FERPA Considerations:
Data Retention & Destruction

2019 NCES Summer Forum

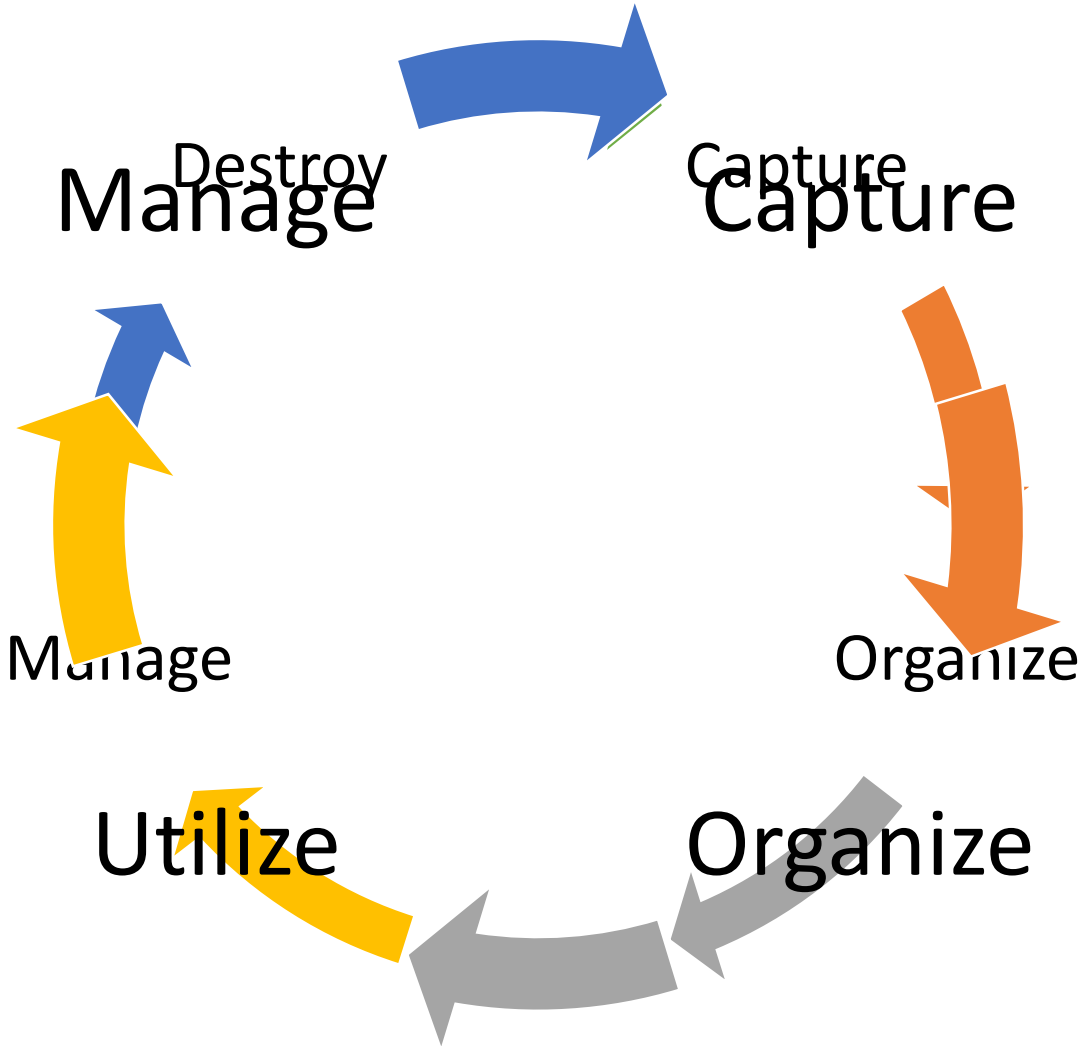
July 23, 2019

Mike Tassey & Eric Gray
Privacy Technical Assistance Center (PTAC)

Your Mileage May Vary!

- 50 Different takes on data retention / destruction
- *Each State*:
  - *Different data classification / sensitivity*
  - *Different storage methods*
  - *Different length of retention*
  - *Different reporting requirements*
  - *Different approved methods of destruction*

Data Life Cycle



What Does FERPA Say about Record Retention?

(This Slide Intentionally Left Blank)

Requirements for the inspection and review of education records

What rights exist for a parent or eligible student to inspect and review education records?

- School must comply with request within 45 days.
- Schools are generally required to give copies only if failure to do so would effectively deny access, or make other arrangements to inspect and review – example would be a parent or student who does not live within commuting distance.
- **School may not destroy records if request for access is pending.**

"Reasonable" Record Retention – Steps to Creating a Policy

- Check your State Laws!
- How long do you need to keep certain records?
- Storage methodology – physical vs. electronic
- Do a risk analysis!
- Align with destruction methodology, keep what you need to keep, destroy what you don't. (Remember FERPA'S right to access!)
- Consider ALL of the applicable laws both Federal and State that apply to records retention and data destruction

What if the Law Doesn't Apply to Education?

Do a **data inventory**

- *Where does it live*
- *Who owns it*
- *How sensitive is it?*

Match **data** with **business need**

- *Why do we have this*

Convene **stakeholders** to **determine** retention **needs**

- *How long do we need to keep this*

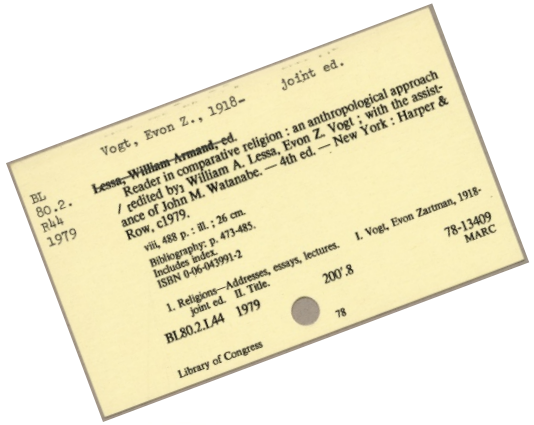
Data Destruction

What are we talking about?

- *Not simply hitting "delete"*
- *Secure destruction so that it can't be recovered*
- *Especially applicable to third-parties*
- *Not just Federal, but also State law*

Why Deletion Isn't Destruction

- Think of your hard drive like a library!
- Libraries have books (data)
- They also have Card Catalogs



Why Deletion Isn't Destruction

- The books are stored in an ordered structure
- The Catalog cards just tell you where to find the data
- What happens when the library gets rid of a book like your hard drive deletes files?

Why Deletion Isn't Destruction

- They would simply tear up the catalog card for the book they are getting rid of
- They wouldn't bother removing and throwing away the book from the shelf!
- This is why deletion is not sufficient to destroy data… the book (file data) is still there

Methods of Destruction

- **Clearing** – Removing data by software methods like overwriting the data or "formatting" the entire partition or disk
- **Purging** – Removing the data through physical or logical means such as applying strong magnetic fields to reduce the magnetic signature used to store data on disk
- **Destroying** – Removing the data by rendering the medium it is stored within unusable, typically through pulverizing, incinerating or shredding

Cloud Data Destruction Considerations

- Shared resources may limit destruction possibilities
- Distributed architecture means your data may not exist in the same place
- What assurances do you have that data is destroyed

Work with your vendors to address the FERPA requirements! Craft written agreements that address the tail end so there are no surprises!

Deletion by Encryption

- Option of last resort
- Can be useful to increase assurance in distributed, shared, or complicated environments where removal or destruction is not an option
- Does not destroy the data, just obfuscates it
- Predicated on the strength of the algorithm chosen

Where Do We Go Wrong

- Emails contain huge amounts of untracked data
- Our backups contain copies of our data
- Employee personal computer hard drives, network drives
- Shadow IT (Google Drive, DropBox, etc)

FERPA & Data Destruction

FERPA requires educational institutions to protect Personally Identifiable Information (PII) from student records from unauthorized disclosure without consent.

- *You must have written consent from the Parent (or guardian) or the eligible student or;*
- *The data must be disclosed under one of the exceptions to FERPA*

FERPA & Data Destruction

But wait, FERPA doesn't say I have to destroy any records?

- *What about contracted parties?*
- *When the study is over?*
- *If you switch cloud service providers?*
- *Stop using an app?*

The Studies Exception

The disclosure of PII from student education records must be for, or on behalf of, an educational agency or institution, in order to:

a) *Develop, validate, or administer predictive tests;*

b) *Administer student aid programs; or*

c) *Improve instruction*

Information disclosed under this exception MUST be destroyed when no longer needed for the study purposes!

The disclosing entity MUST also enter into a written agreement with the organization performing the study

The Studies Exception

Written agreements under the studies exception must:

1. Specify the purpose, scope, and duration of the study and the information to be disclosed.
2. Require the organization to use PII from education records only to meet the purpose or purposes of the study as stated in the written agreement.
3. Require the organization to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests.
4. Require the organization to destroy all PII from education records when the information is no longer needed for the purposes for which the study was conducted, and specify the time period in which the information must be destroyed.

Audit or Evaluation Exception

The disclosure of PII from education records must be to:

a) Audit or evaluate a Federal- or State-supported education program; or

b) Enforce or comply with Federal legal requirements related to the program.

Audit or Evaluation Exception

a) Must enter into a written agreement to designate anyone other than its employee as its authorized representative; and

b) Is responsible for using reasonable methods to ensure to the greatest extent practicable that the authorized representative
   i. Uses the PII only for the authorized purpose;
   ii. Protects the PII from further unauthorized disclosures or other uses; and
   iii. Destroys the PII when no longer needed for the authorized purpose and in accordance with any specified time period set forth in a written agreement.

Written Agreement Best Practices

- Bind individuals to the agreement
- Specify Points of Contact / Data Custodians
- Set terms for data destruction
- Maintain the right to audit
- Have plans to handle a data breach

Take Home Points

- "Delete" is not destroyed
- Securely destroy data you no longer need
- Data destruction is a key element in contracting for services that process FERPA data
- When considering cloud services, think about how you can ensure that your data does not remain
- Consider ALL of the applicable laws both Federal and State that apply to records retention and data destruction

Resources

- Data Destruction Best Practices
- FERPA Exceptions Summary
- Guidance for Reasonable Methods and Written Agreements
- Cloud Computing FAQ

All these resources and more can be found at the PTAC website:
https://studentprivacy.ed.gov

Questions?

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

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

privacyTA@ed.gov

http://studentprivacy.ed.gov

(855) 249-3073