STUDENT DATA PRIVACY UNDER FERPA IN THE DIGITAL AGE

2019 SCSBA School Law Conference
August 24-25, 2019
David T. Duff (email: dduff@dfl-lawfirm.com)
Duff Freeman Lyon, LLC (tel.: 803-790-0603)

1

1974 – Schools maintained paper student records in file cabinets

Today – Student records are often maintained electronically

2

TODAY

Districts are moving their work, including innovative learning tools, and data they collect and store, to cloud-based platforms

3

TODAY

Cloud-based platforms reduce the need for a server on-site and allow anytime/anywhere access

4

TODAY

Teachers and students are taking advantage of internet and cloud-based learning tools separate from any "official" school district program

5

TODAY

Most cloud computing options are now available not only on district-owned computers, but also on personal employee cell phones. Many school employees have cell phones that contain confidential student information in the form of emails, electronic documents, and sometimes even web access to school databases and programs that contain student information

6

TODAY

Technology companies are creating apps daily that allow teachers/students to collaborate and communicate

7

TODAY

With implementation of curriculum standards and the emphasis on testing to access and improve student achievement and to incentivize learning, school districts are collecting and using student data like never before

8

SO WHAT IS THE PROBLEM?

The loss of privacy and security that accompanies the transfer of personal student information to cloud-based storage

9

STUDENT DATA PRIVACY RISKS -

1) Data breaches
2) Data destruction/recovery
3) Collection and aggregation of personally identifiable data for potential use in advertising and sale to third parties

10

WHAT LAWS GOVERN STUDENTS DATA PRIVACY?

- "**PPRA**" – Protection of Pupil Rights Amendment
- "**COPPA**" – Children's Online Privacy Protection Act
- "**FERPA**" – **What is it???**

11

WHAT IS "FERPA"

FERPA = **F**amily **E**ducation **R**ights & **P**rivacy **A**ct - 1974

12

FERPA

Prohibits school districts from disclosing – except in limited instances – "personally identifiable information" ("PII") contained in students' education records without the consent of the parent or eligible student (18 years or older).

13

Third-party service providers & data privacy – is storing student information in the cloud permitted under FERPA?

What about utilization of computer software, mobile educational apps, and other web-based tools provided by third parties that schools, students and/or their parents access via the Internet and use as part of school activity?

14

EDUCATION RECORD

"Education Record" under FERPA – records, files, documents, and other material that contain "personally identifiable information" ("PII") and which are maintained by the district, e.g., student grade reports, student progress reports, academic or physical testing results, attendance records, discipline records, Special Education records; emails related to the student, videos depicting the student

15

EDUCATION RECORD

In 1974 the term referred to hard-copy recordkeeping practices of the day. Today, we should think in terms of "data" not "records," since so much information is not exchanged or maintained in email, cloud storage, text-messaging, or teachers' phone apps.

16

"PII"

"Personally Identifiable Information" under FERPA – direct identifiers like the student's name and Social Security number, but also indirect identifiers such as the student's date and place of birth and mother's maiden name, e.g., parents'/guardians' addresses and emergency contacts, grades, test scores, courses taken, official correspondence regarding student status or discipline

17

EMAILS

Are not categorically excluded under the FERPA definition of "record" but they must be directly related to a student and maintained by the school to be covered by FERPA

18

VIDEOS

Where a video (or other picture image) of one or more students is taken, the video is "directly related" to and thus the "education record" of the student or students who are the focus of the video (such as two students in an altercation). Therefore, students' parents of students who are the "focus" of the video may view the video since it is their "education records." The video is not the education record of students whose image is incidental or captured as part of the background.

19

PARENT CONSENT RULE/NONDISCLOSURE REQUIREMENT

In general, FERPA requires written parental (or eligible student) consent before a district can disclose PII derived from a student's education records to a third party. But there are a few exceptions to the rule ….

20

EXCEPTIONS TO PARENTAL CONSENT RULE

Two of the FERPA exceptions to parental consent are most useful in allowing school staff to disclose PII in education records to online service providers

1. Directory Information
2. "School Official" Exception

21

DIRECTORY INFORMATION

FERPA permits districts to disclose "directory information" to third parties without obtaining prior written parental consent. Directory information is information that historically has not been harmful if disclosed, such as a student's name or address. Directory information cannot be SS#, race, grades, disability status, standardized test scores, financial information.

22

DIRECTORY INFORMATION (Cont'd)

Directory information must be designated as such by the district and published in a public notice that specifies the types or categories of information that will be disclosed without consent. Since parents can opt out of disclosure of directory information, it is problematic for districts to regularly rely on directory information to transfer student information to third parties like online educational services.

23

"SCHOOL OFFICIALS" EXCEPTION

Districts are not required to obtain consent before disclosing PII from education records to "school officials" within the district who have a legitimate educational interest in the information. "School officials" may include teachers, principals, APs, school psychologists and counselors, support personnel, school attorneys, and school board members.

24

"SCHOOL OFFICIALS" EXCEPTION (Cont'd)

Outside parties may qualify as "school officials," such as a contractor, consultant, volunteer, or other party if the individual or organization -

1) performs an institutional service or function that otherwise would be performed by a district employee,

2) is under the control of the district (such as through a contract or agreement) regarding the use and maintenance of the records), and

3) uses the PII only for purposes for which the disclosure is made and does not redisclose the PII to any other party without parental consent.

25

"SCHOOL OFFICIALS EXCEPTION (CONT'D)

The so-called "school officials" exception allows "outsourcing" and disclosure of education records/PII to cloud service providers if the requirement are met. Online service providers, their apps and services need to be vetted to protect PII and aggregated data; acceptable vendors and their services must be placed under proper service agreements.

26

VETTING THE ONLINE EDUCATIONAL SERVICE PROVIDER

Red Flags - look for language in the terms of service suggesting the vendor may –

- Sell student data
- Advertise to students
- Profile students for advertisements
- Take ownership of student data

27

TERMS OF SERVICE (TOS) AGREEMENTS

FERPA regulates educational entities, not cloud service providers. Assume tech companies do not have a working knowledge of FERPA or other school specific laws. When the "school official" exception is utilized, the provider cannot use FERPA-protected information for any purpose other than that for which it was disclosed.

28

TOS AGREEMENTS (Con't)

Standard terms of agreements used by third-party online educational service providers can lead to violations of FERPA. So-called "click-wrap" agreements with fixed terms often have default terms granting the provider authority to collect, use, and sell data from their users, including students.

29

TOS AGREEMENTS (Con't)

Because third-party service providers accessing PII through the "school officials" exception to FERPA may not redisclose student data without prior written parental consent, districts must ensure that all such providers comply with the confidentiality provisions of FERPA. Therefore, the procurement process of obtaining third-party digital tools and services requires districts and vendors to negotiate specific contractual terms in a written agreement.

30

TOS AGREEMENTS (Con't)

Sample "Data Privacy" clause : "As required by FERPA, Provider will use District Data only for the purpose of fulfilling its duties and providing services un this Agreement. SEE ATTACHMENT A [DESCRIBING THE TERMS OF MORE EXPANSIVE USE/SHARING]."

31

TOS AGREEMENTS (Con't)

Sample "Data Transfer Upon Termination or Expiration clause": "Upon termination or expiration of this Agreement, Provider will ensure that all District Data, in its possession, or in the possession of any subcontractor or agents to which Provider might have transferred District Data, is rendered unusable, as directed by District."

32

DATA BREACHES – DETECTING, MONITORING, AND RESPONDING

School and districts are not immune from computer viruses, server hacks, ransomware, phishing, and other cyber-related incidents; in fact they often are easy targets, or their educational online providers are.

Policies and procedures need to be in place addressing cybersecurity and physical threats; monitoring and reporting data security breaches; and responding to data breaches.

33

DATA DECONSTRUCTION AND RECOVERY

A data breach can occur if recovery tools can be used to extract improperly erased or overwritten data or discarded electronic devices. Vendors will say they want to "anonymize" data, but the chances of re-identifying someone based on bits of information is getting easier. Agreements must require appropriate data deletion methods to ensure the data cannot be recovered.

34

BEST PRACTICES AND DISTRICT POLICY FOR CLOUD COMPUTING

1) Adopt a comprehensive approach to safeguarding and protecting student privacy regarding the use of cloud-based learning tools and services

2) Conduct an audit of all online educational services and digital tools

35

BEST PRACTICES AND DISTRICT POLICY FOR CLOUD COMPUTING (Con't)

3) Establish policies and procedures for evaluation and approval of internet/cloud-based educational services to be used by teachers and staff, including policies/procedures for purchasing and using hardware, software, and online educational tools

36

BEST PRACTICES AND DISTRICT POLICY FOR CLOUD COMPUTING (Con't)

4) Train staff and educate students and parents regarding district policies on release, use, and access to student data for internet-based educational services

5) Consider creating a district-level Chief Privacy Officer

37

RESOURCES

PTAC - The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student data and student-level longitudinal data systems. PTAC information and assistance is available at jttp://studentprivacy.ed.gov.

38

MORE RESOURCES

- "50 Years of School Technology: Lessons Learned from the Past and Legally Defensible Practices of the Future " (available thru NSBA/COSA)
- Cybersecurity and Student Privacy: Best
- Practices and Solutions for FERPA Compliance
- (available thru NSBA/COSA)

39

MORE RESOURCES

- "DATA IN THE CLOUDS: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era" (available thru NSBA/COSA)
- "Data Privacy Law Update: Ten Things to Advise Your School Board Clients – Before It's Too Late" (available thru NSBA/COSA)

40