advent of interactive technology, there are oftentimes students interacting directly with third-party vendors and there is not the teacher or administrator there.

And therefore, policies and laws are needed to ensure that schools, in fact, are not selling personal information, whether there is monetary compensation or in kind, software composition, effectively selling information that isn't really theirs because the parents of the minor did not give them the permission to do that.

I want to go to Ms. Knox. And recognizing that we can learn from state efforts, notably SOPIPA in California that protects student privacy. And this is fundamentally a demand driven by parents across the country. Certainly, in my own state of Colorado.

Could you elaborate on how some of those innovative policies can be taken to the federal level, building upon the pledge which 100 companies, including yours, have already signed?

Ms. KNOX. Sure. Sure. And I would be remiss not to also thank Representative Messer for your leadership on the Student Privacy Pledge. So thank you for that. I know you joined a little after Mr. Polis or Representative Polis.

The state bill. So the California bill was very constructive. We found it constructive for the larger conversation. I think the data that came out of 2014 where there were 106 student privacy bills introduced, I think 28 of them had to do specifically with protecting student privacy. And I think it came from, like, there were 32 dif-

ferent states. The numbers are even, you know, at that level and getting higher as we speak.

What is interesting is that there is such a different kind of mix of the state bills. So some of them are looking at governance. You know, how—we should have a security officer or a CIO or a student privacy leader at the state level, you know, setting up governance systems, versus sort of this idea of how companies should behave in relation to student privacy, and especially third-party vendors.

So I think the Student Privacy Pledge has really helped specify and clarify and bring the industry together to commit to the eight specific objectives of the pledge. And we have been able to say okay, we would like to take these commitments and make sure that the other state bills that are moving right now, we want to make sure that they kind of work in conjunction with each other.

Mr. POLIS. And I want to go to Professor Reidenberg.

I think one of the dangers, absent the types of controls that parents want to see so that their own kid's information isn't sold without their permission, the danger seems to be that parents understandably—and this has occurred in districts in my state—rebelled the other way, where they effectively throw vendors out of schools that could otherwise be helpful at providing an individualized education, if only the legitimate concerns were addressed.

So I am wondering if you can address how we can harvest the great potential and power of educational technology and individualized education to boost student learning, while at the same time ensure that the concerns of parents are met.

Mr. REIDENBERG. I think that is exactly the challenge. Because the concerns parents have arise from the lack of trust, I think in part from a lack of transparency as to the sharing arrangements that are taking place and what the companies are doing. In the absence of effective privacy protection for their children's information, parents will oppose the technology. We have seen this. We saw this, for example, with the collapse of the InBloom platform. There were lots of things that coalesced in enbloom to cause its collapse. But one of the major reasons was the way InBloom dealt with privacy or didn't deal with privacy.

The other thing that I think is important to recognize, parental consent, we have to be very careful when we talk about engagement and giving parents the authority to consent and then everything is fine. The reason I say we have to be very careful is we have to be sure we are not dealing with forced consent. You can't put a parent in the position that they have to waive their child's privacy for their child to be able to engage in school.

As a parent, we experienced this several years ago. We had to sign up for the parent portal for our local school. And in signing up for the portal, you have to click I accept. And essentially, we had to accept waiving our child's privacy rights for my child to be able to get his homework assignments. So we have to be very careful about. That it is important to have parents engaged. Parents have to have rights to consent. But we can't be putting parents in the position where their choice is their kids gets an education or they have privacy, they can't have both.

Chairman ROKITA. Gentleman's time is expired. I thank the gentleman.

Also pleased to recognize Mr. Messer, from Indiana, another welcome member of the full committee, for 5 minutes.

Mr. MESSER. I thank the Chairman and the Ranking Member for their leadership on this important issue. Certainly thank the panelists as well for being here today an issue that I think a lot of parents are concerned about and yet don't they don't know a lot about either; that we are trying to wade our way through the issue.

You know, several testimonies have mentioned that the Student Privacy Pledge—thank you, Ms. Knox—and actually, Ms. Sevier and the PTA and the parent organizations that were part of our efforts to pull that together—obviously, we don't have a law today. So to have at least 100 industry leaders step forward and make clear that we ought to do some simple things, like not sell student information, not behaviorally target advertising, use data for authorized educational purposes only, and all the rest of the pats of the pledge.

You remember from our meetings together before, I have believed all along that the pledge alone wouldn't be enough, and that we ought to look at other ways that we can legally protect parents' rights to protect their child's privacy.

Yesterday in the ESEA bill we had an amendment that dealt with that. I think amending FERPA is part of that, as well. And looking at what other additional protections that we are seeing at the states could we could supply up here, like Mr. Polis and I are working on. Maybe a federal version. Not exactly the same, but a bill that would mirror the HPPA law that you know of in California.

I wanted to maybe start with Ms. Abshire and expound on the testimony at the end of the last questions. You know, it is important here that we protect student privacy. But it is also important that we make—ensure that any new laws intended to create student privacy don't create—that are intended to create a student privacy floor do not also create a digital learning ceiling.

And could you expound on that a little bit, reference—how do we find that spot in policy where we are protecting students and their privacy concerns, but still getting the remarkable educational benefits that come from having this kind of aggregated data?

Ms. ABSHIRE. Well, I think it is a partnership conversation. I think that there is deep experience in the field with my colleagues and school superintendents and school board members that are grappling with this every day at the district level, with organizations such as CoSN and ISTI that represent the types of leaders that also toil with these ideas.

In our work, we are not absent that thinking every day that contracts that we sign, systems we put in place, don't hold great responsibility for those of us that are in the educational system. So it is a constant thought on our mind. And the news and the media and the new tools that are emerging constantly bring that to the forefront of our thinking. Because we know what we have to do to make sure that our children are safe in a world that in many ways is unexpected from day-to-day as to what will happen.

But I think at the heart of this is the conversation—deep, abiding conversations that we as school leaders and policymakers have with the people that we entrust this information to, which are our

providers. I do commend Microsoft and other people for coming to the forefront and putting it together. And certainly, people that have worked at the state and the national level on this. But it is not gonna be an easy conversation.

Mr. MESSER. Sure.

Ms. ABSHIRE. And that is why I am so thrilled that this is happening today. Because we have got to probe at this and look at what the technology is doing in terms of securing privacy but enabling learning. So I think it is an ongoing conversation. I don't think we have the answers in our hands today. But I think they are emerging. And I think this panel today helped give you some insight.

And I know the conversations will continue. And we appreciate you talking to practitioners and to companies and to parents to know that we are all thinking about the same thing. No one is ignoring this important issue in elevating learning.

Mr. MESSER. Yes. Thank you very much. You know, I would just say again thank the Chairman for today's hearing. Thank the witnesses for your remarkable testimony.

There are incredible benefits to student learning that come from this data. But as you heard from the testimony today, parents are worried about protecting their children first.

Ms. Sevier, you want to finish?

Ms. SEVIER. Thank you. I would. If you went to the street and you pulled ten parents and you asked them well, how do you feel about biometric data and should it be collected on your student? Depending on the article that they just read that morning, they might just say they are thinking of that grilled cheese sandwich and no, you can't scan my child's eyes so that they can move through the lunch line. But maybe you have got other parents that are thinking about their child that is in speech therapy, and that biometric data is being used to accelerate their learning. And so it is all about conversations and information, definitely.

Mr. MESSER. Great point. Thank you.

Chairman ROKITA. Gentleman's time is expired. I thank the gentleman.

And the ranking member is recognized for closing.

Ms. FUDGE. Thank you, Mr. Chair.

And again, I thank all of you for being here. Very insightful. Very educational. We have learned a great deal today, and certainly will take parts of the discussion to try to determine how we best can serve students, as well as to make sure that their educational experiences are what they can be in this age of technology. Thank you all. And thank you, Mr. Chairman.

Chairman ROKITA. I thank the gentlelady. As always happens with these kinds of hearings, we learn a lot. I especially. So I want to thank each one of you for your testimony today.

Something perhaps not exactly orthodox. I am going to—because this is so important, I want to just say a few things and then I want to yield each of you 30 seconds—and it will just be 30 seconds—to make my closing for me, to say what you think we need to take away from today, what is most important for us as we go back and we look at updating FERPA, overhauling it for the 21st Century so that it has the appropriate enforcement mechanism; so

that it has that right kind of balance, so that third parties can be brought into this in a meaningful way so that, again, we can do what we all said we wanted to do and was first on our mind, and that is protect our kids, that they can have a lifelong successful learning.

So with that, Ms. Sevier, for 30 seconds, what should we take away from today?

Ms. SEVIER. The takeaway for today is to consider parents as partners in education, and not bystanders; to always support outreach and information; to consider not just who has the data and how it is being stored, but how it is being used in schools. Grilled cheese, speech therapy. And whether or not parents have a right to review that information. Because I can give content. But if it is a one-time thing, I am still a bystander.

Chairman ROKITA. Thank you.

Ms. Knox?

Ms. KNOX. It is very possible to strike a great balance between harnessing the power of personalized learning, while also safeguarding our students' data. Ask more from companies. There is no question that they need to be transparent, articulate clear contracts; that they need to make sure that they have comprehensive data security systems; and that they commit to not using data for noneducational advertising practices.

Chairman ROKITA. And FERPA, if I understand your testimony is a primary vehicle for doing that?

Ms. KNOX. We would like it to be part of it. Yes.

Chairman ROKITA. Okay. Thank you.

Dr. Abshire.

Ms. ABSHIRE. Yes, sir. Please be careful in your consideration of what changes in this law and how they will filter down and affect the business of school districts educating students. While we are painfully aware of the issues around student privacy and PII, I am also painfully aware that it is a very difficult and complicated process to manage student learning and to be wise stewards of all of this information. And so in terms of burden, we often talk about that, seek out professionals in the field, practitioners that will have to implement what you decide to do around this.

Chairman ROKITA. Thank you appreciate it.

Mr. Reidenberg.

Mr. REIDENBERG. Three quick things. Without modernizing FERPA, innovation is going to be opposed and will stall. It is just not going to work. I think Congress—message I would like to give is Congress needs to protect all student information, not just things that were considered educational records in 1974.

And lastly, the privacy protections have to apply to all of the participants in the educational environment, which means the schools, the vendors, the parents. The entire educational community set of actors have to be covered by these protections.

Chairman ROKITA. Thank you. There being no further business for the subcommittee, it stands adjourned.

[Additional submission by Mr. Dreiband follows:]

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON WORKFORCE PROTECTIONS
OF THE EDUCATION AND THE WORKFORCE COMMITTEE

Hearing on H.R. 4959, "EEOC Transparency and Accountability Act," H.R. 5422, "Litigation Oversight Act of 2014," and H.R. 5423, "Certainty in Enforcement Act of 2014"

Wednesday, September 17, 2014

10:00 a.m.

2175 Rayburn House Office Building

I. Introduction

Good morning Chairman Walberg, Ranking Member Courtney, and Members of the Subcommittee. Thank you all for the privilege of testifying today. My name is Eric Dreiband, and I am a partner at the law firm Jones Day here in Washington, D.C.

I previously served as the General Counsel of the United States Equal Employment Opportunity Commission ("EEOC" or "Commission"). As EEOC General Counsel, I directed the federal government's litigation under the federal employment antidiscrimination laws. I also managed approximately 300 attorneys and a national litigation docket of approximately 500 cases. I was privileged to work with many public officials who dedicated their careers to serving the public, enforcing the civil rights laws, rooting out unlawful discrimination, and working to ensure that our nation reaches the ideal of equal opportunity for everyone. These individuals continue their important work. They investigate charges of discrimination. They mediate and conciliate disputes and work with individuals, unions, and employers to resolve very difficult and often painful problems. They pursue enforcement through litigation in the federal courts, at every level up to and including the Supreme Court of the United States. And, these very able EEOC officials have the awesome power of the United States government to back them up.

Any law enforcement agency can make mistakes, no matter how well intentioned its officials. And, any law enforcement agency can, at times, become so convinced of the righteousness of its work and its motives that it can become prone to excess in certain circumstances. This includes the EEOC, which is a federal law enforcement agency that is charged with enforcing very important federal laws against discrimination on the basis of race, color, sex, religion, national origin, age, disability, and genetic information, among others.

It is with this background that I appear here today, at your invitation, to speak about three bills that are pending before this Subcommittee: H.R. 4959, the "EEOC Transparency and Accountability Act"; H.R. 5422, the "Litigation Oversight Act of 2014"; and H.R. 5423, the "Certainty in Enforcement Act of 2014."

Before I address the specific provisions of these bills, a little background on the structure and powers of the EEOC will be helpful.

II. The EEOC's Structure And Authority

Congress created the Commission when it enacted the Civil Rights Act of 1964.[1] The Commission is "composed" of five members who are appointed by the President with the advice and consent of the Senate.[2] No more than three of these members can be members of the same political party, and they serve staggered five year terms.[3] The President "shall designate" one member to serve as Chair and one member to serve as Vice-Chair of the Commission.[4] The statute vests the administrative operations of the agency in the Chair, and she has authority to appoint attorneys, administrative law judges, and other employees.[5] The Commissioners other than the Chair have authority to vote on policy matters presented to them by the Chair; litigation recommendations presented by the General Counsel; petitions to revoke or modify subpoenas; and a few other matters. The Commissioners other than the Chair do not have operational authority over the EEOC's investigators, litigators, or anyone other than their immediate staffs.

When Congress enacted Title VII of the Civil Rights Act, the statute did not authorize the EEOC to sue anyone. The EEOC could receive charges, provide notice of the charges to those named in the charge, investigate charges, and attempt to reach a settlement. The Attorney General's litigation authority was limited to intervening in cases that involved matters of public importance and to bringing pattern or practice lawsuits, which are akin to class action lawsuits that the government can bring to remedy widespread, egregious unlawful discrimination.[6]

In 1972, Congress amended Title VII in multiple ways and, among other things, authorized the EEOC to file lawsuits in federal court. Congress retained Title VII's multi-step administrative enforcement scheme and determined that the EEOC must satisfy several administrative prerequisites before it can file a lawsuit. Congress tied the EEOC's litigation authority to charges of discrimination, and it required the EEOC to notify the respondent of the charge within 10 days and to investigate charges.[7] Congress also required that "[i]f the Commission determines after such investigation that there is reasonable cause to believe that the charge is true, the Commission shall endeavor to eliminate any such alleged unlawful employment practice by informal methods of conference, conciliation, and persuasion."[8] As a

---

[1] 42 U.S.C. § 2000e-4(a).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Civil Rights Act of 1964, Title VII, §§ 705-07, 78 Stat. 241, 258-62 (1964).

[7] 42 U.S.C. § 2000e-5(b).

[8] *Id.*

result, the EEOC must "refrain from commencing a civil action until it has discharged its administrative duties."[9]

In 1972, Congress also transferred to the EEOC the Attorney General's authority to bring pattern or practice cases and to intervene in pending litigation against private sector employers and unions.[10] Congress assigned the Attorney General with the responsibility to bring litigation against state governments and agencies, and subdivisions of state governments.[11]

The 1972 amendments to Title VII also created the position of General Counsel of the EEOC. The General Counsel would be "appointed by the President, by and with the advice and consent of the Senate, for a term of four years."[12] Congress assigned "responsibility for the conduct of litigation" to the General Counsel and authorized the Commission to "prescribe" other duties for the General Counsel.[13] Congress also directed the General Counsel to "concur with the Chairman of the Commission on the appointment and supervision of regional attorneys."[14]

Notwithstanding the General Counsel's responsibility for the conduct of litigation, the Congress vested the Commission with the authority to direct the agency's attorneys to "appear for and represent the Commission in any case in court."[15] The EEOC has generally interpreted this to mean that the Commission retains the ultimate authority to authorize the Commission to litigate cases.

In 1996, the Commission adopted its "National Enforcement Plan" ("NEP"). The goal was to "free[] the Commission to focus on policy issues."[16] To accomplish this goal, the NEP delegated nearly all of the Commission's litigation authority to its General Counsel.[17]

Specifically, the NEP "delegat[ed] to the General Counsel the decision to commence or intervene in litigation in all cases except the following":

---

[9] *Occidental Life Ins. Co. v. EEOC*, 432 U.S. 355, 368 (1977).

[10] 42 U.S.C. § 2000e-6(c)-(e).

[11] *See* 42 U.S.C. § 2000e-6(c).

[12] 42 U.S.C. § 2000e-4(b).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] U.S. Equal Employment Opportunity Commission, *National Enforcement Plan* (1996), *available at* http://www.eeoc.gov/eeoc/plan/nep.cfm (last visited Sept. 11, 2014).

[17] *Id.*

A. Cases involving a major expenditure of resources, *e.g.* cases involving extensive discovery or numerous expert witnesses and many pattern-or-practice or Commissioner's charge cases;

B. Cases which present issues in a developing area of law where the Commission has not adopted a position through regulation, policy guidance, Commission decision, or compliance manuals;

C. Cases which, because of their likelihood for public controversy or otherwise, the General Counsel reasonably believes to be appropriate for submission for Commission consideration; and

D. All recommendations in favor of Commission participation as amicus curiae which shall continue to be submitted to the Commission for review and approval.[18]

These standards are quite vague and therefore give the General Counsel a great deal of discretion in determining whether to send litigation recommendations to the full Commission for an up-or-down vote. More recently, it appears that the number of matters presented to the Commission by the General Counsel has diminished significantly. One current EEOC Commissioner has explained:

> Most people I talk to assume that when the Commission files a lawsuit, that lawsuit has first been reviewed, studied, deliberated, discussed and voted on by the Commissioners. People are shocked when I tell them that, in fact, most lawsuits are filed without the Commissioners' knowledge. For example, last year – [Fiscal Year 2012], 122 lawsuits were filed in the name of the Commission, but under the rules of the Delegation to the General Counsel, only 3 of the 122 lawsuits were sent up to the Commissioners for their review and vote. All the rest were filed without a vote by the Commission.[19]

These numbers give the impression of a Commission made up of potted plants and disinterested bystanders.

In December 2012, the Commission adopted its "Strategic Enforcement Plan." That Plan largely reaffirmed the NEP's delegation of authority to the General Counsel. It also required that each District Office – of which there are fifteen – "present[]" a "minimum of one litigation recommendation" for "Commission consideration each fiscal year."[20] The Strategic Enforcement Plan does not articulate any criteria for this "minimum."

---

[18] *Id.*

[19] Commissioner Constance S. Barker, Comments for the Record, Public Commission Meeting on the Implementation of the EEOC's Strategic Plan for Fiscal Years 2012-2016 (February 20, 2013).

[20] U.S. Equal Employment Opportunity Commission, *Strategic Enforcement Plan* (2012), *available at* http://www.eeoc.gov/eeoc/plan/sep.cfm (last visited September 11, 2014).

This approach does not appear to have worked. To be sure, the Commission's litigation program has had some impressive victories in the last few years, thanks in large part to the very fine work of some highly talented and dedicated lawyers. For example, in 2013, a jury in Iowa returned a multi-million dollar verdict in the Commission's favor after it found that the defendant subjected a group of 32 men with intellectual disabilities to severe abuse and discrimination for a multi-year period. My friend and former colleague, EEOC Regional Attorney Robert Canino successfully tried that case, and I commend him and his colleagues for a very important victory.[21]

Regrettably, however, the Commission has suffered several embarrassing losses.

For example, a federal judge in Iowa dismissed the EEOC's claims for 67 alleged victims of sexual harassment after the judge determined that the EEOC did not comply with its presuit investigation, reasonable cause, and conciliation obligations. The U.S. Court of Appeals for the Eighth Circuit substantially affirmed the district court's decision, and then, in August 2013, the district court sanctioned the EEOC approximately $4.7 million dollars.[22] Unless an appellate court overturns that decision, the American people will have to pay this sanction.

In another case, the Commission brought a very high profile race discrimination class action that alleged that the defendant unlawfully denied employment opportunities to applicants who had poor credit histories. The case was so flimsy that the district court judge dismissed it after she found that the EEOC could not offer admissible evidence that proved any violation. On April 9, 2014, the U.S. Court of Appeals for the Sixth Circuit affirmed the district court's decision and chastised the EEOC because it sued defendants for "using the same type of background check that the EEOC itself uses" and because the EEOC brought the case "on the basis of a homemade methodology, crafted by a witness with no particular expertise to craft it, administered by persons with no particular expertise to administer it, tested by no one, and accepted only by the witness himself."[23]

In another high profile class action, the Sixth Circuit affirmed a district court's decision to dismiss an EEOC class action and to sanction the EEOC approximately $750,000. The court found that the EEOC incorrectly claimed that an employer had a policy that excluded anyone with a criminal record and then continued to litigate the case, even though it knew that the employer did not, in fact, maintain the discriminatory policy that the EEOC alleged in its complaint.[24]

---

[21] *See* EEOC Press Release, "Jury Awards $240 Million for Long-Term Abuse of Workers with Intellectual Disabilities" (May 1, 2013), *available at http://www.eeoc.gov/eeoc/newsroom/release/5-1-13b.cfm*

[22] *EEOC v. CRST Van Expedited*, No. 07-00095, 2013 U.S. Dist. LEXIS 107822 (N.D. Iowa Aug. 1, 2013).

[23] *EEOC v. Kaplan*, 748 F.3d 749, 750, 754 (6th Cir. 2014).

[24] *EEOC v. Peoplemark*, 732 F.3d 584 (6th Cir. 2013).

These cases are not isolated examples:

- The Commission brought a class action lawsuit against an employer that it alleged unlawfully excluded applicants who had a criminal record. The district judge threw the case out after he determined that the EEOC had no admissible evidence of any violation.[25]

- The U.S. Court of Appeals for the Fifth Circuit affirmed the dismissal of a class action age discrimination suit that challenged an employer's decision to maintain an age 60 retirement policy for pilots.[26]

- A district court in Alabama dismissed the EEOC's challenge to an employer's policy about hairstyles after it determined that no Title VII precedent supported the Commission's claim and that the employer's policy was lawful.[27]

- The U.S. Court of Appeals for the Fourth Circuit affirmed an award of nearly $200,000 in sanctions against the EEOC after it found that the EEOC filed suit against an employer even though its years-long delay in investigating the allegations, and the employer's decision to close the facility where the alleged discrimination occurred, meant that no monetary or injunctive relief would have been possible.[28]

- A district court in North Carolina sanctioned the EEOC after it found that the EEOC failed to preserve evidence.[29]

- Federal courts in New York, Arizona, Colorado, Hawaii, California, and Texas, among others, dismissed all or significant portions of EEOC's class action lawsuits because the Commission did not comply with Title VII's multi-step administrative enforcement scheme before it filed suit.[30]

---

[25] *EEOC v. Freeman*, 961 F. Supp. 2d 783 (D. Md. Aug. 9, 2013), *appeal pending*, No. 13-02365 (4th Cir. Nov. 7, 2013).

[26] *EEOC v. Exxon Mobil Corp.*, 560 Fed. Appx. 282 (5th Cir. 2014).

[27] *EEOC v. Catastrophe Mgmt. Solns.*, No. 13-00475, 2014 U.S. Dist. LEXIS 50822 (S.D. Ala. Mar. 27, 2014).

[28] *EEOC v. Propak Logistics, Inc.*, 746 F.3d 145 (4th Cir. 2014).

[29] *EEOC v. Womble Carlyle Sandridge & Rice, LLP*, No. 13-00046, 2014 U.S. Dist. LEXIS 38219 (M.D.N.C. Mar. 24, 2014), *report and recommendation adopted by* 2014 U.S. Dist. LEXIS 58938 (Apr. 29, 2014).

[30] *EEOC v. Sterling Jewelers, Inc.*, No. 08-00706, 2014 U.S. Dist. LEXIS 304 (W.D.N.Y. Jan. 2, 2014), *report & recommendation adopted by* 2014 U.S. Dist. LEXIS 31524 (W.D.N.Y. Mar. 10, 2014), *appeal pending* No. 14-1782 (2d Cir. May 15, 2014); *Arizona v. GEO Grp., Inc.*, No. CV 10-1995-PHX-SRB, 2012 U.S. Dist. LEXIS 102950 (D. Ariz. Apr. 17, 2012), *appeal pending*, No. 13-16292 (9th Cir. Jun. 24, 2013); *EEOC v. Swissport Fueling, Inc.*, 916 F. Supp. 2d 1005 (D. Ariz. 2013); *EEOC v. The Original Honeybaked Ham Co. of Georgia, Inc.*, 918 F. Supp. 2d 1171 (D. Colo. 2013); *EEOC v. Am. Samoa Gov't*, No. 11-00525, 2012 U.S. Dist. LEXIS 144324 (D. Haw. Oct. 5, 2012); *EEOC v. Dillard's Inc.*, No. 08-CV-1780, 2011 U.S. Dist. LEXIS 76206 (S.D. Cal. July 14, 2011); *EEOC v. Bass Pro Outdoor World, LLC*, 884 F. Supp. 2d 499 (S.D. Tex. 2012).

The available data does not present a better picture. The EEOC publicizes annual cumulative information about its litigation program that dates back to 1997. According to the EEOC, the Commission recovered $44.2 million dollars during the fiscal year that ended in September 2012 and $38.6 million during the fiscal year that ended in September 2013. These are the lowest amounts reported for any fiscal year that is available. By contrast, when I served at the EEOC, the Commission's litigation program recovered an average of about $140 million each year for victims of unlawful discrimination.[31]

The EEOC sometimes brings hundreds of cases each year. The agency cannot be judged only on those cases in which it was unsuccessful. Nor should anyone suggest that the EEOC's career staff lack a commitment to the agency's core mission of stopping and remedying unlawful employment discrimination. Nonetheless, it takes only a handful of cases in which a court finds that the EEOC used "homemade methodology"[32] or submitted statistics with a "mind-boggling number of errors"[33] before the EEOC begins to lose credibility with the courts and, ultimately, with the public.

Two of the bills you are considering today would provide safeguards to ensure that the EEOC does not diminish its credibility as the nation's foremost protector of civil rights in employment. Under current law, the EEOC's General Counsel and Regional Attorneys have almost unchecked discretion to initiate or intervene in lawsuits on behalf of the Commission. H.R. 4959 and H.R. 5422 would limit this discretion and provide for greater reporting of the EEOC's litigation results, in order to hold the agency publicly accountable.

In addition, H.R. 4959 addresses the EEOC's statutory obligation to facilitate dispute resolution prior to litigation. That Bill provides that the EEOC's conciliation efforts before it files a lawsuit must be "bona fide" and "in good faith." Moreover, under H.R. 4959, the EEOC's conciliation efforts would indisputably be reviewable by a court.

III. H.R. 5422 May Restore The Commission's Oversight Of Enforcement

H.R. 5422 would ensure that the EEOC cannot bring major or controversial litigation without a full up-or-down vote by a majority of the Commission. First, it would require the Commission to approve or disapprove by majority vote any cases involving multiple plaintiffs, allegations of systemic discrimination, or pattern or practice claims.[34] Second, it would give each EEOC Commissioner the power to require a majority vote on the commencement of any litigation.[35] Implementation of these measures would mean that the EEOC's decision to file

---

[31] EEOC Litigation Statistics, FY 1997 through FY 2013, *available at* http://www.eeoc.gov/eeoc/statistics/enforcement/litigation.cfm.

[32] *Kaplan*, 748 F.3d at 754.

[33] *Freeman*, 961 F. Supp. 2d at 796.

[34] H.R. 5422, § 2.

[35] *Id.*

lawsuits would be determined after consideration and deliberation by the five bipartisan members of the EEOC.

H.R. 5422 would neither impede the EEOC's efficient prosecution of civil rights litigation nor interfere with the Commission's ability to focus on policy. As an initial matter, the bill would make Commission approval mandatory only for cases with multiple potential victims. The bill would not require that Commissioners vote on dozens of small-dollar or uncontroversial cases before the Commission files suit.

The bill would, however, increase significantly the number of cases presented to the Commission for a vote. This is not unreasonable. After all, the American taxpayers pay Commissioners and their staff millions of dollars every year, and it is not too much to require that they actually consider whether additional taxpayer resources should be spent litigating EEOC lawsuits. Nor is there any reason to suspect that increased deliberation by the Commission would hinder enforcement. When I served as the EEOC's general counsel, I regularly sent litigation recommendations to the Commissioners for a vote. Nonetheless, the Commission obtained relief for thousands of discrimination victims during my tenure, and the EEOC's litigation program recovered more money for discrimination victims than at any other time in the Commission's history.

IV. H.R. 5422 And H.R. 4959 May Enhance The EEOC's Accountability For Litigation Decisions

H.R. 5422 and H.R. 4959 would both require the EEOC to post data publicly, in an effort to increase public accountability for the agency's litigation decisions. The EEOC already posts some litigation data, and these bills would increase the reporting requirements. Specifically, H.R. 5422 would require the Commission to post information about every lawsuit that it brings pursuant to a vote of the Commissioners, including each Commissioner's vote on the litigation.[36]

H.R. 4959 has a much more extensive series of reporting requirements specifically related to cases in which the EEOC is sanctioned or ordered to pay fees and costs. The Bill would require the EEOC to track and publicly post data on these cases in conjunction with information regarding whether the litigation was submitted to the Commission for an up-or-down vote.[37] These figures would ultimately allow the Commission and Congress to determine statistically whether the Commission's delegation of authority to the General Counsel is undermining the agency's integrity.

H.R. 4959 also contains reporting requirements to Congress. Specifically, in any case where a court orders the EEOC to pay fees and costs or imposes sanctions, the agency's Inspector General would be required to notify the House Committee on Education and the Workforce, as well as the Senate Committee on Health, Education, Labor, and Pensions, and

---

[36] *Id.*

[37] H.R. 4959, § 2(a)(1).

conduct an extensive investigation to determine why such an order was imposed.[38] This investigation would entail interviews with the EEOC staff involved on the case, estimates of the resources used in prosecuting the case, an explanation of whether the case was brought to a full vote by the Commission, and other relevant information.[39] The Bill also would require the Commission to submit a report to Congress about the steps it is taking to reduce instances in which it is ordered to pay fees or is sanctioned.[40]

Increased record-keeping and reporting requirements always run the risk that they may serve no purpose other than to compound bureaucracy. Nonetheless, this legislation would require the EEOC to take a break after a negative outcome in litigation, to step back, and to evaluate why a court sanctioned the Commission. It would also enable the Congress and the public to understand better what happened and why.

V. H.R. 4959 May Hold The EEOC Responsible For Meeting Its Conciliation Obligations

H.R. 4959 would prevent the EEOC from rushing to litigation in another way: it specifically provides for court review of the sufficiency of the agency's conciliation efforts. In addition, it makes clear that the EEOC cannot file a lawsuit without first clearly identifying its claims, and any putative victims thereof, to a putative defendant.

The provisions of H.R. 4959 merely clarify obligations that are already written into Title VII. Title VII outlines a multi-step process that the EEOC must satisfy before it can file a lawsuit. This process requires the EEOC to provide prompt notice of the charge to the employer, investigate the charge, and make a reasonable cause determination if it finds that a violation occurred. Thereafter, the EEOC must "endeavor to eliminate any such alleged unlawful employment practice by informal methods of conference, conciliation, and persuasion."[41] The EEOC may file a lawsuit only after it "has been unable to secure from the [employer] a conciliation agreement acceptable to the Commission."[42]

From 1972 to December 2013, the federal courts policed the EEOC's compliance with its presuit obligations, including the obligation that the Commission conduct meaningful conciliation proceedings as part of an effort to settle any dispute and that the EEOC file suit only if conciliation proves impossible. In December 2013, the U.S. Court of Appeals for the Seventh Circuit became the first court "to reject explicitly the implied affirmative defense of failure to

---

[38] *Id.* at § 4(a).

[39] *Id.*

[40] *Id.* at § 4(b).

[41] *See* 42 U.S.C. § 2000e-5(b).

[42] 42 U.S.C. § 2000e-5(f)(1).

conciliate."[43] The case, *EEOC v. Mach Mining*, is pending before the Supreme Court of the United States, and that Court may settle the issue once and for all. A decision is expected by June 2015.[44]

H.R. 4959 would settle the issue by statute.[45] The Bill would require the EEOC to use "good faith efforts" to engage in "bona fide" conciliation.[46] Section 3(3) of the Bill would require the Commission, at a minimum, to give accused employers:

> all information regarding the legal and factual bases for the Commission's determination that reasonable causes exist as well as all information that supports the Commission's requested monetary and other relief (including a detailed description of the specific individuals or employees comprising the class of persons for whom the Commission is seeking relief and any additional information requested that is reasonably related to the underlying cause determination or necessary to conciliate in good faith).[47]

Finally, H.R. 4959 expressly provides that an employer may use documents related to the conciliation process in proceedings to test the validity of the EEOC's conciliation efforts.[48]

Undoubtedly, H.R. 4959 would provide important protections for employers, by requiring the EEOC to give them all of the information necessary to evaluate properly the agency's settlement demands. In addition, the legislation would pre-empt the "sue first, ask questions later" mentality that has led to highly-publicized EEOC defeats.[49] By requiring the EEOC to provide all factual and legal bases for its reasonable cause determination and to identify with specificity each employee who was allegedly wronged, H.R. 4959 will ensure that the EEOC returns its focus to conciliation first, and then litigation, as required by the statute.

VI. H.R. 5423 – The Certainty In Enforcement Act Of 2014

I would also like to say a few words about the third piece of legislation this Subcommittee is now considering: the Certainty in Enforcement Act, or H.R. 5423. This Bill responds to new enforcement guidance that the EEOC issued in 2012 about the use of arrest and

---

[43] 738 F.3d 171, 182 (7th Cir. 2013). *See also* Press Release, U.S. EEOC, *In Landmark Ruling, Seventh Circuit Holds Employers Cannot Challenge EEOC Conciliation* (Dec. 20, 2013), *available at* http://www.eeoc.gov/eeoc/newsroom/release/12-20-13b.cfm (last visited May 20, 2014).

[44] The docket number for this case is 13-1019.

[45] H.R. 4959, § 3.

[46] *Id.* at § 3(1).

[47] *Id.* at § 3(3).

[48] *Id.* at § 3(2).

[49] *See EEOC v. CRST Van Expedited*, No. 07-00095, 2009 U.S. Dist. LEXIS 71396, at *64 (N.D. Iowa Aug. 13, 2009).

conviction records to make employment decisions. Under the EEOC's guidance, the EEOC presumes that employer use of criminal history information creates a disparate impact that violates Title VII. According to the EEOC, national data shows that African Americans and Hispanics are arrested and incarcerated "at rates disproportionate to their numbers in the general population."[50] Therefore, the EEOC asserts, "criminal record exclusions have a disparate impact based on race and national origin."[51]

The EEOC would impose on the employer the burden of rebutting this presumption during an investigation and would give the employer "an opportunity to show, with relevant evidence, that its employment policy or practice does not cause a disparate impact on the protected group(s)."[52] This so-called "opportunity" is inconsistent with the burdens of proof enacted by Congress, and it saddles employers with the burden of *disproving* discrimination. The message is clear: if an employer excludes anyone because of a person's criminal history – including convictions – the EEOC will assume that the employer has violated Title VII unless and until the employer proves otherwise.

The EEOC's enforcement guidance was not enacted by notice-and-comment rulemaking, and it is unclear whether the federal courts will endorse it. Nonetheless, many are concerned that the guidance adopts an interpretation of Title VII that would have that statute preempt State and local laws that prohibit the hiring of convicted felons for safety-sensitive positions, such as child care. The Commission's guidance says that "an employer may make an employment decision based on the conduct underlying the arrest if the conduct makes the individual unfit for the position in question."[53] But what the EEOC believes makes an individual "unfit for the position in question" is not clear. The Commission's guidance gives only a few examples of what it believes this standard permits, and the Commission's litigation program raises the specter of class action litigation any time an employer excludes any criminals.

For example, in one pending case, the EEOC is suing an employer for violating the "equal employment opportunities" of applicants because the employer allegedly excludes from its workforce those convicted of "Murder, Assault & Battery, Rape, Child Abuse, Spousal Abuse (Domestic Violence), Manufacturing of Drugs, Distribution of Drugs, [and] Weapons Violations," as well as "theft, dishonesty, and moral turpitude."[54] Does a conviction for murder, rape, and theft make an individual "unfit"? According to the EEOC, an employer must show that its criminal conviction policy "operates to effectively link specific criminal conduct, and its dangers,

---

[50] *See* U.S. Equal Employment Opportunity Commission, *EEOC Enforcement Guidance: Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964* (Apr. 25, 2012), *available at* http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm (last visited July 23, 2013) [hereinafter "EEOC Criminal Record Enforcement Guidance"].

[51] *Id.*

[52] *Id. But see* 42 U.S.C. § 2000e-2(k).

[53] *See* EEOC Criminal Record Enforcement Guidance.

[54] Compl., *EEOC v. BMW Mfg. Co.*, No. 13-01583 ¶¶ 19-20 (D.S.C. June 11, 2013).

with the risks inherent in the duties of a particular position."[55] But there are no statistical studies showing that a convicted rapist is more likely to embezzle funds from an employer or that a convicted embezzler is more likely to endanger fellow employees. No company can realistically meet this evidentiary burden.

Worse still, the EEOC's policy makes it impracticable, if not impossible, to justify consideration of prior felonies as a legitimate employment concern, even though the federal government itself takes account of such prior convictions in its own personnel decisions. The EEOC's guidance also repudiates what the federal government's own employment practices make obvious: a person's history of compliance with the law is relevant to any job. Indeed, the Supreme Court recently upheld the federal government's inquiry into whether employees of federal contractors used drugs because "the Government is entitled to have its projects staffed by reliable, law-abiding persons" and "[q]uestions about illegal-drug use are a useful way of figuring out which persons have these characteristics."[56] The Court emphasized that questions about an applicant's "violations of the law," like other questions going to the applicant's "honesty or trustworthiness," are "reasonably aimed at identifying capable employees who will faithfully conduct the Government's business."[57]

As further proof that prior criminal activity is a legitimate, nondiscriminatory employment criterion, the federal government routinely performs criminal background checks on applicants for the federal workforce. Government regulations require a "suitability" review, which includes consideration of "[c]riminal or dishonest conduct," because this bears on "a person's character or conduct that may have an impact on the integrity or efficiency of the service."[58] Although the extent to which criminal convictions automatically disqualify former criminals from federal employment is unclear, the relevant point remains: even the federal government believes that prior criminal convictions are presumptively valid and nondiscriminatory factors that are directly tied to the job-related issue of a potential employee's "character or conduct."

If the government is entitled to have law-abiding workers, then surely private employers are as well. And it is all the more necessary for employers to exclude risky criminals from its workforce because employers may be ultimately liable, under principles of vicarious liability, for the work-related misconduct of their employees. That private employers might be more reluctant to expose their customers and employees to former criminals provides no basis for condemning such prudence as unlawful discrimination, at least when there is no intent to discriminate against anyone because of their race or other protected characteristic.

Adding to this problem is the fact that several federal, state, and local laws place restrictions on employers' decisions about whether to hire persons with criminal convictions.

---

[55] *See* EEOC Criminal Record Enforcement Guidance.

[56] *NASA v. Nelson*, 131 S. Ct. 746, 759-60 (2011).

[57] *Id.* at 761.

[58] 5 C.F.R. §§ 731.101, 731.202.

The EEOC's guidance says that "if an employer's exclusionary policy or practice is not job related and consistent with business necessity, the fact that it was adopted to comply with a state or local law or regulation does not shield the employer from Title VII liability."[59]

All of this presents employers with a Catch-22. They must either hire criminals and risk violating these other laws and exposing themselves to lawsuits for negligent hiring. Or, if they do not hire such criminals, they risk an EEOC investigation and class action lawsuit.

H.R. 5423 attempts to address these problems by making it clear that it "shall not be an unlawful employment practice for an employer . . . to engage in an employment practice that is required by Federal, State, or local law, in an area such as, but not limited to, health care, childcare, in-home services, policing, security, education, finance, employee benefits, and fiduciary duties."[60] This Bill may provide a useful fix that will prevent EEOC's informal guidance from trumping certain State and local laws.

If H.R. 5423 becomes law, the Equal Protection Clause of the Fourteenth Amendment, as well as the equal protection component of the Fifth Amendment, will limit the discretion of Federal, State, and local governments to pass laws that would require employers to engage in discriminatory conduct. Nonetheless, for the purpose of greater clarity, this Subcommittee might consider three amendments to the Bill as it is presently drafted.

First, the Subcommittee may consider revising H.R. 5423 to limit it to laws requiring employers to conduct criminal background checks or credit history checks. This seems to be the primary concern of the Bill and amending it this way would clarify the issue.

Second, the Subcommittee may also consider limiting the bill to allow employers to follow Federal, State or local laws that have a disparate impact on a protected class, so long as the laws are targeted to hiring practices in sensitive industries like healthcare and childcare.

---

[59] *See* EEOC Criminal Record Enforcement Guidance.

[60] H.R. 5423, § 3. Congress should be aware that two provisions of the Civil Rights Act already speak to pre-emption of State and local laws.

Section 708 of Title VII provides:

"Nothing in this title shall be deemed to exempt or relieve any person from any liability, duty, penalty, or punishment provided by any present or future law of any State or political subdivision of a State, other than any such law which purports to require or permit the doing of any act which would be an unlawful employment [282] practice under this title." 42 U.S.C. § 2000e-7.

In addition, Section 1104 of Title XI of the Civil Rights Act of 1964 applies to all titles of the Civil Rights Act, including Title VII and establishes the following standard for pre-emption:

"Nothing contained in any title of this Act shall be construed as indicating an intent on the part of Congress to occupy the field in which any such title operates to the exclusion of State laws on the same subject matter, nor shall any provision of this Act be construed as invalidating any provision of State law unless such provision is inconsistent with any of the purposes of this Act, or any provision thereof." 42 U.S.C. § 2000h-4.

See also California Federal Sav. & Loan Ass'n v. Guerra, 479 U.S. 272, 281-282 (1987), which discusses these statutes.

Third, H.R. 5423 appears to respond to the EEOC's expansive interpretation, in its enforcement guidance, of what may be a disparate impact violation of Title VII. Adding language that specifically addresses disparate impact may help clarify that H.R. 5423 is in no way intended to sanction intentional discrimination.

VII. Conclusion

Thank you again for the opportunity to testify here today. I look forward to your questions.

[Whereupon, at 12:54 p.m., the subcommittee was adjourned.]

○