Vetting Education Technology

Ross Lemke

Privacy Technical Assistance Center

Disclaimer

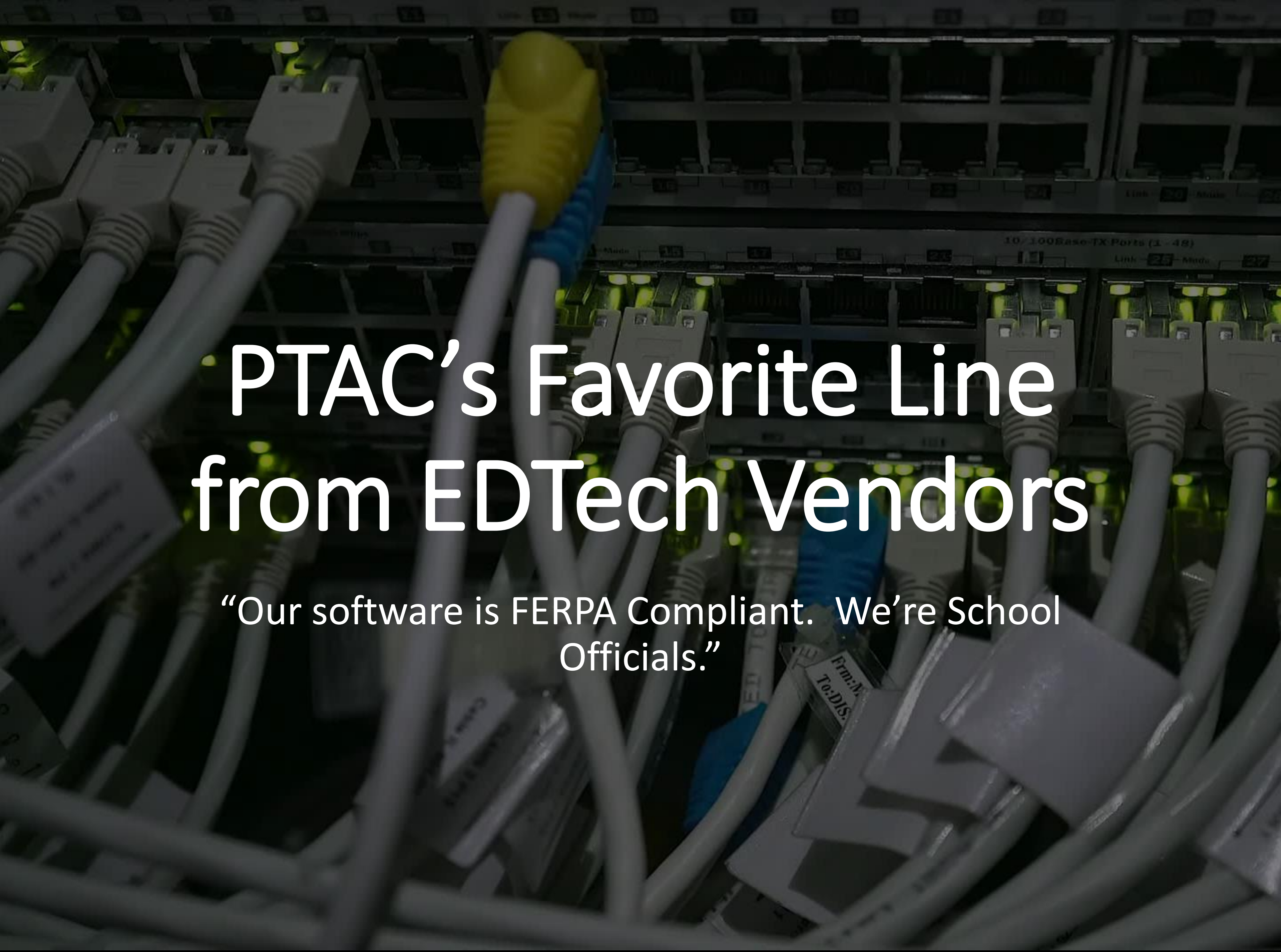
This content was produced by the U.S. Department of Education's Student Privacy Policy Office through its Privacy Technical Assistance Center for the purposes of this presentation. This presentation is provided for informational purposes only. Nothing in this presentation constitutes official policy or guidance from the U.S. Department of Education. Official policy and guidance can be found on our website at https://studentprivacy.ed.gov/.

Online Educational Services

Today’s guidance relates to the subset of education services that are:

- Computer software, mobile applications (apps), or web-based tools;
- Provided by a third-party to a school or district;
- Accessed via the Internet by students and/or parents; AND
- Used as part of a school activity.

**This guidance does not cover online services or social media used in a personal capacity, nor does it apply to services used by a school or district that are not accessed by parents or students.*



PTAC’s Favorite Line from EDTech Vendors

“Our software is FERPA Compliant. We’re School Officials.”

Things that **don’t** Exist

- Unicorns
- Dragons
- Official Department of Education FERPA seal of approval

What is an EdTech Vendor?

For this presentation, EdTech vendors are defined as companies that enhance the teaching and learning process through the power of digital technology.

How can the vendor obtain the Student Education Data?

Parent or Eligible Student Consent

Directory Information Exception

School Official Exception

Written Consent from Parent or Eligible Student

Parents and eligible students have the right to give consent before data is disclosed from the student's education record.

- **Consent from parent or eligible student**
  - Consent must be signed and dated and must:
    - Specify the records that may be disclosed
    - State purpose of disclosure; and
    - Identify party or class of parties to whom disclosure may be made

Directory Information

- Information in a student’s education records that would not generally be considered harmful or an invasion of privacy if disclosed.
- This may include: Name, address, phone number, grade, photograph….
- Each district determines their own directory policy which includes an opt out provision.
- Some districts use a limited directory information policy that restricts who can receive directory data.

Problems with providing data under the Directory Information and Consent

- **Consent** - Getting 100 percent of parents or eligible students to provide written consent is hard
- **Directory Information** – This exception to the consent rule has an opt-out provision reducing the likelihood you would receive a complete data set
- *Which leads us to…*

School Official Exception

- Schools may disclose PII from education records without consent if the disclosure is to other school officials within the school, including teachers, whom the school has determined to have legitimate educational interest.

- Schools may outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, volunteers, vendors, or other third parties **provided certain conditions are met.**

School Official Exception – *****
Conditions for Outsourcing

- Performs an institutional service or function for which the agency or institution would otherwise use its employees;
- Is under the direct control of the agency or institution with respect to the use and maintenance of education records;
- 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;
- 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.

Question

Under FERPA, are third-party service providers limited in what they can do with the student information they collect or receive?

It Depends!

Data in the hands of a Third-Party Service

Consent – Data must be used for the purposes the parent or eligible student consented.

Directory – Data must be used based on the Directory Information policy

School Official Exception – Data must be used for a legitimate educational interest. Stipulations for outsourcing must be followed.

Using Third-Party Services (TPS)

CAUTION!!!!

- Is student data entered into the software?
- Does the IT department know that this software is being used?
- Has the Terms of Service and the Privacy policy been reviewed?
- What data security measures are being applied?
- What are the data privacy measures being applied?

Is student data entered into the software?

Student Data Privacy Questions

- Does the software require directory information only?
- Has any parent opted-out of directory information?
- Is the software vendor receiving education data under the School Official exception?
- Does the FERPA Annual Notification include definition of School Official?
- Is the vendor under direct control of the school/district?
- Did the vendor agree to not share the data without the school/district approval?

Is student data entered into the software?

Student Data Privacy Questions

- Was this free software obtained by the teacher/ or other staff member?
- Do they have the right to bind the school legally and/or financially?
- Was the terms of service vetted and approved?
- Has IT reviewed/approved the software for security purposes?
- What is happening with the data that is being created by using this app?
- Is the data being stored in the cloud in another country?

Is student data entered into the software?

Data Security Questions

- Are there technical security safeguards in place to protect the security of the data in the app?
- Has the IT department reviewed and approved the security provisions of the software?
- Is there a secure authentication methods required to access the data in the app?
- Is the app being used on a laptop or mobile device?
- If it is a mobile app, does it require permissions that required access to the GPS coordinates of the mobile device?
- If the app is storing student education data in their databases, is the data encrypted while at rest and in-transit?

Is student data entered into the software?

Data Security Questions

- Does the use of this app introduce security vulnerabilities to the school IT network?
- Who in the school setting has the responsibility of mitigating risk of a data breach or an unauthorized disclosure?

Be Aware of Security Risk

- Each new application or program downloaded onto the network without the IT department's knowledge and consent could introduce risk to the school's digital environment.

Be Aware of Security Risk

- Schools are vulnerable to known third-party risks when they:
  - Aren’t aware of new software on their network
  - Don’t make timely updates to the software
  - Don’t re-evaluate applications they’ve installed.

Services can be outsourced - Risk Cannot

- The security risk is not transferred when school outsource data-related services.
- **The school is responsible for the security and privacy of its data, as well as the safety of the students.**
- It is important to be aware of the risks associated with third-party vendors and take steps to protect your students, and your school from these risk.

Terms of Service - *BEWARE*

Beware of language concerning use of data:

- *This software uses data to operate its website and deliver services. This software may also use or transfer data to third parties to inform you of products and services available from this software and its affiliates.*

Terms of Service - *BEWARE*

Beware of language concerning use of data:

- *This software uses data to operate its website and de[illegible]rvices. This [illegible]re may also u[illegible]e or transfer da[illegible]ties to inform you of produc[illegible]vices [illegible]from this software and its affiliates.*

Terms of Service – *Data Use*

"Data use" by a provider should be limited to the purposes outlined in the agreement with the school or district.

Always be on the lookout for any provision that contains the phrase "without providing notice to users".

And remember, If the data is being disclosed under the School Officials Exception, look for the Legitimate Educational Interest!

Terms of Service –
Data Use - Example

- For a parent to enroll their child in a cyber school, the parent is asked to agree to the third party's Terms of Service which *permits the third party to use, reproduce, or distribute for any purpose the information it maintains on its students.*

- ***Parent must not be made to agree to a Terms of Service that would effectively nullify their FERPA rights.***

Terms of Service – *Data Use*

- For a parent to enroll their child in a cyber school, the [illegible] is as[illegible] agree to the party's Terms o[illegible] which *permits the [illegible] party to us[illegible]produce, or [illegible]tribute for any purpose the information it maintains on its students.*

- ***Parent must not be made to agree to a Terms of Service that would effectively nullify their FERPA rights.***

Terms of Service - *Access*

FERPA requires schools and districts to make education records accessible to parents.

To fulfill FERPA requirements, providers need to make student data available upon request.

As a best practice, data should be passed from the provider to the school/district.

Terms of Condition- *Rights and License to Data*

Terms of Services
Did you ever read them?

1. **Description of Service:** The Service provides consumer content regarding insurance products and services, for informational purposes only. The Service does not sell any type of insurance and is not an insurer or insurance broker, nor does it recommend, support or endorse any particular insurance plan. The Service enables you to request to receive insurance or discount program quotes from a network of insurance companies, agents, brokers, discount program representatives and other providers (the "Insurance Representatives"). Through the Service, you choose to provide information about yourself and your insurance preferences ("User Information") which is in turn used to attempt to match you with Insurance Representatives who may be able to follow-up on your request. If you use the Service, we cannot guarantee that any of the Insurance Representatives to whom we forward your information will contact you or agree to offer you coverage. We also cannot guarantee the carrier affiliation of any Insurance Representatives who may contact you. We have no responsibility whatsoever for the conduct of any of the Insurance Repre[illegible] to you [illegible]
2. **Your U[illegible]** [illegible] at least [illegible] that, while using th[illegible] the [illegible] (a) [illegible] your affiliation with any person or entity; (b) submit false or misleading information; (c) exploit the Service for any commercial purpose; (d) engage in spamming or other similar activity; (e) restrict or inhibit others from using the Servic[illegible] a virus [illegible] through the Service; (i) take any other actions that would damage, overburden, interfere with, or otherwise harm the Service or the use of the Service by any other party. You acknowledge and agree that you are solely responsible for the accuracy of the User Information you submit. We may delete or destroy User Information at any time and we reserve the right to refuse to post or to remove any User Information, in whole or in part, that we, in our sole discretion, believe to be inappropriate.
3. **Third Party Information and Trademarks:** All content provided on this site about third parties (including companies and brokers) is provided for informational purposes only. Such content is not an endorsement of or a recommendation for any third party. It does not imply, directly or indirectly, any sponsorship or affiliation with such third parties, and no guarantees regarding the same are made herein. All third party trademarks are the property of their respective

Schools/Districts should maintain ownership of student data.

- Some TOS include provisions that would grant providers an exclusive and irrevocable license to student data.
  - This can be a cause for concern.
  - If a license is granted, it should be limited and only allow student data to be used for educational purposes as outlined in the agreement.

Terms of Service-
Marketing and Advertising

- Information gathered in an online educational service or mobile application could be used to create a profile on a student.
- That profile could then be used to direct advertising or marketing materials to students.
- The language in a TOS should be clear that the data collected cannot be used to advertise or market to students.
  - Targeted advertising or marketing could violate privacy laws (federal and state).

Terms of Service – *Data Security*

- Student data needs to be protected, and a provider's TOS should include provisions outlining strong policies safeguarding those data.

- Failure to provide adequate security could lead to a FERPA violation.
  - What technical safeguards are in place for the data in the app?
  - How is the data store? Encrypted or unencrypted?
  - What data does the app have access to?
  - Are the apps using strong access protocols?
  - What data are the apps collecting and using? Mobile device?
  - Where is the data stored? US or other country?

Terms of Service – *Data Security*

- All apps are collecting data about the student in addition to what is entered. Even if it is only metadata.
- For principals or IT leaders to accept risk – they must first understand the magnitude of the risk.
- If IT leaders or principals don't know that the apps are being downloaded and used, they aren't aware of the security risk involved.

Data De-Identification -*BEWARE*

"This software may use de-identified data for product development, research, or other purposes. Data will have all names and ID numbers removed."

Even stripped of identifiers, student data could still be identifiable (through demographic or contextual information collected by the app, or through information available elsewhere).

Best Practices for Protecting Student Privacy and Security

Have policies and procedures to evaluate and approve **<u>proposed</u>** educational services.

Borrow from other education entities or organizations that have already vetted apps and have a list of already approved apps.

Put measures in place to prevent new apps being placed on the network without approval.

Suggestion: Rent a geek to help with risk analysis of apps being used currently.

Best Practices for Protecting Student Privacy and Security

- Create a list of approved software applications and share with teachers.
- Annually, or more frequently, determine the use level of apps.
- When possible, use a written contract or legal agreement.
- Be transparent with parents and students.
- Consider that parental consent may be appropriate.

Best Practices for Protecting Student Privacy and Security

- Don’t be the “NO” person!
- Provide educators a process for requesting and installing digital tools for their classroom.
- Educate teachers on data privacy laws, such as the Family Educational Rights and Privacy Act (FERPA) and the Children’s Online Privacy Protection Act (COPPA).

Best Practices for Protecting Student Privacy and Security

- Ensure the software provider commits to regular updates that address security vulnerabilities and privacy concerns.
- Ask IT to provide technical guidelines to streamline application selection to ensure they meet technical and educational requirements while minimizing potential challenges.
- Technical guidelines can also verify that apps are compatible with the school’s devices, software and operating systems while complying with federal data privacy regulations like FERPA and COPPA.

Question:

Should school or district staff be concerned if a TPP uses a “Click-Wrap” agreement instead of a traditional contract?

Answer: ***It Depends***

- Click-wrap or Terms of Service (TOS) agreements are not prohibited.
- Nothing in FERPA says that staff cannot click that "Accept" button.
- However, there are some considerations… (like everything else we've discussed today)

Can individual teachers sign up for free (or “freemium”) education services?

Here’s a better question: Should individual teachers sign up for Free or “Freemium” services?

Teachers aren’t responsible for making technical decisions about apps.

Click-Wrap Agreements

- These agreements are referred to as “click-wrap” agreements and can operate as a provider’s legally-binding contract.
- Once a user at your school or district clicks “I agree,” the ***terms of this agreement*** will likely govern what information the provider may collect from or about students and with whom they may share it.
- Who is managing the risk of downloading these apps to your network?

Click-Wrap Agreements (cont'd)

- Click-Wrap agreements could potentially lead to a violation of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), or other laws, as well as privacy best practices.
- The onus is on the school or district to review the TOS to see if it is acceptable and complies with Federal and State law.
- *The TPP has a click-wrap agreement to protect them, not necessarily you.*

Technology is here to stay

As education professionals it is our responsibility to ensure student education data is kept private and secure.

Student education data should be used only for the purpose it was shared and not disclosed to an unauthorized entity.

Student education data must be protected.

The first step in this is to develop a policy on the use of apps in the classroom.

- PTAC Training Video

Protecting Student Privacy While Using Online Educational Services

Protecting Student Privacy While Using Online Educational Services
MORE VIDEOS
0:10 / 9:30
CC
YouTube

Contact information

United States Department of Education,
Privacy Technical Assistance Center

☎ (855) 249-3072
(202) 260-3887

✉ privacyTA@ed.gov

💻 https://studentprivacy.ed.gov