Student Privacy vs. Student Retention Data

Jeffrey Alan Johnson
Higher Education Privacy Officer

February 5, 2025

UTAH SYSTEM OF HIGHER EDUCATION

UVU DATA SUMMIT

The Obligatory Disclaimer

This presentation provides technical assistance and discusses sound practices for broadly protecting the privacy of student data as a matter of doing right by our students. While informed by FERPA and other laws that define the core principles of student data privacy in the United States, please direct questions about specific compliance requirements to your institution's legal counsel.

Overview

What is privacy?

How is student data protected?

How can we use protected data for retention research?

WHAT IS DATA PRIVACY?

A traditional definition of data privacy

"Data privacy is a discipline intended to keep data safe against improper access, theft or loss."

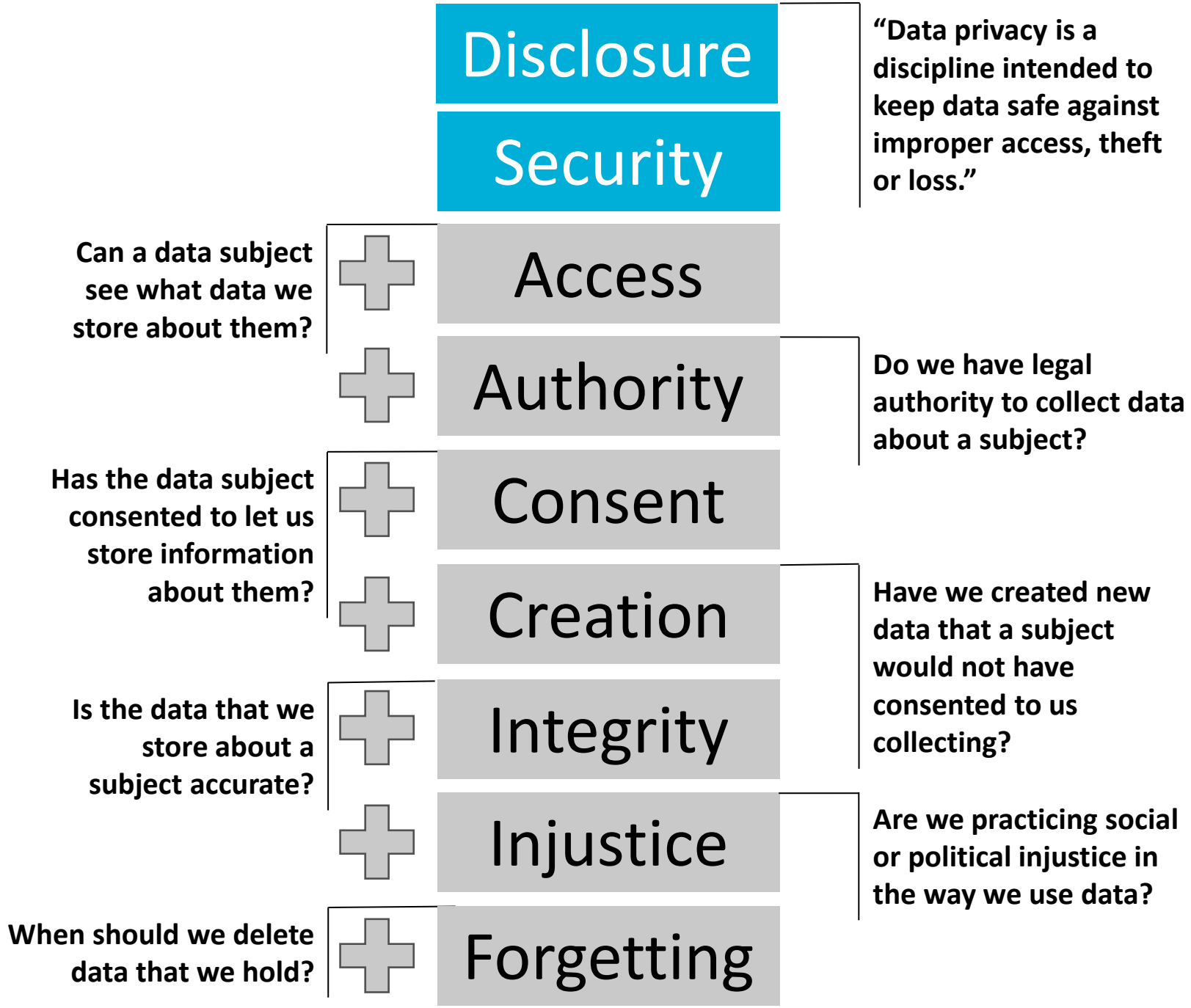
Disclosure

Security

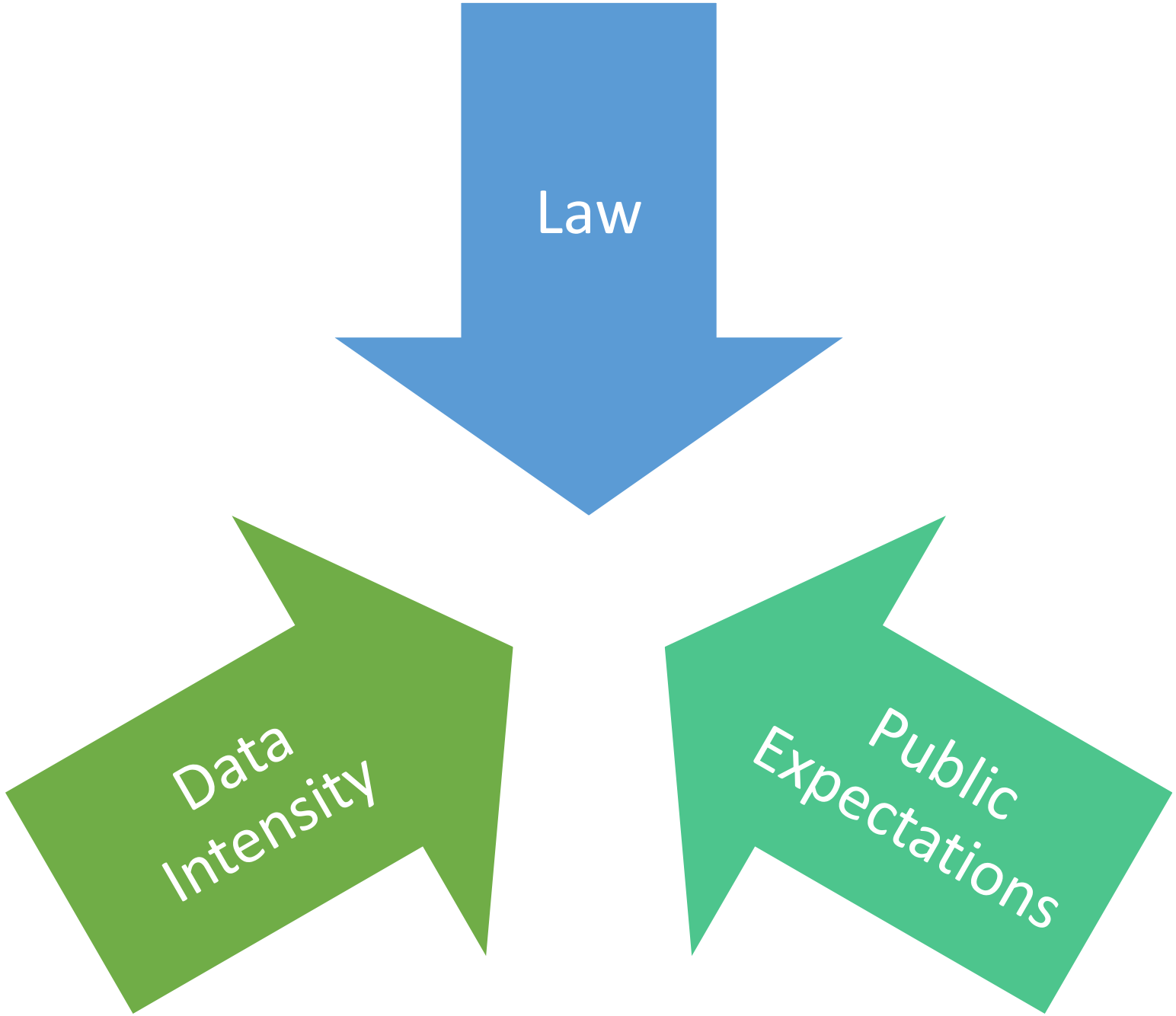
Access

Expanding the scope of data privacy

A sphere of information about one's self to which no one else has a right except by one's consent.



Why Privacy Matters



Privacy by Design/ Privacy by Default

Proactively building data collection and processing technologies with privacy as a design principle.

Discussion: What privacy questions are associated with student retention data?

Disclosure, Security, and Access

Personal Control

WHAT STUDENT DATA IS PROTECTED?

FERPA: Meaningful Access, Meaningful Disclosure Limitations

Someone who maintains education records may disclose personally identifiable information from those records to someone else only with student consent or as permitted under a FERPA-allowed exception to consent.

FERPA's Definition of Protected Data:

Personally identifiable information from the educational records of a student

FERPA's Definition of Protected Data:

Personally identifiable information from the educational records of **a student**

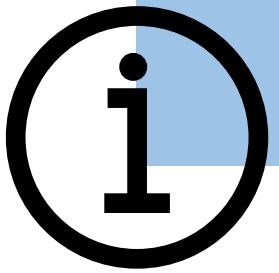
Any individual who is or has been in attendance at an institution.

FERPA's Definition of Protected Data:

Personally identifiable information from the **educational records** of a student

Any information recorded in any way that is:

- Directly related to a student
- Maintained by the institution.



Some exclusions apply. See privacy support staff for details.

FERPA's Definition of Protected Data:

Personally identifiable information from the **educational records** of a student

Information collected on or derived from the FAFSA or ISIR can be used only for financial aid administration.

FERPA's Definition of Protected Data:

Personally identifiable information from the educational records of a student

Direct identifiers such as:

- Student or family member name or address
- Personal identifying numbers (SSN or Student ID)

FERPA's Definition of Protected Data:

Personally identifiable information from the educational records of a student

87% of Americans can be uniquely identified by gender, date of birth, and zip code.

FERPA's Definition of Protected Data:

Personally identifiable information from the educational records of a student

Indirect identifiers that can be combined to identify students:

- Date of Birth
- Place of Birth
- Mother's Maiden Name

FERPA's Definition of Protected Data:

Personally identifiable information from the educational records of a student

Information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person to identify the student with reasonable certainty.

Discussion: When are club membership records protected data?

Personally Identifiable Information	**Education Records**	**Of Students**

DISCLOSURE TO SCHOOL OFFICIALS

FERPA: Meaningful Access, Meaningful Disclosure Limitations

Someone who maintains education records may disclose personally identifiable information from those records to someone else only with student consent or as permitted under a **FERPA-allowed exception to consent.**

Permitted Disclosure under the School Officials Exception

PII from education records may be disclosed to a school official with a legitimate educational interest in the record.

Permitted Disclosure under the School Officials Exception

Generally, “legitimate educational interest” means an official needs access to the record to do their job.

Permitted Disclosure under the School Officials Exception

Disclose only what is necessary and appropriate to the receiving official's legitimate educational interest.

Protecting School Official Disclosures: Data Minimization

Data minimization reduces the scope or granularity of data collected or disclosed.

- Data Subjects
- Data Fields
- Level of Detail

Protecting School Official Disclosures: Secure Disclosure

Transmit data using systems that only allow intended recipients to access PII.

Avoid Transmitting PII

Aggregate Before Sending

Require Receiver Authentication

Protecting School Official Disclosures: Secure Disclosure

Email is not a secure method of disclosure.

- Vulnerability to Hacking
- Risk of Misdirection
- Lack on Ongoing Control

Protecting School Official Disclosures: Data Tools

Easy Solution: Use the Right Data Tool

- Aggregate Reporting
- Individual Transactions
- Data Processing

DISCLOSURE OF DE-IDENTIFIED DATA

Permitted Disclosure of De-identified Data

PII from education records can be disclosed if students are not identifiable through the disclosure.

Limited Disclosure: De-identified Data

De-identification discloses data that cannot be used to personally identify students.

- Aggregation
- Anonymization
- Pseudonymization

Limited Disclosure: De-identified Data

Data has not been de-identified if a student's identity can be inferred from the data and other reasonably available information.

Limited Disclosure: De-identified Data

Secondary disclosure avoidance ensures that data does not contain PII.

- Small Cell Suppression
- Blurring Level of Detail
- Top or Bottom Coding

Discussion: How should your office share or use retention data?

Legitimate Educational Interests

De-Identified Data

Data Minimization

Secure Transfer and Use

For Further Information

Questions?

Jeffrey Alan Johnson, Ph.D.
Higher Education Privacy Officer
Utah System of Higher Education

jeffrey.johnson@ushe.edu