Protecting Student Privacy While Using Online Educational Services

December 2016

BARON RODRIGUEZ
Privacy Technical Assistance Director

United States Department of Education
Privacy Technical Assistance Center

Overview

- The changing landscape of education technology in schools
- The U.S. Department of Education's role in protecting student privacy
- Legal protections for students' information used in online educational services
  - How FERPA and PPRA protect student information used in online educational services
  - Other laws to consider
- Beyond compliance: best practices for protecting student privacy
- Resources for developing your own policy on third party applications

Use of Education Technology in Schools

- Student Information Systems
- Productivity applications
- Educational applications
- Fundamental school services

Online Educational Services

This guidance relates to the subset of education services that are:

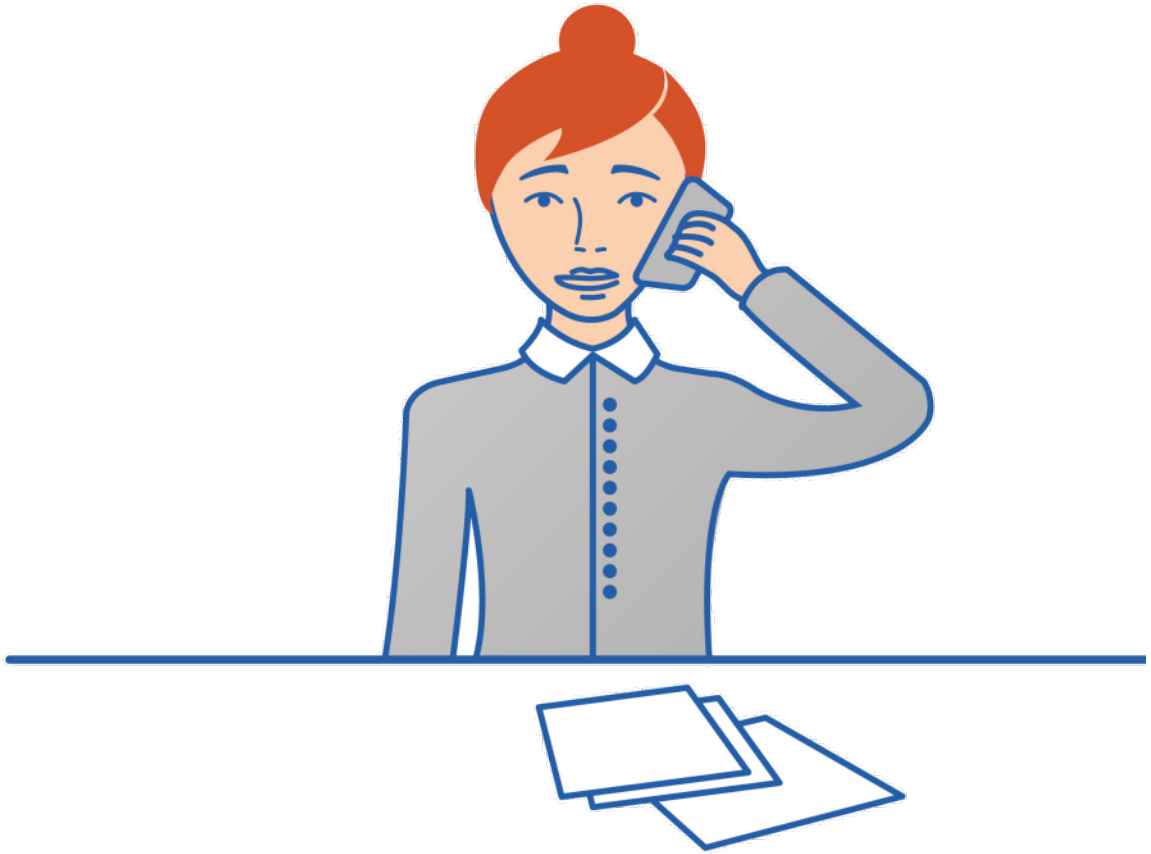
- Computer software, mobile applications (apps), or web-based tools;
- Provided by a third-party to a school or district;
- Accessed via the Internet by students and/or parents; AND
- Used as part of a school activity.

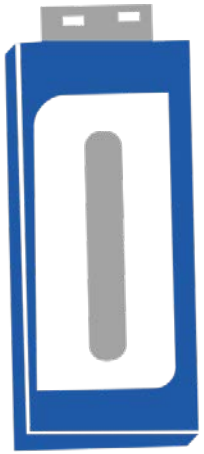
**This guidance does not cover online services or social media used in a personal capacity, nor does it apply to services used by a school or district that are not accessed by parents or students.*

The Challenge of Online Educational Services

- Schools and districts are increasingly contracting out school functions
- We have new types of data, and much more of it!
- Many online services do not utilize the traditional 2-party written contractual business model
- Increasing concern about the commercialization of personal information and behavioral marketing
- We need to use that data effectively and appropriately, and still protect students' privacy

Let's test your data security posture!





Android Best Practices

- The best thing you can do to protect against Android mobile application vulnerabilities and malware is to educate users about access permissions after installing a mobile application. User approval is required before any app can access other data or apps on an Android device. Just as you train users not to open strange email attachments, they should be equally cautious with requests from apps to access data they shouldn't need access to.

Well…

- Mobile application vulnerabilities are not limited to Android apps. A mobile application called Path, for example, offered a new way to socialize with friends and was hailed for its great user interface. Then someone sniffing the network activity of the app revealed that Path uploaded entire contact lists to its servers. It did not ask permission to do so in the iOS version of the app. Path had to apologize for unauthorized storage of users' personal data.

School Official Exception

- Schools or LEAs can use the School Official exception to disclose education records to a third party provider (TPP) if the TPP:
  - Performs a service/function for the school/district for which it would otherwise use its own employees
  - Is under the direct control of the organization 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/LEA's annual notification of rights under FERPA
  - Does not re-disclose or use education data for unauthorized purposes

Protection of Pupil Rights Amendment (PPRA)

- Amended in 2001 with No Child Left Behind Act
- Mostly known for its provisions dealing with surveys in K-12
- Includes limitations on using personal information collected from students for marketing
- May require parental notification and opportunity to opt out
- May require the Development of policies in conjunction with parents
- However … a significant exception for "educational products or services"

Question:

What does FERPA require if PII from students' education records is disclosed to a provider?

What does FERPA require if PII is disclosed to a provider?

- Parental consent for the disclosure; OR
- Disclosure under one of FERPA's exceptions to the consent requirement. Typically, either:
  - Directory Information exception
    - Remember parents' right to "opt-out"
  - School Official exception
    - Annual FERPA notice
    - Direct control
    - Use for authorized purposes only
    - Limitation on re-disclosure
    - *Remember parents' right to access their student's education records*

Question:

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

Are providers limited in what they can do with the student information they collect or receive?

If PII is disclosed under the Directory Information exception:

- No limitations other than what the school/district includes in their agreement with the provider.

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
- TPPs 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

When personal information is collected from a student, the PPRA may also apply!

- *PPRA places some limitations on the use of personal information collected from students for marketing*

What limitations does UT HB358 put on vendors?

- Must have provisions in contracts with 3rd parties that have:
  - Requirements & restrictions related to the collection, us, storage, or sharing of student data
  - Description of people who have access/who they will share the data with
  - Provisions for deletion of data by the 3rd party
  - Prohibitions on secondary use of the data
  - Audit clauses

- Likely every entity in this room is in violation of this clause!! (downloads of click wrap apps)

However… Utah SBE can help!!!

Best Practices for Protecting Student Privacy

- **Maintain awareness of other relevant laws**
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- 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

- Maintain awareness of other relevant laws
- **Be aware of which online educational services are currently being used in your district**
- Have policies and procedures to evaluate and approve proposed educational services
- 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

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- **Have policies and procedures to evaluate and approve proposed educational services**
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Question:

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

Using free or "freemium" educational services

Remember the FERPA's requirements for schools and districts disclosing PII under the school official exception.

- Direct control
- Consistency with annual FERPA notice provisions
- Authorized use
- limits on re-disclosure

These services may also introduce security vulnerabilities into your school networks

It is a best practice to establish district/school level policies governing use of free/freemium services, and to train teachers and staff accordingly.

Districts fighting an uphill battle

- Educators want the freedom to introduce ED-Tech to the classroom…
  - Question 1: Do UT state and local laws allow teachers to enter into legally binding contracts?
  - Question 2: Does Federal Law prohibit the types of data being collected by the app?
  - Question 3: Does UT Law (HB 358) prohibit the types of data being collected by the app?

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- **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

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- 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

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- **Consider that parental consent may be appropriate**

Question:

What provisions should be in a school or district's contract with a provider?

Best Practices for Contract Provisions for Online Educational Services (See Website!!)

- Security and data stewardship provisions
- Data collection provisions
- Data use, retention, disclosure, and destruction provisions
- Data access provisions
- Modification, duration, and termination provisions
- Indemnification and warranty provisions

Question:

What about online educational services that use “click-wrap” agreements instead of traditional contracts?

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.

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.

Regardless of your answer!

- Every school or district should have a policy in place for reviewing agreements before the service or application is used in the classroom.
  - Schools/Districts should establish a review process and/or have a designated individual review TOS before its adoption.
  - The service or application should be inventoried, evaluated, and support the school's and district's broader mission and goals.

But the vendor says it's De-identified first!!

- It can be difficult (and arguably impossible) to completely de-identify data.
  - That's why it's important for providers to not only de-identify student data, but also commit to not re-identify those data, and require any subsequent holders of those data to make the same commitment.

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/marketing materials to students.

Marketing and Advertising (cont'd)

- The language in a TOS should be clear that the data collected cannot be used to advertise or market to students.
  - Targeted advertising/marketing could violate privacy laws.

Modification of Terms of Service

- Many TOS include provisions for provider modification of the Terms of Service
  - Unfortunately, it's not unusual for a TOS to allow the provider to make material changes without notice to or consent from the school or district.
- Requiring notice in order for the provider to change their terms is more common than requiring consent.

Data Sharing

- Providers often use subcontractors.
  - While it's ok to use subcontractors, it's important for providers to be transparent about the data that is being shared and what is being done with those data.

Data Sharing (cont'd)

- The school/district should be made aware of every subcontractor who receives student data
  - And those subcontractors should be subject to the same limitations contained in the provider's TOS

Rights and License In and To Data

- 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.

Knowledge is Power

- Educate Your Staff
- Put a Policy in Place

- PTAC Video Resource: https://www.youtube.com/watch?v=deo2F19DK_o

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

http://ptac.ed.gov

(855) 249-3073