Regulating AI in Education: Trends, Best Practices, & Opportunities

02/18/2025

PUBLIC INTEREST PRIVACY CENTER

Legal Disclaimer

The information provided in this presentation does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available are for general informational purposes only. Information in this presentation may not constitute the most up-to-date legal or other information. Event attendees should contact their attorney to obtain advice with respect to any particular legal matter. No one should act or refrain from acting on the basis of information in this presentation without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.

Amelia Vance

Public Interest Privacy Center

amelia@publicinterestprivacy.org

- 10+ years focused on child and student privacy law and policy
- President & Founder of the nonprofit Public Interest Privacy Center
- Chief Counsel for the Student & Child Privacy Center at AASA, the School Superintendents Association
- Adjunct Professor for Privacy Law and EU Data Protection at William & Mary Law School since 2022 (previously taught at Penn State)
- Co-Chair of the Federal Education Privacy Coalition

About PIPC

- PIPC is a non-profit organization with extensive expertise in the student and child privacy legal landscape and in directly supporting research organizations, policymakers, state and local education agencies, privacy and child advocates, and education membership associations. We bridge the gap between dense legal and regulatory requirements and on-the-ground applications that meet the highest ethical and privacy protective standards.
- Our vision is that high-impact stakeholders at every tier will have the information and tools necessary to protect all children's fundamental right to privacy. By educating and equipping high-impact groups and fostering a culture of privacy, PIPC will help create an environment where all children will enjoy privacy-protected benefits of emerging technologies and data use.
- In addition to our grant-funded projects–primarily focused on creating free publications and providing trainings, news updates, and analysis to policymakers and national organizations–PIPC provides consulting services in our areas of expertise. This includes personalized trainings and workshops, building and implementing privacy programs. We also provide memos on issues such as the likely effect on an organization of new state or federal laws, existing laws applicable to AI in education, the differences in HIPAA and FERPA's deidentification standards, best practices for initial vetting of third party applications used in R&D projects, and what is permissible under FERPA when creating a unique cross-agency ID for integrated data systems.

Defining AI

Defining AI

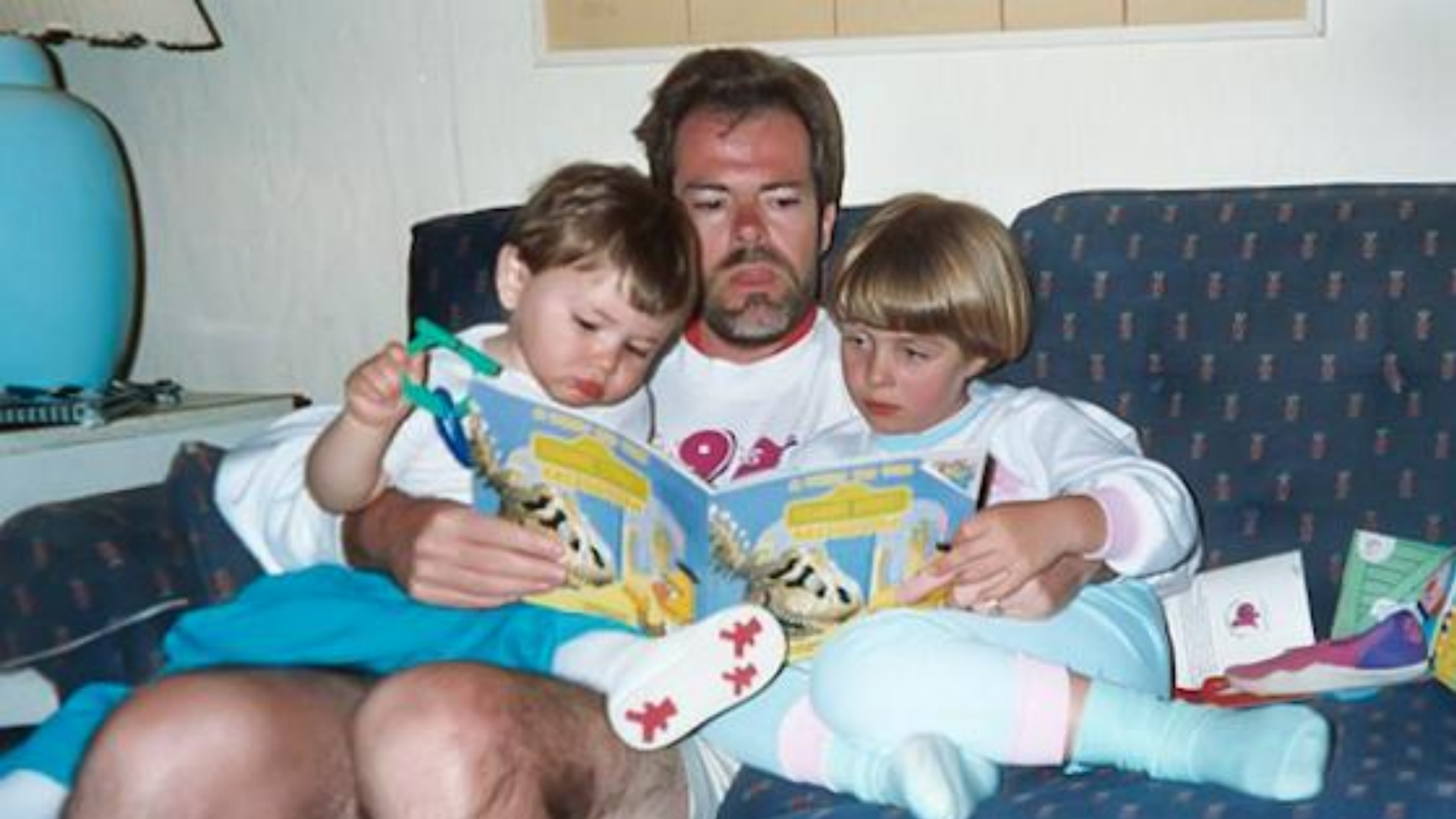
- **Artificial intelligence is the attempt to create machines that can do things previously possible only through human cognition.**
  - The first iteration of AI was “expert systems” - technologists trying emulate human knowledge by programming extensive rules into computers
  - Most of the AI you interact with on an hourly basis is machine learning: finding patterns in seas of data—correlations that would not be immediately intuitive or comprehensible to humans—and then using those patterns to make decisions.

Artificial Intelligence in Higher Education: Applications, Promise and Perils, and Ethical Questions by Elana Zeide
https://er.educause.edu/articles/2019/8/artificial-intelligence-in-higher-education-applications-promise-and-perils-and-ethical-questions

AI isn’t just ChatGPT

- **AI is also…**
  - Online Search Engines
  - Spellcheck
  - Navigation Apps
  - Facial Recognition
  - Recommendations from Amazon, Spotify, or Netflix
  - Photo Editing and Filters
  - OCRing PDFs
- **Generally, AI is in the business of predictions, with limitations and opportunities.**

What is a way that you've been using AI that makes you excited?



all, always the first person that is speaking. I should not talk so much about myself if there were any-body else whom I knew as well." HDT can only talk about himself since he is who he knows. This is HDT's explanation why he is going to answer personal questions asked of him. He is going, as he asks others to do, to account for h and not just write about someone else of w has heard. (The implication is that writing about self is direct and truthful. Writing about o and attempt to ignore and disregard truth.)

8-1-74 Th

"for if he has lived sincerely have been in a distant land to me.

"lived sincerely" is an import phrase. It implies that a person is living the way he does because of a co thoughtful belief in the righ of his mode of life.

51

the leader of the hike was college student from Wisconsin — studying natural resources —

money.

Man
his humanity
who lives under the
laws of Nature

VRS.

Man
the machine —
who lives under the law
of supply & demand

8-17 Saturday

The next sentence seems paradoxical

A wise man always remembers his ignorance — His growth requires that he realize how little he

Townsmen have Unnatural
Thoreau will be trying to bring
and Naturalness

"superfluously" (I think it mean
superficial, busy work) Will wo
more than is sufficient o
essive. (2) unnecessary or

men do Excessive wor
unnecessary — the to
against the grain of nature

is "excessive toil" prevents
the "finer fruits"

What exactly is the dre
is toil excessive?
has "no time to be any th
nine (a commercial fro

136

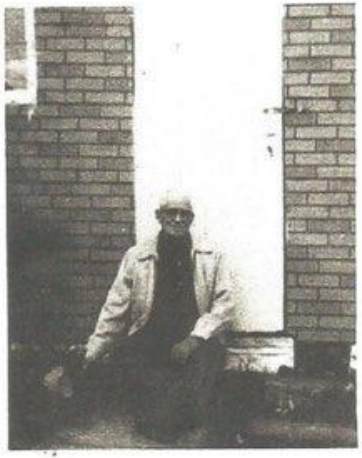
Day 34 Sunday 22 July

up 8:30 A.M.
shower & break camp
leave 9:30 A.M.

Martin

Joshua Martin, son of William and Martha Martin, lived near Round Hill on the farm now owned by Arthur Pedego. Joshua married Elizabeth Edwards, daughter of Riley Edwards. Their children were Henry, Green, Caleb and Louisa J. Caleb married Martha Ellen Fry, daughter of Josephus Valentine Fry and Margaret Morris. Lousia J. (Jenny) married John W. White, a cousin of Daisy Ferguson. Caleb was a grandfather of Stanley Potts who resides at Round Hill now.

During the Civil War, there were many conflicts nearby because Missourians were divided over the slavery question. Mrs. Caleb Martin told of three soldiers who were shot on their farm and left for many days until they wrapped them in white sheets and buried them. There are many stories of how prominent men were called to the front of their homes and shot in cold blood by the enemies. Joshua Martin was shot down at his front yard gate in 1863. His 14-year-old son, Caleb, was standing with his father.



Arthur Pedego is sitting on a step he removed from Joshua Martin's home. [Photo courtesy of Iola Potts.]

In many ways, the biggest challenges–and the greatest solutions–related to AI in K-12 are preexisting challenges about the adoption and use of technology.

Data Traditionally Collected by Schools

Demographic Information

Emergency Contact Information

Discipline Records

Health Records

Attendance

Name

Grades

Risks of Student Data Collection, Use, and Sharing

Risk	Think about...
Safety	Can a stranger or other dangerous person communicate with your students and learn personal information about them?
Permanent Record	Will youthful mistakes that students make follow them forever?
Social Harm	Can collecting and sharing student data contribute to cyberbullying and stigmatization?
Equity Concerns	How might data be biased or used in inequitable ways?
Loss of Opportunity	Will your student lose access to educational opportunities and services?
Commercial	Will companies use student data for profit?

New Data Collected by Educational Technology

Who students interact with online

What content a student accessed

How long a student viewed content

How, when, and from where content was accessed

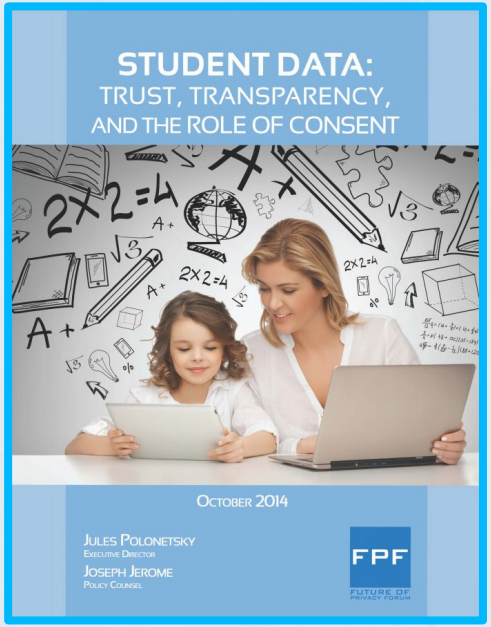
Usernames & Passwords

Individual search queries

Types of Technology

Types of Use	Example
Administrative	Course scheduling, school busing
Instructional	Online homework, learning apps
Assessment and Measurement	Standardized tests, course assessments
Optional and Non-Educational	School yearbooks, PTA fundraising

Suggested Resource:



Educational Technology (EdTech) You Might See in Your School

- Student Information Systems
- Communication & Collaboration Tools
- Learning Management Systems
- Learning Apps
- Accessibility Apps
- Classroom Management Software
- Assessment Tools

Benefits of Using Education Technology

- Makes Learning More Accessible to More Students
- Personalized Learning
- Measuring Success
- Technology Literacy
- Keeps Learning Interesting & Fun

Risks Related to Education Technology

Risk	Think about…
Safety	Are students able to share personal information with others using this technology?
Permanent Record	How long does the technology retain information about your students?
Social Harm	How might educational technology contribute to or enable cyberbullying and stigmatization of your students?
Equity Concerns	What if students do not have access to information or technology?
Loss of Opportunity	Does this technology make decisions about or impact the opportunities and services your students have access to?

THE CHALLENGE:
ALLOW OPPORTUNITIES FOR YOUTH ONLINE WHILE MITIGATING RISKS

EDUCATION

COMMUNITY BUILDING

CIVIC & POLITICAL PARTICIPATION

HEALTH & WELL-BEING

PLAY

CREATIVE EXPRESSION

Wonderful Technology Rarely Comes Without Serious Privacy Risks


ancestryDNA
DNA Activation Kit

20 July 1989

23:23 ENDS >60m

1900 p55_ F...au County.png

File 15 of 21

FARMER'S DIRECTORY OF MONITEAU COUNTY.

Share

Menu

Bureau of Consumer Protection

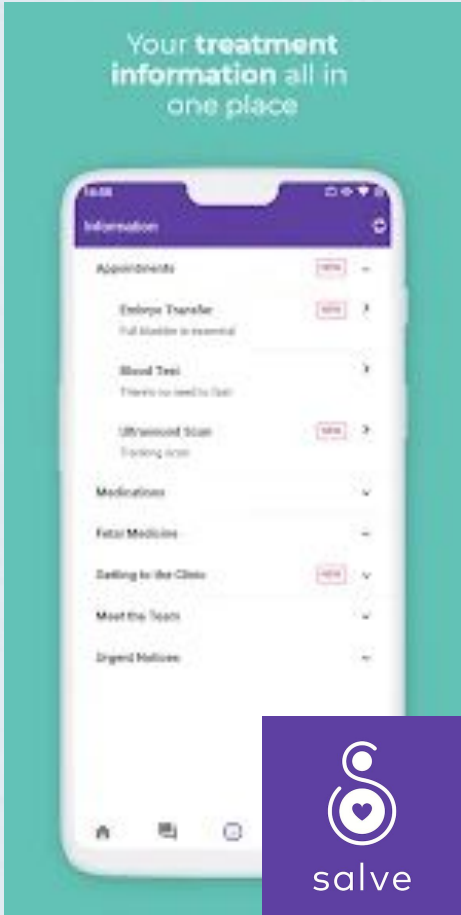
Business Alerts

From the Federal Trade Commission

FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises

By Lesley Fair

In the hierarchy of confidential data, health information ranks right up there. And in the hierarchy of health information, details about a person's mental health may be among the most confidential. But according to the FTC, that's not how online counseling service BetterHelp viewed it. The FTC says the company repeatedly pushed people to take an Intake Questionnaire and hand over sensitive health information through unavoidable prompts. And it promised to keep that information private through statements like: "Rest assured – any information provided in this questionnaire will stay private between you and your counselor." But from the FTC's perspective, a truthful statement would have been "Rest assured – we plan to share your information with major advertising platforms, including Facebook, Snapchat, Criteo, and Pinterest." A proposed FTC settlement with BetterHelp includes $7.8 million for partial refunds for BetterHelp customers and conveys an unmistakable message about just how seriously the FTC takes this kind of betrayal of trust.



We Should Be Able to Trust Companies, But We Can’t

AI Challenges

- **AI efficacy**
  - Widespread puffery (or lies) from edtech providers
  - Lack of efficacy research
  - Misunderstandings about what AI can do
- **AI adoption**
  - AI is already being used in education
  - AI is being incorporated into existing edtech without notice
- **AI understanding**
  - Application of existing laws
  - Lack of awareness about AI/algorithmic harms
  - Lack of awareness of toolkits and other useful resources (and established experts over the past decade)
- **Old challenges**
  - In many ways, the biggest challenges–and the greatest solutions–related to AI in K-12 are preexisting challenges about the adoption and use of education technology.
- **New challenges**
  - Questions about using student PII to train algorithms (past, present, and future)

We Should Be Able to Trust the Companies Used by Our Government

AI Risks for Government

- Risks involving data use and data privacy;
- Risks involving the accuracy, bias, and reliability of outputs; and
- Risks that undermine government authority and accountability.

Privacy Risks

"When you are denied the freedom to decide how your data is used—including whether and when private vendors can access your data or whether an agency will use data from commercial databases to make decisions about you—your privacy is undermined."

"Across the country, AI systems procured by government agencies are built on top of this commercial data, meaning that information you did not provide to the government—including your social media posts and browsing behavior—can influence the decisions that government AI systems make about you."

Accuracy Risks: When AI Makes Mistakes

"Because AI systems make inferences about people based on average trends in data, their outputs are generalizations about how people behave. When an AI system is used to make determinations about someone who falls outside the mean, the difference between a generalization and reality can undermine government decision-making; where a human case worker might see nuance, an AI system sees just one more data point."

"AI systems can exhibit harmful biases that undermine government decisionmaking. Because these systems are trained to recognize patterns in historical data, any historical biases will be reflected in AI decisions…When government AI systems base their determinations on biased data, their outputs can perpetuate harmful biases and strip marginalized beneficiaries of the government benefits they deserve."

Accountability Risks: Undermining Government

"[M]any government AI systems operate without much human oversight and without meaningful opportunities to dispute their outputs. Most companies that provide AI systems to government agencies maintain that the logic of their systems is proprietary, so agencies are forced to rely on contractors to operate AI systems without understanding how those systems function. Without understanding how automated decisions are made, neither agency officials nor the public can readily challenge inaccurate or biased AI decisions."

"When a government agency procures an AI system to make decisions about you, it also outsources its decisionmaking to a private vendor. And those vendors can keep the procedures their AI systems use to make decisions a secret by claiming that the software and machine-learning models behind their AI systems are 'proprietary business information.'"

Children and students are uniquely vulnerable to privacy risks, and their futures are more likely to be damaged by AI harms.

WHY CHILDREN NEED ADDITIONAL PROTECTIONS*

- Brains are not fully developed
- Lack of experience
- Different conception of privacy
- Potentially more acute harms

***BUT THEY ALSO NEED PROTECTIONS THE DAY THEY TURN 18!!!**

AASA THE SCHOOL SUPERINTENDENTS ASSOCIATION

STUDENT & CHILD PRIVACY CENTER

PIPC PUBLIC INTEREST PRIVACY CENTER

Potential Harms

Health & Safety	Is a stranger or someone dangerous able to communicate with my child or learn where my child lives?
Over-Collection & Over-Surveillance	How much information is being collected about my child?
The Permanent Record	Will my child's mistakes be recorded forever?
Loss of Opportunity	What information will be used to make determine which opportunities my child doesn't have access to?
Equity Concerns	What if the information is biased? What if it is used in an inequitable way? What if my child and I can't or don't have access to the information or technology?
Age-inappropriate Content	Is my child accessing content that isn't appropriate?
Social Harm	Is my child being cyberbullied or stigmatized?
Commercialization	Are companies selling my child's data or targeting advertising to them?

How We Can Use AI in Privacy-Protective Ways

Federal Laws

FERPA

- **ACCESS: Guarantees parents (and eligible students) access to their child's educational records; and**
- **PRIVACY: Prevents unauthorized disclosure of educational records without consent or very specific safeguards.**

But FERPA was passed in 1974, so interpreting the law in light of today's technologies can be difficult, even for experts!

Computerized record-keeping systems by several school districts may make detection of errors somewhat more difficult unless extreme care is taken by school personnel… the more frequently that records are examined…the more likely it is that mistakes will be discovered and corrected. The eventual widespread use of computers in schools, therefore, should be accompanied by policies encouraging more frequent access to school records by parents, as well as school personnel.

Does FERPA Apply?

FERPA covers **personally identifiable information** in **education records**.

Education records: records that are **directly related** to a student and are **maintained** by an educational agency or institution or by a party acting for the agency or institution. (*34 CFR § 99.3*)

But remember: *Does not include grades on peer-graded papers before they are collected and recorded by a teacher.*

Does it matter? If your state has a student privacy law, then you might want to just skip this analysis since most of the laws passed since 2014 broadly protect PII.

When can information covered by FERPA be shared with third parties?

1. Consent
2. An exception applies

Common K-12 FERPA Exceptions

Other schools to which a student is transferring; 1	Specified officials for audit or evaluation purposes; 2	Appropriate parties in connection with financial aid to a student; 3	Organizations conducting certain studies for or on behalf of the school; 4	Accrediting organizations; 5
To comply with a judicial order or lawfully issued subpoena; 6	State and local authorities, within a juvenile justice system, pursuant to specific State law. 7	Appropriate officials in cases of health and safety emergencies; 8	School officials with legitimate educational interest; 9	Directory Information; 10

...or with the Parent's or Eligible Student's Written Consent

The School Official Exception

*A contractor, consultant, volunteer, or other party **to whom an agency or institution has outsourced institutional services or functions** may be considered a school official under this paragraph provided that the outside party -*

(1) Performs an institutional service or function for which the agency or institution would otherwise use employees;
*(2) Is under the **direct control** of the agency or institution with respect to the use and maintenance of education records; and*
(3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

*An educational agency or institution must use **reasonable methods** to ensure that school officials obtain access to only those education records in which they have **legitimate educational interests** [specified in the school/LEA's annual notification of rights under FERPA].*

Legalese	What It Means
Performs an institutional service or function for which the agency or institution would otherwise use its employees;	**In an ideal world, the school would do it themselves**
Is under the direct control of the agency or institution with respect to the use and maintenance of education records;	**Can the school delete on demand? Place limitations on how the vendor is using the data? How much autonomy does the vendor have to do whatever they want with the data?**
PII from education records may be used only for the purposes for which the disclosure was made, and may not be redisclosed without the authorization of the educational agency or institution and in compliance with FERPA;	**Vendors can only use PII for the reasons why they received the PII, unless they receive additional authorization/consent from the school or parent**
Meets the criteria specified in the school, LEA, or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.	**The school's notice about the school official exception has to be broad enough to encompass what the vendor is doing for them (this is almost never an issue!)**

Direct Control Likely Does NOT Exist If A Third Party…

- Narrowly defines the data protected by the policy, or retains the right to share protected data that the user is not knowingly providing to the service, such as metadata that may be personally identifiable;
- May share de-identified information and has a broad definition of what constitutes de-identified information that would easily allow for re-identification;
- May use student data to market or advertise to students or their parents or mine or scan data and user content for the purpose of advertising or marketing to students or their parents;
- May modify the terms of agreement at any time without notice or consent from the school or district;
- May collect data about the student beyond what is needed to fulfill the educational purpose (also a red flag if provider collects data from a third-party source if the student logs into the service through a third-party website, such as a social networking site);

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf

FERPA and AI

- **FERPA Foundations**
  - FERPA's goals were to protect student records, give parents and eligible students (generally students who are 18 and older) access to records, and "prevent erroneous, biased, or unfounded allegations from limiting students' future prospects."

FERPA and AI

- **FERPA and algorithms**
  - Right of Access: “a parent or eligible student must be given the opportunity to inspect and review the student's education records” (34 CFR § 99.10)
  - Explanation of Records: “The educational agency or institution, or SEA or its component shall respond to reasonable requests for explanations and interpretations of the records.” (34 CFR § 99.10)
    - Including explaining how automated decisions in education records were made
  - Right to Amend: “An educational agency or institution shall give a parent or eligible student, on request, an opportunity for a hearing to challenge the content of the student's education records on the grounds that the information contained in the education records is inaccurate, misleading, or in violation of the privacy rights of the student” (34 CFR § 99.21)

FERPA and AI

- **Access: Eligible students and parents may need to access an algorithmic model to determine whether records are accurate**
  - Example: online proctoring technology
    - Access requests may include the algorithmic model that flagged their work because the student "would need to see at least an answer key in order to assess whether the answers in their education record are accurate." (Elana Zeide, Big Proctor: Online Proctoring Problems and How FERPA Can Promote Student Data Due Process)
- **Explanation of records: Eligible students and parents must be given enough information to understand and interpret information in education records**
  - This includes explaining how automated decisions in education records were made
- **Amend: Eligible students and parents have the right to contest and amend records that are inaccurate, misleading, or a violation of privacy**
  - Predictive algorithms may create inaccurate or misleading records

FERPA and AI

- **School Official Exception: Direct Control**
  - A school must be able to maintain “direct control” over a school official’s use, retention, and deletion of student data (34 CFR § 99.31)
  - Edtech using student data to train algorithms
    - School officials must be able to delete all PII used to train the algorithm at the school’s request.

LEGAL CONSIDERATIONS: AI AND BUSINESS CONTRACTS

APRIL 22, 2024
10:00 - 10:45 AM PT / 1:00 - 1:45 PM ET

F3 Law

AASA
THE SCHOOL SUPERINTENDENTS ASSOCIATION

STUDENT & CHILD PRIVACY CENTER

PIPC
PUBLIC INTEREST PRIVACY CENTER

FERPA School Official Exception: Application of Parental Consent Requirement

- ***Educational software typically falls within the exception to FERPA's parental consent requirement because it is considered a "school business official" that is performing an administrative function of the district and has a legitimate educational interest in the student data collected. Additionally, these companies limit resharing to serve the original purpose of the Agreement.***

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

FERPA and AI

- **Health and Safety Exception**
  - Standard: actual, impending, or imminent emergency and a school must determine whether an “articulable and significant threat” exists on a case-by-case basis, taking into account the totality of the circumstances pertaining to a threat to the health or safety of a student or others (USEd, FERPA FAQs)
  - AI technologies: schools cannot solely rely on the system's flags to disclose a student's information to outside parties

FERPA and AI

- **AI can increase the risk of re-identification**
  - FERPA has a fairly high standard for de-identification: whether "a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances [could] identify the student with reasonable certainty" (34 CFR § 99.3)
    - Proper de-identification "involves removing or obscuring all identifiable information until all data that can lead to individual identification have been expunged or masked." (PTAC, Frequently Asked Questions—Disclosure Avoidance)
  - Directory information: "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed." (34 CFR § 99.3)
  - "the risk of re-identification may be greater for student data than other information" because of the large amount of student data that is disclosed, including de-identified data and directory information. (73 Fed. Reg. 74,834)

De-identification and FERPA

A few reminders:

- **FERPA's definition of PII includes anything linked or linkable to the student - a higher standard than HIPAA!!!**
- **Aggregate data may still contain PII**
- **Removing direct identifiers is rarely sufficient to de-identify individual-level data.**
- **FERPA does not have a "Safe Harbor" de-identification standard.**
- **There may be unpleasant consequences for not safeguarding student data: The Five Year Ban!**

Parent / Guardian Consent May Be Required Because Open Generative AI Likely Exceeds FERPA Exception

- **Collecting student data which populates AI knowledge base beyond school setting likely goes beyond a “legitimate educational interest.”**
- **Populating AI knowledge base with student inserted content is also likely resharing student data beyond the scope of the original purpose of the educational software.**

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

FERPA: The Agora Letter

- Parents cannot be required to waive their FERPA rights as a condition of enrolling in an education program.
- Schools should use the School Official Exception, rather than consent, for the required apps and services.
- Review vendors' Terms of Service closely to ensure that "direct control" has been properly established.

See Letter to Agora for more information: https://studentprivacy.ed.gov/resources/letter-agora-cyber-charter-school

COPPA

COPPA does not apply to schools and there are no penalties for school violations of COPPA. However, a school might acquire COPPA parental consent obligations via contract (clickwrap or separate) with a company subject to COPPA.

The Children's Online Privacy Protection Act applies when children under 13 engage with many online learning tools. COPPA regulates companies and requires verifiable parental consent for the collection, use, or disclosure of PII from children.

If COPPA is implicated, **schools** instead of parents **may provide consent** for the disclosure of PII from children under the age of 13 to a company, if the company uses student information **solely for the benefit of the school**, not for commercial purposes.

Tip: Look for practices like whether a tool uses third-party trackers for advertising purposes which would require parental consent.

Under COPPA, a school can consent on a parent's behalf only when:

- The data collected is used only for a school authorized educational purpose;
- The company provides the school notices required under COPPA;
- If the school requests it, the company provides the school a description of the types of personal information collected; an opportunity to review a child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information; and
- Operators to delete children's personal information once the information is no longer needed for its educational purpose.
- The FTC also recommends that, as a best practice, schools consider sharing the notices provided by the company with parents and allowing parents the ability to review personal information collected.

Section 5 of the FTC Act

Federal Agencies and AI

“Technological advances can deliver critical innovation—but claims of innovation must not be cover for lawbreaking. There is no AI exemption to the laws on the books, and the FTC will vigorously enforce the law to combat unfair or deceptive practices or unfair methods of competition.”

–FTC Chair Lina Khan

- **Civil Rights Laws Potentially Implicated by AI**
  - Title VII of the Civil Rights Act of 1964
  - Title IX of the Education Amendments of 1972
  - The Americans with Disabilities Act (ADA)
  - Section 504 of the Rehabilitation Act (Section 504)

- **Discriminatory Impact: Algorithms can discriminate against students if trained on biased or unrepresentative data**
  - **AI systems that incorporate protected characteristics may violate anti-discrimination laws if racial or ethnic minorities are disproportionately flagged or receive disparate treatment**
  - **Schools may be required to provide reasonable accommodations to students that struggle to use certain AI-powered learning or assessment tools**

The Future of Federal AI Enforcement: On Hold

State Laws

STUDENT PRIVACY LAWS BY STATE

FUTURE OF PRIVACY FORUM

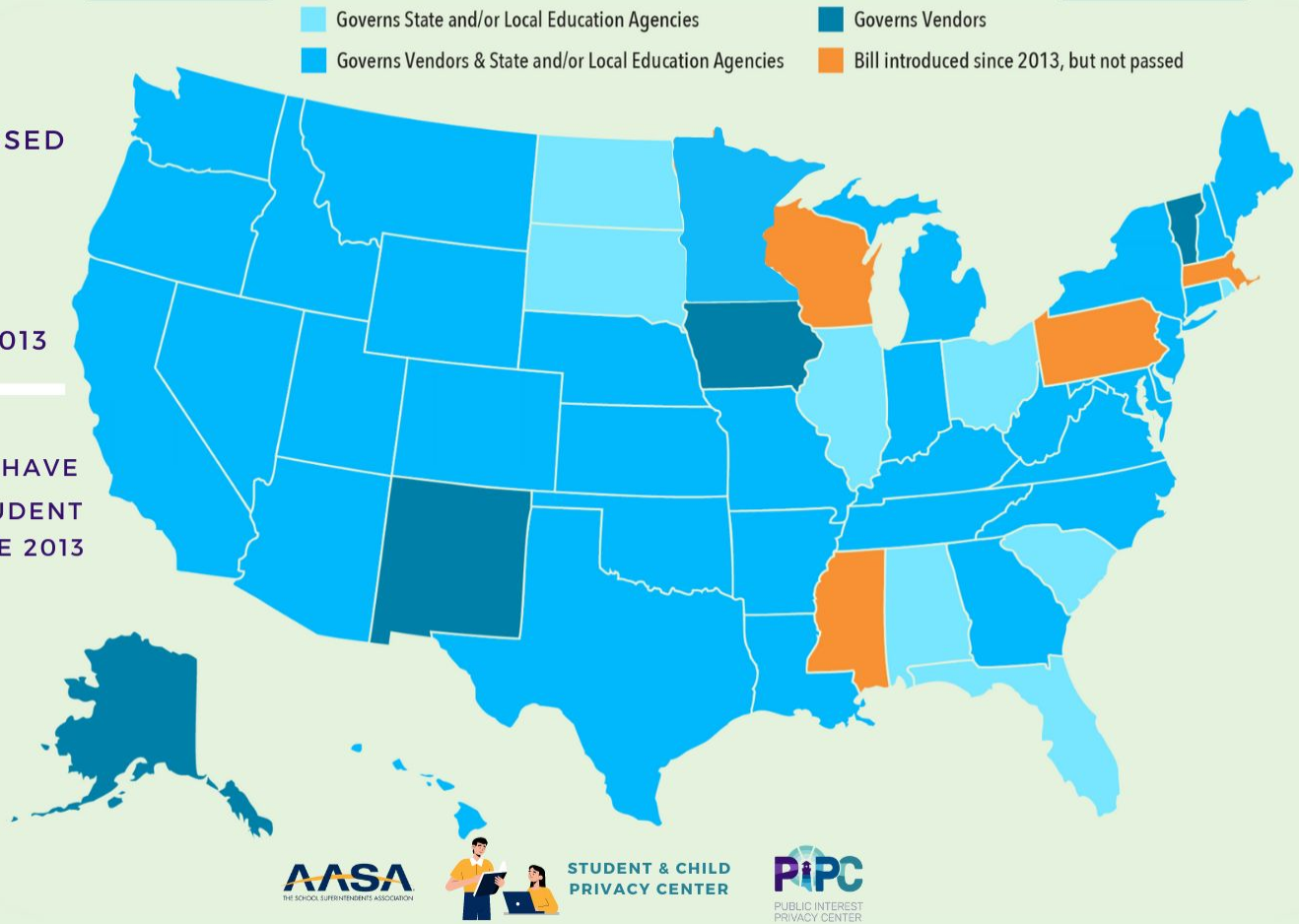
47

STATES HAVE PASSED

130+

LAWS SINCE 2013

ALL **50** STATES HAVE INTRODUCED A STUDENT PRIVACY LAW SINCE 2013

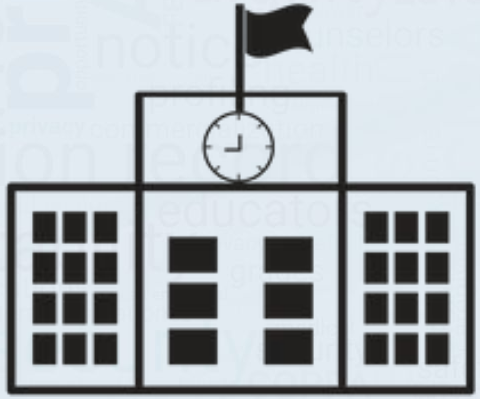


AASA THE SCHOOL SUPERINTENDENTS ASSOCIATION

STUDENT & CHILD PRIVACY CENTER

PIPC PUBLIC INTEREST PRIVACY CENTER

Two Types of Laws



based on FERPA

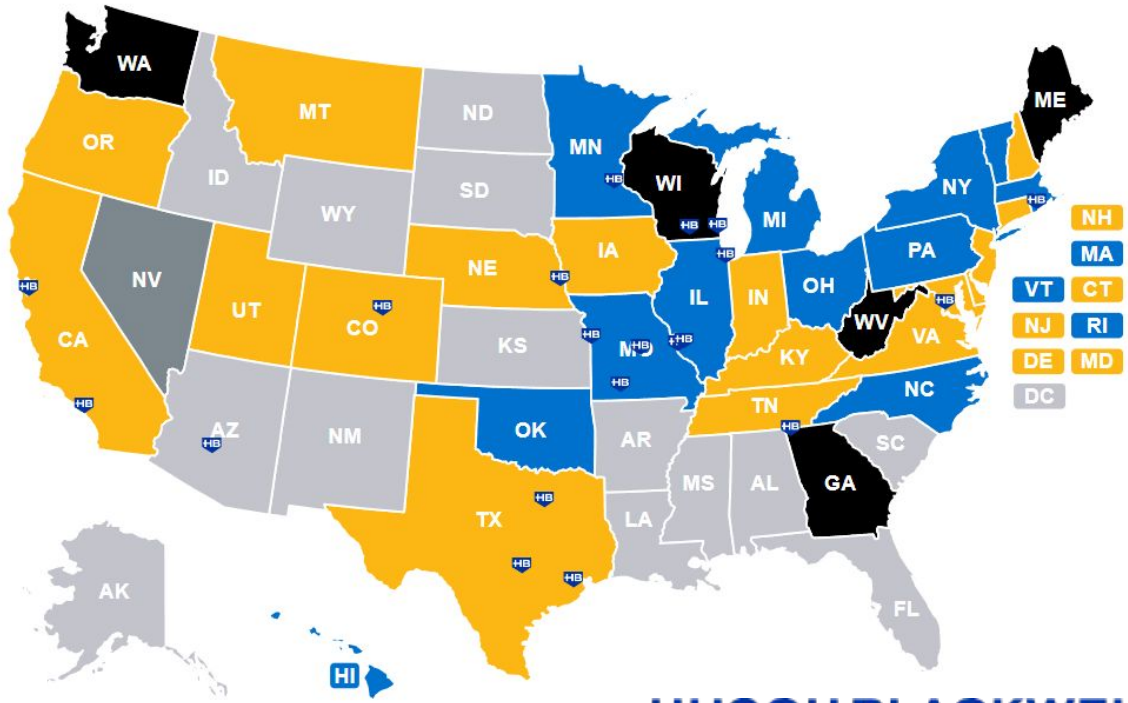
VS

based on SOPIPA

State Student Privacy Laws & AI

- State student privacy laws primarily focus on school interactions with vendors, and therefore will have broad applicability to the adoption and use of AI in schools
- As of 2020, 24 of the 36 states and Washington D.C. that regulate vendors permit them to use covered information for "adaptive learning or personalized or customized education/student learning purposes."

State Consumer Privacy Laws



- Enacted legislation
- Active legislation
- Did not pass in 2024
- Excluded legislation
- Legislature not in session in 2024
- No bill proposed

HUSCH BLACKWELL

Last updated: May 13, 2024

Consumer Privacy Laws

Opt-out of automated decision making: Numerous state consumer privacy laws give consumers the right to opt out of automated decision-making that produces legal or similar significant effects

- Including effects on education enrollment or opportunities
- Automated decision making may include profiling consumers based on their "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements"

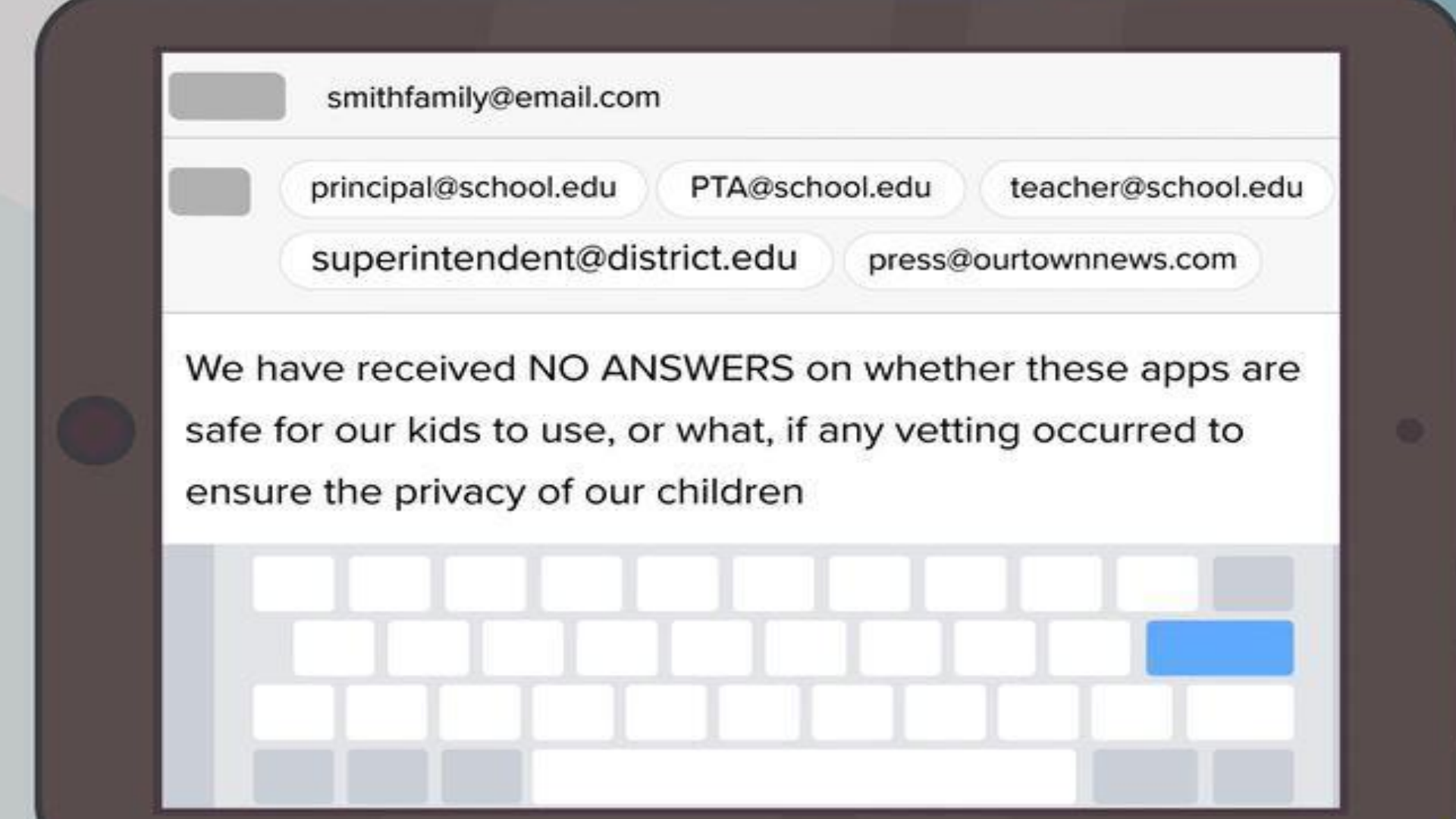
Decisions made in the educational environment have the potential to produce significant effects that follow students for a lifetime

So What Do We Do in the Absence of Clear Laws?

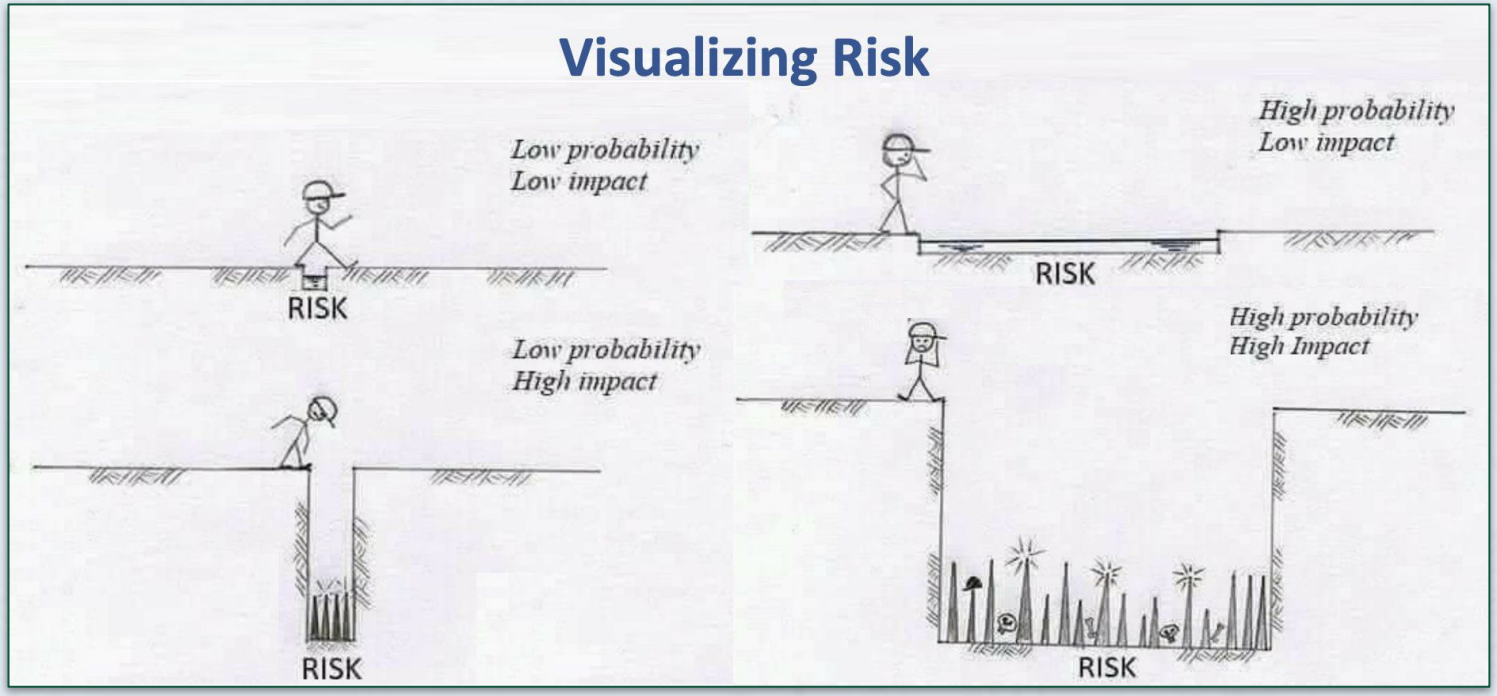
AI Challenges

- **AI efficacy**
  - Widespread puffery (or lies) from edtech providers
  - Lack of efficacy research
  - Misunderstandings about what AI can do
- **AI adoption**
  - AI is already being used in education
  - AI is being incorporated into existing edtech without notice
- **AI understanding**
  - Application of existing laws
  - Lack of awareness about AI/algorithmic harms
  - Lack of awareness of toolkits and other useful resources (and established experts over the past decade)
- **Old challenges**
  - In many ways, the biggest challenges–and the greatest solutions–related to AI in K-12 are preexisting challenges about the adoption and use of education technology.
- **New challenges**
  - Questions about using student PII to train algorithms (past, present, and future)

In many ways, the biggest challenges–and the greatest solutions–related to AI in K-12 are preexisting challenges about the adoption and use of education technology.


smithfamily@email.com
principal@school.edu
PTA@school.edu
teacher@school.edu
superintendent@district.edu
press@ourtownnews.com
We have received NO ANSWERS on whether these apps are safe for our kids to use, or what, if any vetting occurred to ensure the privacy of our children

We all have to become better at risk analysis



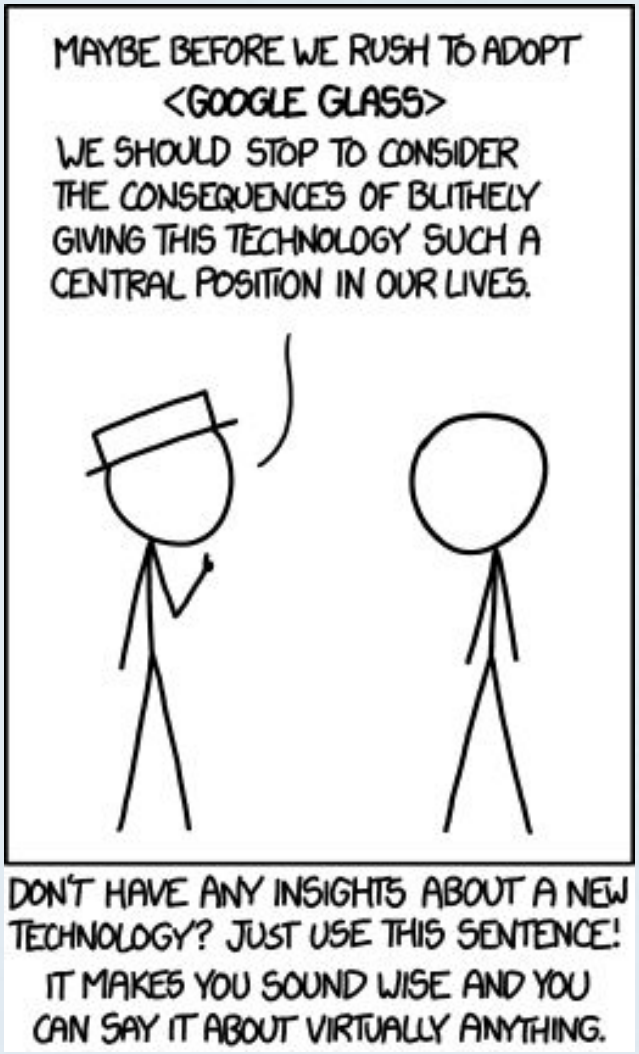
https://twitter.com/AgileMario/status/1320043917967036416

AI Risks for Government

- Risks involving data use and data privacy;
- Risks involving the accuracy, bias, and reliability of outputs; and
- Risks that undermine government authority and accountability.

Just Asking Questions is VITAL

- What questions are you trying to answer or what problem are you trying to solve?
- Where's your community's "creepy line"?
- What are the privacy risks posed by how you are collecting, using, storing, or sharing data? The key benefits?
- What governance structures, policies, and procedures do you have in place?
- How can you be proactive about public communication and engagement around privacy?



Just Asking Questions is VITAL

Raising Awareness of Why Being Careful Matters

Respecting Privacy

The success of educational programs is dependent on:

- **Local, state, and federal privacy laws and regulations**
- **Technical safeguards**
- **Ethical norms**
- **Social license: legitimacy, credibility, and public trust.**

When privacy isn't adequately supported

- **Failing to address stakeholders' privacy perceptions and concerns—even with strong privacy safeguards in place—can disrupt or end educational initiatives.**

Risks of Sharing Data Without Adequate Privacy & Security Protections

Social Harm	Sharing personal student data, especially data related to priority population status, may result in stigmatization and can lead to bullying.
Safety	Sharing sensitive data that has not been properly de-identified can endanger students by enabling bad actors to learn private information about them and potentially even locate them.
Loss of Control	If data is shared with too many third parties, it may be unworkable to keep track of every data flow and the school may ultimately lose control over who gets downstream data access.
Secondary Use	Without contractual limitations in place, third parties with whom data is shared may use project data for their own purposes in a way that exceeds the scope of participant consent and violates applicable laws (such as FERPA).
Autonomy	Participants have chosen to share their data with the school, not with unnamed third parties. Sharing project data with third parties without prior disclosure to participants would violate their decisional autonomy–and their trust–over who has access to their personal data.
Increased Attainability	Data that is shared without adequate security protections (such as encryption) may be intercepted by bad actors and made available to unintended third parties.

Encourage People to Think About…

- **AI efficacy**
  - Widespread puffery (or lies) from edtech providers
  - Lack of efficacy research
  - Misunderstandings about what AI can do
- **AI adoption**
  - AI is already being used in education
  - AI is being incorporated into existing edtech without notice
  - Questions about using student PII to train algorithms (past, present, and future)
- **AI understanding**
  - Application of existing laws
  - Lack of awareness about AI/algorithmic harms
  - Lack of awareness of toolkits and other useful resources (and established experts over the past decade)

Algorithmic Harms in Education

- **AI systems can inadvertently be unfair**
- **Algorithms are opaque and it is harder to identify when students are being harmed**
- **Students have limited control in the educational environment**
    - “Participation in…education in the United States now implicitly requires that students consent to sharing their personal information with third parties with little transparency or control over their own information.” *Cecilia Parks*

Setting Up Your Staff to Succeed

Ensuring Responsible Use in the Classroom

- ☑️ Does district have equipment to offer AI tools equitably?
- ☑️ Have staff been trained to ensure that AI generated content is free of bias and is accurate?
- ☑️ Does district have guidelines for staff and student on academic integrity and prohibition on misuse of AI?
- ☑️ Does digital literacy program include guidance on identifying misinformation and deepfakes?

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

EPIC Recommendation: Stronger Contract Language

- Improving Data Oversight and Control
- Imposing Transparency or Reporting Requirements
- Incorporating Sunsetting Clauses or Procedures to Transition Ownership to Agencies
- Requiring Human Review

A human in the loop on its own *is not* sufficient

PROCTORU TO DISCONTINUE EXAM INTEGRITY SERVICES THAT RELY EXCLUSIVELY ON AI

MAY 24, 2021 | PRESS RELEASES | SHARE:

ProctorU will become the largest test security provider to use trained human proctors for every test session.

HOOVER, Ala. (May 24, 2021, 8:00 a.m. EDT) – ProctorU—the academic division of Meazure Learning—which is the nation's leading provider of remote proctoring and integrity safeguards for online testing and assessments, today announced it will no longer offer services that do not include trained human test proctors, effectively eliminating the use of AI-only products company-wide.

The new policy details:

Games to Learn About AI Risks

Most Likely Machine - predictive yearbook awards

Moral Machine (press “start judging”) - self-driving cars

Cop Out: Automation in the Criminal Legal System

COMPAS risk assessment - criminal justice sentencing

Survival of the Best Fit - hiring

Example: Key Components of Parental Consent for AI

- ☑️ Educational benefit of Open Generative AI tool
- ☑️ Clear explanation of what data may be collected
- ☑️ If and how data may be shared beyond students' educational purpose
- ☑️ School district liability waiver

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

Accuracy & Error in Algorithmic Systems

Some technologies used by governments are inaccurate. They don't measure or detect what they claim to, or they do it poorly. This can result in decisions that adversely affect some individuals more than others. A single error in some contexts can result in a fatal or life-altering situation.

EXAMPLE–>

Automated license plate readers *can misidentify letters and numbers on the plate or the state where the plate was issued.*

EXAMPLE–>

Facial recognition systems *are never completely accurate; photos of suspects can be incorrectly matched with mugshots in a police database and falsely identify a person.*

GOALS:

Policymakers should be able to demonstrate that:

- ❑ **The system won't make false or misleading assessments**
- ❑ **People using the system are trained to recognize situations where false results are likely**
- ❑ **Robust, auditable oversight of the system is in place.**

https://www.aclu-wa.org/AEKit/questions

Accuracy & Error in Algorithmic Systems

1. **How accurate is the system? How often and under what conditions does it make mistakes? Does it have settings to adjust for more precise predictions?**
   a. What evidence is there that the accuracy of the system has been independently tested, besides the manufacturer's claims?
   b. How will the system perform in the local context where it is being deployed? Systems should be checked for their real-world performance in the places they are used.
   c. How does the system perform when presented when presented with diverse characteristics such as skin tone, lighting, signal interference, movement, or incomplete information?
2. **What policies and procedures are in place when the system makes a mistake?**
   a. How are users of the system trained to recognize and resolve errors?
   b. How do reporting processes publicly disclose errors when they occur?
   c. What mechanisms are in place for auditing outcomes?
   d. What is the role of community oversight in monitoring errors and outcomes?
   e. What penalties exist for harms resulting from inaccurate assessments?
   f. What protections are there for whistleblowers?

https://www.aclu-wa.org/AEKit/questions

Injustice in Algorithmic Systems

Even when a system works perfectly accurately, it can still cause harm. The records that the system replies on can reflect previous discrimination, or the system can be applied in unjust ways.

EXAMPLE–> ***Applicant tracking systems*** *can replicate discriminatory hiring practices because of reliance on records of previous hiring.*

EXAMPLE–> ***A 100% accurate facial recognition system*** *could be used for harmful applications, such as identifying protestors.*

https://www.aclu-wa.org/AEKit/questions

Accuracy & Error in Algorithmic Systems

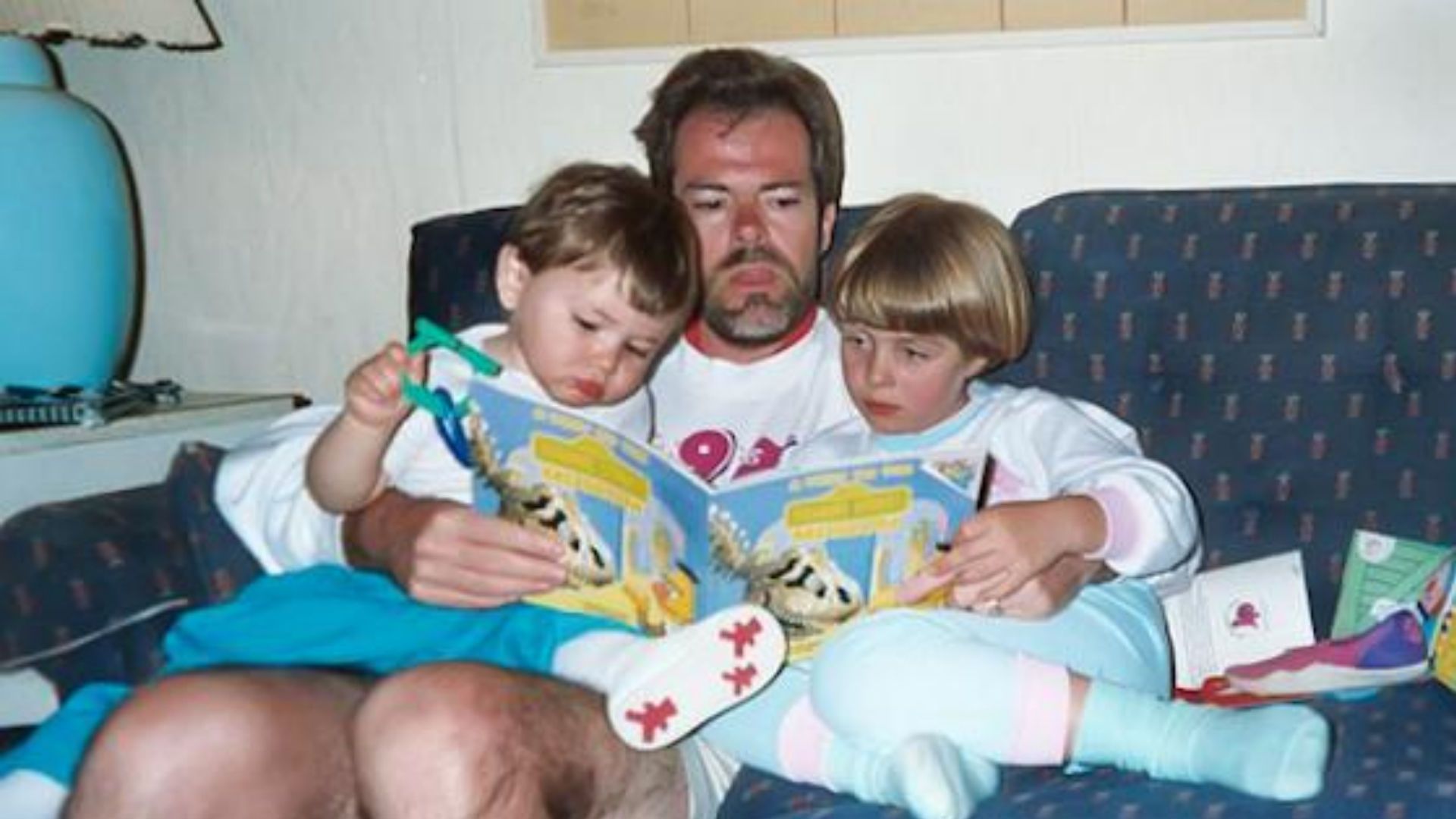
1. **Where does the data that the system is using come from? Who gathered that data, with what tools, and for what purposes?**
   a. How has the data been audited to ensure it does not reflect discriminatory practices?
   b. Will the data be repurposed from the original reason it was collected? If so, how?
2. **If the system works without errors, does it still perpetuate injustice?**
   a. What say do community members have in how the system is implemented (including where and when the system is used)? Can community members object and have their objections heard?
   b. How can the public access and correct system records?
   c. What are the explicitly intended and allowable uses of the system?
   d. Are there oversight mechanisms in place to ensure that the system is only being used for the specific purposes claimed? If so, what are they?
   e. Are there any disciplinary penalties for misuse of the system? If so, what are they?

https://www.aclu-wa.org/AEKit/questions

Making People Care

Rights-Impacting AI in Education

- Blocking, removing, hiding, or limiting the reach of protected speech
- Conducting biometric identification for one-to-many identification in publicly accessible spaces;
- Detecting or measuring emotions, thought, impairment, or deception in humans;
- detecting student cheating or plagiarism; influencing admissions processes; monitoring students online or in virtual-reality; projecting student progress or outcomes; recommending disciplinary interventions; determining access to educational resources or programs; determining eligibility for student aid or Federal education; or facilitating surveillance (whether online or in-person);
- conducting risk assessments for suicide or other violence; detecting or preventing mental-health issues;
- Translating between languages for the purpose of official communication to an individual where the responses are legally binding; providing live language interpretation or translation, without a competent interpreter or translator present, for an interaction that directly informs an agency decision or action



The Challenge: Allow Use of AI for Staff While Mitigating Risks

The Challenge: Enable AI-Assisted Opportunities for Students While Mitigating Risks

Questions?

amelia@publicinterestprivacy.org

PUBLIC
INTEREST
PRIVACY
CENTER