AI and COPPA: Statutory Analysis and Contract Drafting

We WANT your input!

Access 4 Learning Community & PESC

SESSION PRESENTERS

Jim Siegl

Senior Technologist

jsiegl@fpf.org

Mark Williams

Partner, F3 Law

mwilliams@f3law.com

The Staggering Impact of AI

In perhaps an overheated initial analysis AI has been called a paradigm shifting invention, and compared by some commentators with the internet, electricity, the steam engine or even fire.

In the short term AI and the support it needs will lead to a massive reallocation of resources in such areas as water, energy, chips and data centers. Investments and planned investments total hundreds of billions of dollars.

However it is viewed, AI can be characterized as new, rapidly expanding in its use and already ubiquitous, across many fields

Drinking From a Firehose

AI can have an overwhelming impact on the readers, with daily,even hourly articles, news, press releases and reports of new uses in such diverse fields as construction, the law and military applications.

Our presentation on AI today will have a much narrower focus. We will focus instead on the procurement and oversight of AI products by local agencies to ensure legal compliance and to help ensure products that are both safe and advances your educational goals.

Three Sources of Guidance

To accomplish this goal we will point you to three resources:

1. Recent Statutory enactments and bills likely to become statutory enactments
2. FPF - “Vetting Generative AI Tools for Use in Schools”
3. Sample Contract language.

After we examine each resource we will see commonalities between each source and the solutions each offers.

Legislation: EU Artificial Intelligence Act

The legislation is enormous, 564 pages long, included portions of 800 amendments.

Organizes scrutiny and requirements of AI systems on a hierarchy of use sensitivity: (1) Unacceptable use; (2) High risk; (3) Limited risk; and (4) Minimal risk.

Education Records: Many types of education records are considered “High Risk”.

Artificial Intelligence Act

As High Risk many education record are subject to the following requirements:

1. Adequate risk assessment
2. High quality of datasets (e.g. minimizing algorithmic bias)
3. Documentation for authorities to review.
4. Clear and adequate information to deployer
5. Human oversight
6. Appropriate security
7. Post-deployment monitoring.

United States Analog? California AB 2930

AB 2930: “Automated Decision Tools”

Not made its way to Governor’s desk yet, but now has important backing.

Regulates how decisions are made by Automated decision tools (ADTs) in a wide variety of activities, employment, loan applications , government aid and education.

Education decisions affected include, assessment (not defined) plagiarism, accreditation, admissions, financial aid, certifications.

Requirements for ADTs

1. Purpose of tools
2. Outputs of ADTs and how it affects decisions
3. Data used to make the decision
4. How the system is trained
5. How was ADT's reliability was confirmed (similar to hallucinations)
6. Any potential impact on persons from protected categories (Algorithmic bias)
7. Ability of affected person to "opt out" of system if decision is based solely of the ADT.

Very Limited Existing Guidance

Legitimate Educational Interest: Training a LLL as “product improvement”

- Existing FERPA guidance and many state laws hold that a company “may use PII to improve its delivery of these [district contracted] applications. The provider may also use any non-PII data, such as metadata with all direct and indirect identifiers removed, to create new products and services.” Some state laws (e.g. NY 2-D) consider “improvement” a commercial use)
- FERPA also provides parents th

Vendor Terms of Service

- ChatGPT prohibits use under 13 and requires parental permission for 13-17. It may not be used for any purpose that could have a legal or material impact on that person, such as making [educational decisions] about them.

Future of Privacy Forum Policy Brief

"Vetting Generative AI Tools for Use in Schools" A Policy Brief and Checklist

Major points focus on the unique attributes of AI in education:

1. Use case dependent
2. Data collection
3. Transparency and explainability
4. Product Improvement
5. Unauthorized disclosure of Student PII
6. High risk decision making

Additional FPF AI Resources: Generative AI for Organizational Use: Internal Policy Checklist and Best Practices for AI and Workplace Assessment Technologies

Contract Clauses

Draft of new AI contract clauses

1. Ownership and use of data
2. Detection and mitigation of algorithmic bias
3. Detection and mitigation of hallucinations.
4. Continuing oversight

Caveat: Performance standards have not yet been established, contract clauses may need frequent modifications as technology evolves.

The Proposed COPPA' Rule's Impact on EdTech

Access 4 Learning Community & PESC

Children's Online Privacy Protection Act (COPPA)

Applies to operators of commercial websites or online services that:

- are **directed to children** and collect personal information from children under 13; or
- have **actual knowledge** that they collect personal information from children under 13
- are Third parties that collect personal information on sites directed to children (such as ad networks or plug-ins, added in the 2013 update)

COPPA requires that covered operators:

- provide **a direct notice** with certain details about the operator's collection of personal information
- obtain **verifiable parental consent** prior to that collection (and on material changes)
- provide parents with **access** to their child's personal information
- Give parents the opportunity to **withdraw** consent to the use of personal information
- Retain child data no longer than necessary to further the purpose for which the provider collected the information.

COPPA Enforcement

- Enforced by FTC or state Attorneys General with penalties up to $50,120 per violation

WHEN CAN SCHOOLS PROVIDE COPPA PARENTAL CONSENT?

Schools *may* provide parental consent for a COPPA tool IF ALL of the following are TRUE….

1. Schools is
    - **contracting** with the vendor and,
    - considers its **obligations under FERPA and other Laws.**
2. The Operator
    - Uses student data for the **sole benefit** of the school or student (and for no other commercial purpose)
    - provides school with COPPA-required notices and rights
    - maintains data for no longer than necessary to provide the educational service
    - complies with **all other COPPA requirements**

http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools

Significant Updates Ahead for EDTech

2024 Proposed COPPA Rule

- New School Authorised Education Purpose Language
- New Security and Data Retention Requirements

Access 4 Learning Community & PESC

Jim's Three Laws of COPPA / FERPA Interaction

In the style of Asimov's Three Laws of Robotics

1. An Operator may not use the data of a student under the age of 13 for a commercial purpose or, through action or inaction, cause the school that authorized the school educational purpose to violate FERPA.
2. An Operator must obey orders given it by a school except where such orders would conflict with the First Law.
3. An Operator may disclose child PI to protect its own existence (the safety, security or integrity of the user, Web site , or online service); as long as such action does not conflict with the First or Second Law.

School Authorized Education Purpose (SAE)

Definitions

- **School-authorized education purpose** means any school-authorized use related to a child's education. Such use shall be limited to operating the specific educational service that the school has authorized, including maintaining, developing, supporting, improving, or diagnosing the service, provided such uses are directly related to the service the school authorized. School-authorized education purpose does not include commercial purposes unrelated to a child's education, such as advertising.

FTC Question

- What types of services should be covered under an SAE purpose''?
  - For example, should this include services used to conduct activities not directly related to teaching, such as services used to ensure the safety of students or schools?

School Authorized Education Purpose (SAE)

Requires: Written Agreement, Direct Notice, Online Notice, Notice/Consent on material chance.

Operator must ensure school receives direct & online notices & must have a **written agreement** with school that:

- **Indicates the name and title of the person providing authorization and attests that the person has the authority to do so;**
- Limits the operator's use and disclosure of the personal information to a school-authorized education purpose only and no other purpose;
- Provides that the operator is under the school's direct control with regard to the use, disclosure, and maintenance of the personal information collected from the child pursuant to school authorization; and sets forth the operator's data retention policy

FPF notes: Completely new language. Written agreement is not defined and has a different meaning under FERPA. Given the ambiguity on "has the authority" how would district disputes be handled, what if the person authorizing has left the school? Are vendors responsible for determining if title implies authority, what if the teacher lies? Authorizing email address is implied but not listed; if "Teacher" or class model, should authority/retention last beyond the current school year?

School Authorized Education Purpose (SAE)

***Implementations Considerations and Unknowns**:*

Does this mean that when the Rule becomes effective (likely in January or July 2025) that companies will need to get new contracts and new consent?

What if they don't / can't?

Required in Direct Notice to School

1. A school's authorization is required for the collection, use, or disclosure of personal information, and that the operator will not collect, use, or disclose any personal information from the child if the school does not provide such authorization;

2. The operator's use and disclosure of personal information collected from the child is **limited to a school-authorized education purpose**;

3. [Must list]
   a. the **items of personal information** the operator intends to collect from the child,
   b. how the operator **intends to use such information**, and
   c. the **potential opportunities for the disclosure** of personal information;

4. Where the operator discloses the personal information to third parties, list the **identities or specific categories of third parties and the specific school-authorized education purposes**;

5. A hyperlink to the **operator's online notice** of its information practices; and

6. **The means** by which the school can authorize the collection, use, and disclosure of the information.

7. Provide notice and obtain new SAE consent for any material change (term not defined in COPPA)

   FPF note: Completely new language. How should this requirement/language be viewed given the common case of separate DPAs that take typically precedence over other "agreements"?

Required Online Notice under SAE

- Must state that the operator has obtained authorization from a school to collect a child's personal information;
- That the operator will use and disclose the information for a school-authorized education purpose and no other purpose;
- That the school may review the information; and that the school may request deletion of the child's personal information, and the procedures for doing so.*

*Under SAE- The Operator is not required to provide such rights to a parent whose child has provided personal information to the website or online service. However, this right is maintained under FERPA (see note)

FPF note: The language does not specifically include the "correction" option under FERPA. It only says "request" rather than "direct". Should the "means" for school authorization be required to be listed in the online notice? How should this requirement/language be viewed given the common case of separate DPAs that take precedence over other agreements?

Potential COPPA <> FERPA Gaps

- Possible gaps between “School Authorized” and “FERPA’s “School Official” Exceptions
- Existing COPPA language related to the support for the internal operations of the Web site website or online service means means activities necessary to…
  - (v) Protect the security or integrity of the user, Web site website, or online service;
  - (vi) Ensure legal or regulatory compliance;

FPF note: School Authorized could potentially include a broader set of disclosures than what is permitted under FERPA’s school official exception, or FERPA generally. The [existing] language around permitted disclosure under internal operations is very broad, & could allow disclosures that could cause a school to be in violation of FERPA

Potential COPPA <> FERPA Gaps

- Possible **gaps** between “School Authorized” and “FERPA’s “School Official” Exceptions
- Existing COPPA language related to the support for the internal operations of the Web site website or online service means means activities necessary to (protect the security or integrity of the user or online service and ensure legal or regulatory compliance.
- **Written agreements:** Written agreement is an undefined term, but has a specific definition under FERPA’s Studies, and Audit/Evaluation exceptions. It is unclear if click through ToS meet the FTC definition, and few teachers have the authority to enter into a binding contract for a school.
- **Definition** of "personal information" in the context of school-authorized purposes vs PII in FERPA
- **Conflicts** in Data retention / deletion requirements with FERPA and state-specific laws
- **Lack of** data breach notification requirements for schools
- **Clarification needed** for "commercial purposes unrelated to a child's education"
- Potential impact on common “freemium” and trial EDTech business models (depending on interpretation of “written agreement” and who is “authorized”) and services that are both SAE and parent directed.
- **Clarification needed for** the role if any of the school as “intermediary”

New Security Requirements (§312.8)

Establish, implement, & maintain **written children's personal information security program** to:

- Designate one or more employees to coordinate children's personal information security program;
- Identify and, at least annually, perform additional assessments to identify security (CIA) risks to child PII and the sufficiency of any safeguards in place to control such risks;
- Design, implement, and maintain safeguards to control identified risks;
- Regularly test and monitor the effectiveness of the safeguards in place to control identified risks;
- At least annually, evaluate and modify the children's personal information security program to address identified risks, results of required testing and monitoring, new or more efficient technological or operational methods to control for identified risks, or other circumstances that an operator knows or has reason to know may have a material impact.
- For 3rd party disclosures-determine [they] are capable of maintaining the confidentiality, security and integrity of such the information, and must obtain written assurances for "reasonable security measures"

New Data Retention Requirements

- Personal information collected online from a child may not be retained indefinitely.
- At a minimum, the operator must establish, implement, and maintain a written children's data retention policy that sets forth the purposes for which children's personal information is collected, the business need for retaining such information, and a timeframe for deletion of such information that precludes indefinite retention.
- The operator must provide its written children's data retention policy in the notice on the website or online service provided

FPF note: This may have different requirement under SAE as operators are under the "Direct control" of the school, and most states have retention requirements for education records.