EWA
Higher Education Analytics Seminar

Brenda Leong
Senior Counsel and Director of Operations,
Future of Privacy Forum

Future of Privacy Forum

- The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.
- The forum is led by Internet privacy experts and is supported by over 100 leading companies. It includes an Advisory Board comprised of leading figures from industry, academia, law and advocacy groups.
- FPF covers consumer privacy issues across topics such as Location, Beacons, Big Data, Mobile/Apps, Connected Cars, De-Identification, Smart Places, and Education (Student) Data Privacy.

Fair Information Practice Principles (FIPPs)

- **Transparency:** Organizations should notify individuals regarding collection, use, dissemination, and maintenance PII
- **Access:** Provide mechanisms for appropriate access, correction, and redress regarding data.
- **Purpose Specification**: Specifically articulate the purpose or purposes for which data is intended to be used.
- **Data Minimization**: Only collect data that is necessary to accomplish the specified purpose(s) and only retain for as long as is necessary to fulfill the specified purpose(s).

Fair Information Practice Principles (FIPPs)

- **Use Limitation:** Use data solely for the purpose(s) specified in the notice or for a purpose compatible with the original notice.
- **Data Quality:** Ensure that data is accurate, relevant, timely, and complete.
- **Security:** Protect data through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, by procedural, technical and physical means.
- **Accountability**: Stated commitment for complying with these principles, providing training to all employees and contractors who use data, and auditing the actual use of data to demonstrate compliance

What Does FERPA Protect?

- "Educational Records" – Records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the educational agency or institution
- "Personal Information" – direct identifiers (such as a student's or family member's name) and indirect identifiers (such as date of birth, mother's maiden name)
  - Exceptions:
    - De-identified Data – De-identified data is data which has been stripped of all direct identifiers as well as indirect identifiers that may in combination identify a particular individual, may be shared with third parties without consent
    - Metadata – Metadata is contextual or transactional data (ex. data about how long a student took for a particular activity, when the activity was completed, etc.) that has been stripped of all direct and indirect identifiers is not covered by FERPA
    - (These data points *could* still be Personal Information if a reasonable person in the community could identify the individual student with this data in combination with readily available public information).

Privacy Perspective

We're talking about universities strategically collecting, analyzing, and using data for beneficial outcomes

KEY TAKEAWAY – What happens when the interests, motivation, and benefits for universities and students may not align?

“Ecosystem” of Education – P20+

- Proposals include description of data collection on K-12 -> Higher Ed -> State Labor Workforce -> Interstate Exchanges -> Federal Agencies
- PII and Student Records – linking data-sets – creating new information
- Universities have:
  - On-line, device ID, Location, Food, Health, Reading, study, academics, Friends, Shopping, Religion, Off-campus activities (student ID discounts)
- Third party vendor partners

Benefits

- 19 Times paper – “data for good”
- Interventions – low-income and minority students
  - Missing same support structures
- Improved matches of students to schools; improved retention and graduation rates; improved student satisfaction
- More equitable treatment, programs, and outcomes

Areas of Concern – macro
"Fields of gold"

- Algorithms – transparency, trust, and bias
  - "Analytics becomes the prerequisite to taking action"
  - "See where the data leads us"
- Behavioral tracking – data brokers – targeting
  - Correlation v. causation
  - How long is micro-data retained?
  - Employer access
- Law Enforcement access
- Security; Information Leakage

De-Identification

- A spectrum, not an on/off switch
- Volume, sensitivity, access, and controls
- Reidentification Risks – linked datasets and levels of protection
  - Birthday/gender/zip code is unique for up to 87% of US residents
- Consolidation at department, major, or program level
- Upwardly combined across institutions, intra- and inter- state

Areas of Concern – micro

"Over Parenting" or "Intrusive advising"

- Professor bias – do interventions have unintended effects
- Visiting HS Senior – web search over lunch; following interview addresses perceived interests or concerns
  - Early, and appropriate, targeting
- Treating potential or current students differently based on data they may not even know you have/Price profiling
- Agency – informed choice v. directed action for students

Strategies

- Transparency – Notice – Opt-in – Opt-out – Accountability
  - Volume, sensitivity, access, and control
  - Disclose predictive analytics policies and practices
- Trusted third parties/ratings – BBB, Consumer Reports
  - Credit scores
- Staff Training, Resources, Data Literacy
- Best Practices, Industry Standards – Contracting

Final Thoughts

- Expectations – different for all stakeholders
  - Spectrum of sophistication for both institutions and students
- Research – data scientists – increasing specialization/ability
  - Social goods
- Surveillance culture
- *How is an individual student's life or circumstance improved?*

Future of Privacy Forum

Brenda Leong
bleong@fpf.org
@BrendaKLeong
@futureofprivacy
@ferpasherpa
www.fpf.org
www.ferpasherpa.org