Student Privacy
and Ed Tech
Introductory Remarks

Kristin Cohen
Federal Trade Commission
Opening Remarks

Thomas B. Pahl
Acting Director, Bureau of Consumer Protection
Federal Trade Commission
Panel 1: Setting the Stage
“Technology can be a powerful tool for transforming learning. It can reinvent our approaches to learning and collaboration, shrink long-standing equity and accessibility gaps, and adapt learning experiences to meet the needs of all learners.”

— 2017 National Education Technology Plan
Technology Advancement Timeline

- Ipod: Oct. 2001
- Ipad: Apr. 2010
- Apple Watch: Sept. 2014
- Hoverboards: May. 2015
- Echo Dot: June. 2015
- Driverless Car: 2016/17
- Iphone: June 2007
- Virtual Reality: 2014
- Touchable 3D Holograms: June 2015
- Gene editing: 2016

OFFICE OF Educational Technology
INFRASTRUCTURE
To Support Everywhere, All the Time Learning

- High-Speed Connectivity to Schools
- Quality Digital Content & Resources
- Data Privacy & Security
- Digital Citizenship & Responsible Use
- Leadership
- Assessment
- Teaching
- High-Speed Wifi Throughout Schools
- Home Internet Access
- High-Quality, Low-Cost Devices
94% of schools meeting 100kbps per student goal
6.5 million students left to connect
Reimagining the Role of Technology in Education:

National Education Technology Plan

January 2017

tech.ed.gov/netp
» **Adaptive learning**: technology used to assign human or digital resources to learners based on their unique needs.

» **Individualized learning**: the pace of learning is adjusted to meet the needs of individual students¹

» **Differentiated learning**: the approach to learning is adjusted to meet the needs of individual students

» **Competency-based learning**: learners advance through a learning pathway based on their ability to demonstrate competency, including the application and creation of knowledge along with skills and dispositions
Personalized learning

refers to instruction in which the pace of learning and the instructional approach are optimized for the needs of each learner. Learning objectives, instructional approaches, and instructional content (and its sequencing) may all vary based on learner needs. In addition, learning activities are made available that are meaningful and relevant to learners, driven by their interests and often self-initiated.
PERSONALIZED LEARNING

Anywhere, anytime learning
Students needs
Student ownership
Close learning gaps
Student centered learning
Mastery Learning
Environment for learning
Immediate feedback
Find us online:

https://www.facebook.com/officeofedtech/
@OfficeOfEdTech
Web: tech.ed.gov
Blog: https://medium.com/@OfficeofEdTech/
The Children’s Online Privacy Protection Act

Peder Magee
Federal Trade Commission
COPPA BACKGROUND

- Statute enacted in 1998
- FTC’s Rule in 1999 (amended in 2012)
- Goals
  - Allow parents to make informed choices about when and how children’s personal information is collected, used, and disclosed online.
  - Enable parents to monitor their children’s interactions and help protect them from risks of inappropriate online disclosures.
BASIC REQUIREMENT

- Operators of commercial websites and online services must provide NOTICE and obtain parents’ CONSENT before collecting personal information from children < 13.
COPPA applies to Online Collection

- Websites – content accessed through Browser
- Online Services – any service available over the Internet, or that connects to the Internet or a wide area network.
  - Mobile apps
  - Internet-enable gaming platforms
  - Voice-over-Internet protocol services
  - Connected toys
Who must comply?

- Operators of child-directed websites and online services collecting personal information.
  - Assume everyone coming to site or using service is a child.

- Operators with actual knowledge they are collecting personal information from kids under 13.
  - Can include general audience sites and service collecting on their own or through another child-directed site or service.
“Personal Information”

- Full name
- Physical address
- Online contact info
- Screen or user name (functions like online contact)
- Telephone
- Social Security #
- Persistent ID
- Photo, video, audio of child’s image or voice
- Geolocation (street and town)
- Info combined with above
If covered, you must ...

- **Provide Notice**
  - Post a privacy policy and links to the policy wherever personal information collected.
  - Give parents direct notice of information practices.

- **Obtain Consent**
  - With certain exception, obtain verifiable parental consent before collecting personal information.

- **Other Data Responsibilities**
  - Access, security, collection and retention limits.
COPPA and Schools

- COPPA applies to operators of commercial websites and online services, **not to:***
  - Nonprofits
  - Public Schools
School Consent

- Operators can get consent from schools instead of parents to collect personal information from students.
  - As long as for use and benefit of the school and no other commercial purpose.
  - Best practice is go through school or district.
  - Provide notice to school.
Questions

- How should schools provide COPPA consent?
- What process should the Ed Tech provider use to obtain consent?
- What are the appropriate limits on the use of data when school provides consent?
- How should requirements concerning notice, deletion, and retention of records be handled and by whom and when?
FERPA 101 for Ed Tech

Michael B. Hawes
U.S. Department of Education
Family Educational Rights and Privacy Act (FERPA)

- Gives parents (and eligible students) the right to access and seek to amend their children’s education records
- Protects personally identifiable information (PII) from education records from unauthorized disclosure
- Requirement for written consent before sharing PII – unless an exception applies

(20 U.S.C. §1232g & 34 CFR Part 99)
Personally Identifiable Information (PII) under FERPA

- Direct Identifiers (e.g., name or id number)
- Indirect Identifiers (e.g., date or place of birth)
- “Other information that, alone or in combination, is linked or linkable to a specific student…” (§ 99.3)
“Education Records” are records:

– Directly related to the student; and

– Maintained by (or on behalf of) an educational agency or institution.
Is student information used in online educational services protected by FERPA?

It depends!

Some data used in online educational services are protected by FERPA.

Other data may not be.

Schools and Districts will typically need to evaluate the use of online educational services on a case by case basis to determine if FERPA-protected information is implicated.
FERPA Exceptions to Consent

Two of FERPA’s exceptions to the parental consent requirement are most relevant when using education technology:

– Directory information exception
– School official exception

See §99.31 for information on other FERPA exceptions and their requirements.
Directory Information Exception

- Allows schools to release certain information without consent.
- Schools/Districts must designate the data elements they consider to be Directory Information.
- Parents have a right to opt-out of disclosures under the Directory Information exception!
School Official Exception

Schools or districts can use the School Official exception to disclose education records without consent if the recipient:

• Performs a service/function for the school/district for which the school/district would otherwise use its own employees
• Is under the direct control of the school/district with regard to the use/maintenance of the education records
• Uses education data in a manner consistent with the definition of the “school official with a legitimate educational interest,” specified in the school/district’s annual notification of rights under FERPA
• Does not re-disclose or use education data for unauthorized purposes
3 Ways to Provide Student Information to Service Providers

- Consent
- Directory Information
- School Official Exception

Each method has its own limitations and requirements!
Are providers limited in what they can do with the student information they collect or receive?

If PII is disclosed using **Written Consent**:
- Limited by the provisions of the consent statement

If PII is disclosed under the **Directory Information** exception:
- Typically, no limitations

If PII is disclosed under the **School Official** exception:
- PII from education records may only be used for the specific purpose for which it was disclosed
- Providers may not sell or share the PII, or use it for any other purpose except as directed by the school/district and as permitted by FERPA
For More Information:

Protecting Student Privacy while Using Online Education Services: Requirements and Best Practices

Available at https://studentprivacy.ed.gov
Privacy Technical Assistance Center

http://studentprivacy.ed.gov/

Help Desk (privacyTA@ed.gov)

Guidance and Best Practice Documents
  o Data Sharing under FERPA
  o Data Security
    ...and much, much more.

Videos
  o FERPA for Parents and Students
  o Designing a Privacy Program
    ...and many others.
State Student Privacy Laws

Amelia Vance, Education Policy Counsel
Future of Privacy Forum
Landscape of Privacy Concerns

- The “cloud” and other amorphous terminology
- The scope and type of student data schools collect
- Who is collecting and accessing student data/education records
  - Federal/State
  - Third parties
- How student data is being used
- Privacy beyond data
States Have Passed 124 Laws Since 2013

40 States Have Passed 124 Laws Since 2013

Legislates Vendors and SEAs and/or LEAs
Legislates Vendors
Legislates SEAs and/or LEAs
Introduced but did not pass into law
## State Student Privacy Laws

**Passed 2013-2017**

<table>
<thead>
<tr>
<th>Year Passed</th>
<th>State</th>
<th>Bill Number</th>
<th>High Level Summary</th>
<th>Early Ed (Y/N)</th>
<th>K-12 (Y/N)</th>
<th>Higher Ed (Y/N)</th>
<th>Legislateing Vendors (Y/N)</th>
<th>Legislateing SLAs (Y/N)</th>
<th>Legislateing LEAs (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Arizona</td>
<td>SB1450</td>
<td>For school districts that release directory information to educational and</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>occupational/industrial recruiters, they must provide students with the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>opportunity to opt out of or that released. Student transcripts cannot be</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>be released unless the student consents in writing.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Arizona</td>
<td>SB1430</td>
<td>An Act Relating to School Accountability: Requires the Department to</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>compile an annual achievement profile – any disclosure of educational</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>records compiled by the department of education must comply with</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FERPA.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Arizona</td>
<td>HB2000</td>
<td>HB 2008 prohibits public schools from administering specified assessments or</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>surveys to students without notifying and obtaining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>written informed consent from parents and receiving written consent for</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** [https://ferpasherpa.org/state-laws/](https://ferpasherpa.org/state-laws/)
19 States Have Passed Laws Based on SOPIPA

Student Privacy and Ed Tech

December 1, 2017
SOPIPA

- Applies to operators of a website, online service, or online or mobile application when their product is for K-12 school purposes and was also designed and marketed for K-12 purposes
SOPIPA

- SOPIPA protects personally identifiable information or materials, in any media or format, that:
  - is provided to the operator by a student or parent for K-12 school purposes;
  - is created or provided to the operator by the school, district, or other LEA; or
  - is gathered by the operator through the operation of their service and is descriptive of a student or otherwise identifies a student.
SOPIPA

- An operator must not:
  - Target advertising
  - Create a profile (except for K-12 school purposes)
  - Sell a student’s information
  - Disclose covered information
SOPIPA

- An operator must:
  - Implement and maintain reasonable security procedures and practices
  - Delete information when asked by the LEA
General State Law Trends
Louisiana schools struggle with strict privacy law

In Louisiana, a new law bars school districts from sharing personally identifiable information without parental consent too far.

State Withholds High School Graduation Rates

By Nate Robson July 29, 2015

New State Law Complicates Classroom Recording For N.H. School Districts

By RICK GANLEY & MICHAEL BRINDLEY - NOV 11, 2015

A new state law limiting when schools can record in classrooms is having unintended consequences for some New Hampshire school districts.
Interesting Trends

- Governance
- Training
- Audits
- Opt-In or Out Requirements
- Device and social media privacy
- Penalties
Panel 2: School Perspective

Panelists

Allen Miedema, Technology Director, Northshore School District, Washington
Chris Paschke, Executive Director of Data Security, Jeffco Public Schools, Colorado
Jim Siegl, Technology Architect, Fairfax County Public Schools, Virginia
Rachael Stickland, Co-Chair, Parent Coalition for Student Privacy

Moderator

Michael Hawes, Director of Student Privacy Policy, Department of Education
Panel 3: Student Privacy Issues and Challenges

Panelists

Linnette Attai, President, Playwell LLC
Dan Crowley, Trust & Safety Manager, Quizlet
Bill Fitzgerald, Technologist, Common Sense Media
Priscilla M. Regan, Professor, Schar School of Policy and Government, George Mason University
Melissa Tebbenkamp, Director of Instructional Technology, Raytown Quality Schools, Missouri

Moderators

Michael Hawes, Director of Student Privacy Policy, Department of Education
Peder Magee, Senior Attorney, Federal Trade Commission
Panel 4: Where do we go from here?

Panelists

David LeDuc, Senior Director, Public Policy, Software & Information Industry Association
David Monahan, Campaign Manager, Campaign for a Commercial-Free Childhood
Francisco Negrón, Chief Legal Officer, National School Boards Association
Steve Smith, Chief Information Officer, Cambridge Public Schools, Massachusetts
Rachael Stickland, Co-Chair, Parent Coalition for Student Privacy
Amelia Vance, Education Policy Counsel, Future of Privacy Forum

Moderators

Kristin Cohen, Senior Attorney, Federal Trade Commission
Kathleen Styles, Chief Privacy Officer, Department of Education
Closing Remarks

Kathleen Styles
Chief Privacy Officer
U.S. Department of Education