ED.gov U.S. Department of Education

Search

Advanced Search

Funding Policy Research News About ED

ARCHIVED INFORMATION

Technology in Education: Privacy and Progress

Remarks of U.S. Secretary of Education Arne Duncan at the Common Sense Media Privacy Zone Conference

FEBRUARY 24, 2014

Contact: (202) 401-1576, press@ed.gov (mailto:press@ed.gov)

I want to thank Jim Steyer and Common Sense Media for bringing this event together and starting this important dialogue – and for your tireless efforts to keep the digital world that our kids inhabit safe and healthy.

America's families, including my own, owe a debt of gratitude to a lot of people here today. Anyone who has children, or works with them, knows that keeping children safe and secure is the most important thing in the world. Privacy is a part of our children's safety and security – especially in our fast-changing world.

Technology has brought the ability to do things that would've seemed like science fiction not long ago.

Our two kids get to hold conversations in full-color video with their grandparents in Australia on a quarter-inch-thick screen that they can hold in their hands – in my childhood that would've seemed like something that Q invented for James Bond.

But technological advances have also brought a host of new worries to parenting. My wife and I constantly feel the need to get smarter about those issues – and so many of the folks in this room are helping America's parents do just that.

I'm also glad to know you will be hearing shortly from Senator Ed Markey, whose work in this area has been so important. And I know that my partner Jim Shelton is going to have a great conversation with Commissioner Julie Brill of the FTC, who is fighting for consumer privacy.

That effort could not be more important now.

A generation ago, a phone was a thing with a wire plugged into the wall, a file went in a drawer, a tablet was something you took if you had a headache, a text was a book that students carried in heavy backpacks, and social media meant watching some TV with your friends.

The new normal embraces a stunning variety of tools and connectedness. In schools, like everywhere else, these new tools and connections have offered extraordinary learning opportunities.

Schools now have not just new ways of working, but vast amounts of new information that can empower teachers, students, and families.

But technological advances have brought with them new cautions. Online banking and email have improved our lives – but they have also given us more to defend. Our identity and privacy are treasures that we must protect in ways we wouldn't have conceived of not too long ago.

People – especially young people — are creating vastly more information than ever before — everything from pictures to news articles to restaurant recommendations and much more.

We can do our banking from a coffee shop or a ski slope! Yet we've never been more worried about inappropriate access to, or use of, our personal information.

This is something we think about a lot at home, with our 12-year old daughter and 10-year old son. Ours is not a low-tech home, although my kids, correctly, claim they have a pretty low-tech dad since they have to share my iPad, and because my wife and I limit their non-educational screen time. We've been learning to code together, though they are ahead of me.

Our kids can access their school assignments on the web, and turn them in, using document sharing. They track their own grades and progress. And we use some web-based tools to support their learning, including online video lessons and foreign language courses.

Of course, all that just scratches the surface of what's possible. We're far from the most advanced house in America.

In education, it would be easy to see the benefits, and the cautions, of this new world as a zero-sum game. I'm going to ask you not to look at it that way.

What I want to say to you today is that the benefits for students of technological advancement can't be a trade-off with the security and privacy of our children.

We must provide our schools, teachers and students cutting-edge learning tools. And we must protect our children's privacy. We can and must accomplish both goals – but we will have to get smarter to do it.

Let's start with why technology matters.

In schools, technology – when it's used wisely – can enable teachers to focus their time on the things they do best, like teaching critical thinking and helping kids who are struggling.

It can provide them up-to-the-minute information on where students are doing well and where they need more help. And it can help them reinvent the most traditional school experiences.

Take what's happening at the Brenda Scott School in Detroit. In one classroom I visited, a teacher named Kristie Ford was working directly with just a few students who immediately needed her help.

The rest were engaged in small-group projects, building 3-D models or working on laptops – a flexibility made possible by digital technology and independent learning plans.

In New York, some schools use a similar strategy to let kids work at their own pace on the material that's right for them – while teachers focus on those who are struggling. Each day, teachers receive a report on each student's progress, and recommendations for learning the next day.

At Nashville Prep, school leaders and teachers analyze data about student achievement, attendance, and discipline every week—as a team—to spot trends and sync up about each student's needs.

And in Huntsville, Alabama, teachers and school leaders can get real-time snapshots of student progress in math. That helps educators to help kids.

The direct benefits to students can be big, too. Just imagine the inspiration that two high school girls, in Kentucky and Virginia, felt when they used open government data to discover a super-fast spinning millisecond pulsar star.

Technology also can empower parents, giving them a stronger connection to what their kids are learning.

Look at Khan Academy, which lets parents look at their children's progress in the language the parent speaks — regardless of the language in which their children are working.

Look at the programs used in Newark and here in DC that generate notes for parents about their children's progress in reading or math—as well as advice about what parents can do to further their kids' learning at home each night.

Now, parents don't have to just ask "what did you do in school" (and, if they're teenagers, have them say, "Nothing"). Now they can start a dialogue about what their kids actually were learning that day!

Here's what these examples – and thousands and thousands more like them – are starting to add up to.

It's about helping teachers work smarter, and helping students learn more quickly and stay more engaged.

It's about helping school systems support teachers more effectively, and helping families stay informed about their kids' education. And it's about parents partnering more actively with children's teachers.

All of that can be transformational. But we must increase access and take on the digital divide with a greater sense of urgency. Some of our international competitors are well ahead of us in providing broadband to their schools – an unacceptable opportunity deficit in our system that President Obama has laid out a plan to fix.

But that's just the beginning. We're behind our international competitors in so many important ways.

Technology can help us catch up – it can help us increase both equity and excellence — if everyone works together to produce solutions that serve students well.

Smart policies will support – not impede – educators who want to put technology to work for kids.

We live in a new, fast-changing time. And in fact, many teachers aren't waiting.

Every day, teachers face the challenge of making education work for each individual child in their classroom, and finding ways to tailor learning to each child's gifts, skills and needs. We need to give teachers every possible tool to help them succeed – but frankly we haven't.

According to a PBS survey, 91 percent of teachers have access to computers—but only one fifth say they have access to the right level of technology.

So no one should be surprised when hard-working, committed teachers go out on their own to find the best tools they can for their classrooms. Whether it's an online grade book, or text message homework reminders, teachers are often finding their own solutions.

Schools and districts need to develop policies that allow rapid adoption of technologies that meet privacy and security standards – and rejection of those that do not.

The practices of districts and schools are changing rapidly as well. Like many organizations, school districts are striving to get smarter about using data to drive improvement.

School systems that have been especially thoughtful in their use of data – like those in Tennessee and Washington, DC – have reaped real learning benefits for kids. And, increasingly, school systems are looking for outside, expert help in analyzing their data.

Like most other organizations these days, district and state educational systems are managing much more digital data. Partly, that's because new technologies are producing more data, and partly because traditional data like bus routes, attendance, food service and business records have moved online.

Like other organizations, school systems often opt to store those data "in the cloud" – meaning, in remote data centers.

To be clear, the motivation here is entirely positive: To find better ways to engage students, to give teachers new tools, to improve instruction, and to help strapped school systems operate more efficiently.

The consequence of all these changes, however, is an exponential growth in the variety and quantity of data. As the use of technology and the quantity of digital data have grown, so have the concerns of parents, and of advocates, like many of you here today.

The questions you are asking are vitally important: What steps are being taken to keep student data secure, and, just as important, to keep outside businesses and other organizations from making inappropriate use of those data?

No one should make the mistake of thinking that these are unreasonable or unimportant questions. In fact, failing to take privacy questions seriously means failing to understand the modern world.

Most days, you don't have to turn far past the front page of the paper to learn something new and unsettling involving personal data. Unwanted revelations can do real and lasting damage. And obviously, the stakes are that much higher when our children are involved.

So I want to be absolutely clear that school systems owe families the highest standard of security and privacy.

No one makes you sign up for Facebook, but you have to go to school. Our expectations for the protection of children must be paramount.

The truth is, in every generation – perhaps now more like every five to ten years – a new revolution in technology forces us to contend with new questions about how to keep our kids safe.

Privacy rules may well be the seatbelts of this generation. I'd like to see vigorous self-policing by the commercial players. Frankly, it's in their interest to do so— and I'm glad to see the conversation starting here.

But I'm not going to wait for industry or rely on promises. It's on all of us – government leaders, advocates, and educators – to act.

This can't be a choice between privacy and progress. It doesn't mean—it can't mean—rolling back the availability of technology.

We know that's a historical impossibility. The toothpaste isn't going back in the tube, and we shouldn't want it to: we cannot stand between teachers and the tools they need to do their jobs and reach every child where they are.

On the contrary, we need to do a far better job of getting useful technology to educators, students, and families that deepens and accelerates learning.

We cannot ask our schools to choose between privacy and progress. School systems must have the ability to use data to get their basic business done — whether that involves organizing bus routes or analyzing instructional information.

None of that conflicts with a powerful commitment to privacy.

Protecting our students' information is more than a legal requirement – it's a moral imperative. Our children's privacy is not for sale and must not be put at risk.

Personal information that students and families provide for educational purposes should be used for educational purposes only. And both school systems and technology providers should have appropriate policies for how they handle data.

Taking action on those principles involves laws and policies, but it's also a matter of priorities and clear, consistent communication.

On the legal side, as most of you here know, three keystone federal laws protect student privacy: The Family Educational Rights and Privacy Act, The Protection of Pupil Rights Amendment, and the Children's Online Privacy Protection Act.

Together, these statutes place significant limits on how student information can be used.

But these are complex issues, and the field is developing rapidly – which is why we're committed to stepping up the pace at which we provide guidance to help school systems and educators interpret the law, including examples of best practice.

Tomorrow, we will release new guidance, with more coming in the weeks ahead.

Our Administration takes these issues seriously. That's why I appointed the first-ever executive-level Chief Privacy Officer in the Department of Education, Kathleen Styles, who has helped us to start offering technical assistance to states, districts and schools, around student privacy. Kathleen has been fantastic, and I thank her for her leadership. We established the Privacy Technical Assistance Center to provide that hands-on help.

But federal law provides only some of the guard rails for data and privacy practice. Much of the control over these issues lies in the policies of states and districts.

And, for the record, the Department of Education itself isn't allowed to create a national database of individual student-level information, aside from mandated purposes like college loans. We don't, we haven't, and we won't do that—period.

And nothing about the new assessments, developed by consortia of states as part of new, higher standards, changes that.

But there's a lot of hard work ahead. As an education community, we have to do a far better job of helping teachers and administrators understand technology and data issues. And we need to do a better job reaching the general public too.

Too often, the public discussion on these issues has become muddled, conflating separate issues.

For example, the mere fact that student data is stored in the cloud doesn't mean that it is used for an improper purpose, or that unauthorized parties or vendors have access to it. Data stored in the cloud can actually be more secure than data stored on a computer at a school. But too many families today have been led to believe that remote storage of student data means it's up for sale.

Put plainly, student data must be secure, and treated as precious, no matter where it's stored. It is not a commodity. In truth, while we have seen security breaches in schools — with both paper and digital records — we have seen few significant instances of systemic misuse of student data.

As you know, though, many of our school systems have work to do to bring policy into line with fast-changing technologies. This isn't a matter of bad intention; it's a matter of priorities. And for our schools, privacy needs to be a higher priority.

Schools and school systems should be asking themselves some hard questions. Here are five quick examples:

- Do you know what online services your schools and teachers are using?
- Are you offering teachers timely approval of technology they want to use?
- Do your contracts explicitly lay out the ownership and appropriately limit the use of any data collected?
- Are you transparent with parents about how your district uses data?
- Do your schools allow students to bring their own devices as tools for learning, and do your policies protect them?

Some districts and states are demonstrating real leadership and thoughtfulness in these areas, and we all can learn from them. For example, the Kansas State Department of Education has developed an innovative data quality certification program to train staff on data quality practices and techniques, including privacy and security.

And closer to home, Fairfax County tests software and applications to verify that vendor security and privacy promises are accurate.

But the responsibility here doesn't lay just with schools systems. Technology providers need to shoulder their responsibility for ensuring the privacy of our students as well.

There's plenty of energy, in this room and around the country, for stronger regulation of your work. Let me say this clearly: It is in your interest to police yourselves before others do.

In part, that means being transparent - not with hundred-page user agreements spread across multiple screens, but with language that parents and educators can easily understand.

It means offering districts something better than take-it-or-leave-it "Click Wrap" agreements that allow the provider to unilaterally amend its privacy practices — without even telling the district. That doesn't build long-term confidence and trust. Please demonstrate that you know what it means to be a leader for our kids, and for us, as their parents.

While I am challenging everyone in this room, I want to make clear that we challenge ourselves, every day, at the Department to be part of the solution.

First, we enforce the statutes we administer. There are important legal safeguards against misuse and commercialization of student data, and we will enforce these safeguards.

Second, we will continue to offer guidance and technical assistance to schools and districts around student privacy – as well as guidance and technical assistance around the use of education data and technology.

As the field develops, we are working to stay current and be helpful. Where we fall short, please push us. We need your best ideas—we want to be challenged.

Let me close with the bottom line: Personal data in education should be used only for educational purposes, not to sell students snack foods or video games.

Parents and schools need clear information that enables them to make good choices. In protecting our children, we all have a role to play.

So I want to challenge advocates, tech leaders, software vendors, educators, policymakers – to make protecting our students' privacy a higher priority.

I want to applaud the hard work and leadership of so many of you here to make that happen.

Together, we can and we must harness the extraordinary potential of technology to empower teachers, students and families – without faltering in our duty to protect them.

Tags:

Tweet 64 Like 37

Notice of Language Assistance: English | español | 中文: 繁體版 | Việt-ngữ | 한국어 | Tagalog | Русский