Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

April 13, 2015

Baron Rodriguez,
Director, Privacy Technical Assistance Center
Shane Morrisey,
Privacy Advisor, U.S. Department of Education

Webinar Logistics

- Phone lines will be muted.
- Interactive polls.
- The recording of this webinar will be made available on the PTAC website: https://studentprivacy.ed.gov
- Citations are available within the new guidance document.

Questions

- Please type your questions in the chat box in the lower right hand corner of the webinar window.

What We'll Cover Today

- Online Educational Services
- The Student Privacy Landscape
- Click-Wrap Agreements
- Good and bad privacy-related Terms of Service (TOS) provisions

What We Hope to Accomplish Today

- Context about the current student privacy landscape as it relates to contractual terms of service
- What it means to click “I accept”
- A better understanding of potential terms of service areas to review

Evaluating Terms of Service

- The Model Terms of Service guidance is offered by the Privacy Technical Assistance Center (PTAC) to help schools and districts evaluate TOS agreements.

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 (if not most) online services do not utilize a traditional 2-party contractual business model

Federal Privacy Statutes

- FERPA, PPRA, NCLB, IDEA, NSLA, Patriot Act, COPPA, and HIPAA
- Overview of statutes—Fig. 2-1 on p.42 of the Forum Guide to Protecting the Privacy of Student Information
  - Protect the privacy rights of students and their families
  - Affect data collection, maintenance, and disclosure procedures
  - Encompass education records kept in electronic and paper media

National Landscape

- In 2014 over 100 bills related to student privacy were introduced in 36 states

- As of February, 102 bills have been introduced in 32 states in 2015!

SOPIPA

- The Student Online Personal Information Protection Act (SOPIPA) was passed last year in California

- While FERPA places privacy obligations on schools and districts, SOPIPA will place obligations on 3rd party providers of educational services and will prohibit the use of student information for advertising purposes

Vendor Response

The Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) announced a K-12 school service providers pledge to safeguard student privacy built around a dozen commitments regarding the collection, maintenance, and use of student personal information.

- There are currently 128 signatories to this pledge

Potential FERPA Changes?

- Hearings with a focus on:
  - Expanding FERPA to apply to vendors and not just educational agencies
  - Expanding the legal definition of an “educational record” to explicitly include digital data and metadata generated by software, websites, apps, and online learning platforms
  - Including a “graduated” enforceable series of penalties for FERPA violators, and allowing individual families a private right of action
  - Including requirements around data security standards and notification of data breaches

Poll: Who is in the Audience?

Please indicate which sector you represent:

A. K-12 Administration
B. K-12 Teachers
C. Post-Secondary Administration or Faculty
D. Education Technology Industry
E. Other (e.g., parent/student, non-profit org., etc.)

FERPA & PII Disclosures

What does FERPA require if Personally Identifiable Information (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*

Providers use of education records

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
- Providers may not sell or share the PII, or use it for any other purpose except as directed by the school/district and as permitted by FERPA

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*

Terms of Service Provisions

- The recently released guidance, *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service* evaluates a number of provisions related to privacy that may be found in a TOS, Privacy Policy, or other contract offered by a provider of online educational services or mobile applications.

Take it or Leave it

- A traditional contract involves a buyer and seller agreeing on a set of terms and signing a contract containing those agreed-upon provisions.
- This is often not the case with many online educational services and mobile applications.

I Agree...?

- Many providers of online educational services and mobile applications (vendors, contractors, and other service providers) rely on a TOS agreement that is not negotiated.
- You've probably (hastily) scrolled past many similar agreements before (quickly) clicking "I agree" when adding an app to your phone or tablet.

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.

Developing District Policy

- 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.

Poll: Familiarity with TOS

We've all seen click-wrap agreements before, but have you actually read an entire agreement before clicking "I agree"?

A. Of course!
B. I skim.
C. Honestly, no.
D. I tell people that I do, but I'm actually lying.

Privacy-Related TOS Provisions

- We'll now begin discussing example provisions from TOS
- The example provisions are intended to give you a general idea of what to expect when reviewing a TOS
  - Please keep in mind that specific language will vary from TOS to TOS

Student Data

- Defining Student Data
  - Often a TOS will begin by providing a definition of “Data” or “PII” that will be used throughout the agreement.
  - When defining student data, the more info protected, the better.

Student Data (cont'd)

- Defining Data
  - Note: the term used to define the student information that is being collected, used, or shared may be different from "Data."
  - "Data" may also be referred to as "Student Information," "Student Data," "Covered Information," or another similar term.

Data De-Identification

- There is a significant amount of data available to providers of educational services.
  - Metadata on students' interaction with the service or app is often collected and analyzed to help improve the product and enable a provider to create more effective educational services.

Data De-Identification (cont'd)

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

Data De-Identification (cont'd)

- 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.

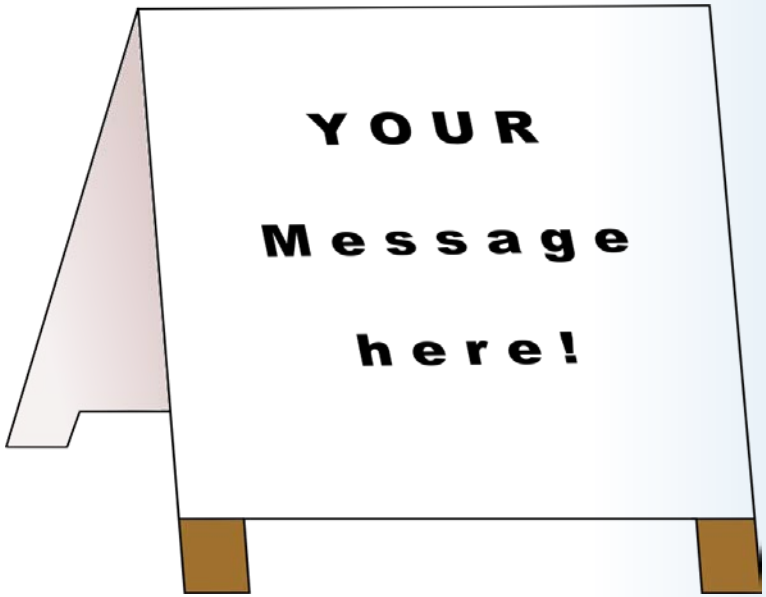
Marketing and Advertising

- 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 Collection

- The amount of data collected by the provider should be limited to only what is necessary to fulfill the obligations of its agreement with the school or district.

- Beware: Providers may view access to their services through a 3rd party social networking site as an exception to established rules limiting data collection.

Data Use

- Just like “data collection”, “data use” by a provider should be limited to the purposes outlined in the agreement with the school or district.
  - Beware of any provision that contains the phrase “without providing notice to users.”

Data Mining

- Providers often perform “data mining” on information they collect to identify patterns in the data, or to infer additional information about their users.
  - Data Mining: the practice of examining large databases in order to generate new information

Data Mining (cont'd)

- Data mining by a provider can be allowed as long as it is performed in accordance with purposes agreed to with the school or district, and used to improve educational services.

- The mining or scanning of student data for targeted advertising directed to students or their parents should be prohibited; if it occurs such activity could lead to a violation of FERPA or PPRA.

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 are 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

Data Transfer and Destruction

- The TOS should retain the school's/district's right to have student data destroyed or transferred to them upon request or upon the expiration of the agreement.
  - Data return or destruction helps limit the amount of personal information available to outside parties and prevents improper disclosure.

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.

Data 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.

Poll: What is your policy for reviewing TOS for your School/District?

A. We have a policy to review agreements for online educational services and applications, and I know what that policy is.

B. We have a policy, but I'm not sure what is involved, or who does the reviewing.

C. I don't know.

D. We do not have a policy for reviewing these agreements.

Security Controls

- Student data need 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.

Read the Guidance Document

https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service

Additional Resources

- For additional information on these topics and best practice recommendations, please visit our websites:
  - Family Policy Compliance Office (FPCO): https://studentprivacy.ed.gov
    - Provides detailed guidance on legal requirements under FERPA and PPRA.
  - Privacy Technical Assistance Center (PTAC): https://studentprivacy.ed.gov
    - Provides guidance documents, trainings, checklists, frequently asked questions, and other resources relating to best practices for data privacy and security.

How Did We Do?

- What did you learn?
- What issues still need clarification?
- What can we do better?
- Please type your questions in the chat box in the lower right corner of the webinar screen.

Questions?

Contact Information

FPCO

Family Policy Compliance Office

Telephone: (202) 260-3887

Email: privacyTA@ed.gov

FAX: (202) 260-9001

Website: https://studentprivacy.ed.gov

Privacy Technical Assistance Center

Telephone: (855) 249-3072

Email: privacyTA@ed.gov

FAX: (855) 249-3073

Website: https://studentprivacy.ed.gov