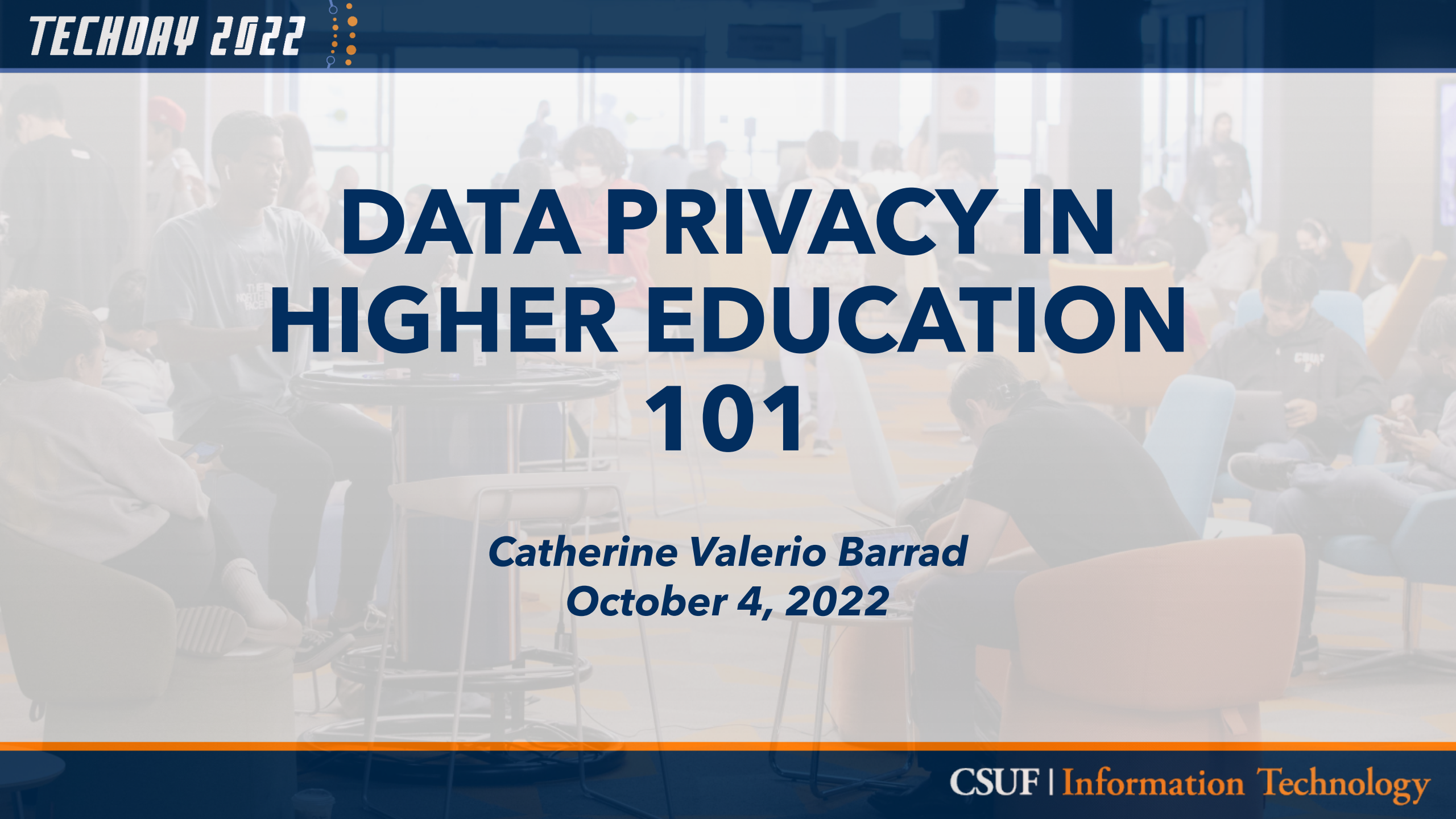

DATA PRIVACY IN HIGHER EDUCATION 101

Catherine Valerio Barrad

October 4, 2022

OVERVIEW

- Data Privacy Principles
- Data Privacy in the Higher Education Setting
  - What data is protected?
  - What laws apply?
- Why Should We Care About Data Privacy in Higher Education?
  - Why universities are vulnerable
  - What you can do to help secure your data and keep other data secure

BASIC OVERVIEW OF DATA PRIVACY

- **Data privacy** refers to the protection of sensitive information about individuals that is collected, processed, stored or transferred by an entity
- **Sensitive information about individuals** includes personal, financial, health and other data
  - **“Personally identifiable information” or PII**
  - **“Personal health information” or PHI**

EXAMPLE: CALIFORNIA'S DEFINITION:

"any information that … identifies or describes an individual"

- Name
- SSN
- Home address
- Email address
- Phone numbers
- Physical description
- Education
- Birthdate
- Financial matters
- Medical history
- Employment history
- Race/ethnicity
- Sexual orientation and identity
- Statements made by or attributed to an individual

Civ. Code §1798.3(a)

DATA PRIVACY PRINCIPLES [FIPPs]

- Data will not be collected absent a specific purpose
- Data will be accurate, and kept only as long as is necessary for the purpose for which it was collected
- Individuals will be told what data is collected and how it will be used
- Data will not be shared with others without permission and only as necessary to fulfill the purpose for which it was collected
- Data will be secured against unauthorized access

PRIVACY LAWS APPLICABLE TO HIGHER ED

- The Privacy Act (5 USC § 552)
  - Regulates the collection, use and disclosure of personal data by federal agencies (such as Department of Education)
- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
  - Regulates the privacy of student educational records
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and *Standards for Privacy of Individually Identifiable Health Information (Privacy Rule)* (45 CFR Parts 160, 164)
  - Regulates the privacy of protected health information *excluding records covered under FERPA*

PRIVACY LAWS APPLICABLE TO HIGHER ED

- Gramm-Leach-Bliley Act (GLBA)
  - Applies to how higher education institutions collect, store and use student financial records containing personally identifiable information
- Fair and Accurate Credit Transitions Act of 2003 (FACTA) Red Flags Rule
  - Detection, prevention and mitigation of identity theft in connection with accounts (such as financial aid, student accounts, stored value cards, etc.)
- The Information Practices Act (Cal. Civ. Code §1798 *et seq.*)
  - Regulates collection, use and disclosure of personal data by California state agencies; also addresses data breach notification requirements

ADDITIONAL PRIVACY REGULATION

- Title V, California Code of Regulations § 42396 *et seq.* – setting out principles of privacy and personal information management principles applicable to the CSU
- Education Code § 89546 – regulating access by employee to certain records and employee's right to request correction
- Govt Code § 6250 *et seq.* – making certain information a matter of public record
- Other State Data Breach Notification Laws
- Government Contracts
- International Data Privacy Laws
  - Regulating movement of personal data across national borders

WHY PROTECT DATA?

- Sharing data is necessary to complete everyday tasks and to engage with other people in society
- Personal data can be exploited to harm individuals
- The proliferation of data, particularly in the online environment, means that individuals have less control over their personal information
- Protection of personal data is designed to minimize that opportunity for exploitation

WHY UNIVERSITIES ARE TARGETED

- Universities store sensitive student and personnel records, financial records and valuable intellectual property from cutting-edge research
- Much of the work, especially academic research, relies on collaboration and the free flow of information both *inside* and *outside* the institution, including the use of shared online resources
- The combination of large quantities of data assets (intellectual property and sensitive data) and a decentralized, collaborative culture make higher education institutions a gold mine for hackers

EXAMPLE: Lincoln College (IL) – March 2022

- December 2021: Lincoln College hit with ransomware attack that shut down critical systems and made it impossible to access computer systems and data
- The hackers demanded $100,000 to restore the systems
- The college could not afford to replace and rebuild their systems, so paid a ransom
- March 2022: Hackers restored access to systems
- May 2022: Already hit hard by declining enrollment during the pandemic, Lincoln College closed down

EXAMPLE: Australian Catholic University

- Threat actors posing as the university sent an email to staff and faculty containing a link to a fake ACU page
- A number of staff and faculty clicked on the link and did not realize the landing page was not authentic
- When staff entered their credentials into the fake page, the threat actors harvested their logins and passwords
- The threat actors then used the credentials to gain access to email and sensitive information (including bank accounts)

BEST PRACTICES -- INSTITUTION

- Strong, unique passwords that you do not share, with multi-factor authentication
- Secure transfer of sensitive information
- Use data only for the purpose for which you have access to it
- Use only encrypted external devices and only ones you trust
- Verify before you trust
  - Email that looks legitimate may be spoofing a trusted vendor or source – check the actual email address to verify
  - If a request seems odd (here's our new bank account information!), it probably is, so check with the person via phone or a new email using the known email address to verify
- Report suspicious activity
- Remote work and international travel may require additional security measures (e.g., VPNs)

BEST PRACTICES -- PERSONAL

- Limit personal information you share online
  - Change privacy settings, including turning off location features
- Strong, unique passwords that you do not share, with MFA
  - Long passwords, upper/lower case, numbers, special characters
  - Try a password manager
- Verify before you trust: when in doubt, DO NOT CLICK
  - Watch for suspicious activity that asks you to do something right away or needs personal information
- Use technology: secure sites, VPNs, antivirus software, firewalls, backups
- Report suspicious activity

Strong Passwords

- Choose a word and a number you can remember

Alifan 07/01/63

Strong Passwords

- Choose a word and a number you can remember
- Intersperse the letters and numbers

Alifan 07/01/63

A 0 l 7 i 0 f 1 a 6 n 3

Strong Passwords

- Choose a word and a number you can remember
- Intersperse the letters and numbers
- Convert some letters and/or numbers to symbols

A 0 l 7 i 0 f 1 a 6 n 3

A 0 ! 7 i 0 f 1 @ 6 n 3

Strong Passwords

- Choose a word and a number you can remember
- Intersperse the letters and numbers
- Convert some letters and/or numbers to symbols

A0!7i0f1@6n3

Thank you for coming!