Higher Education Privacy Bootcamp

10/31/2017
Today’s (Rough) Agenda

▶ 8:00 – 8:15am: Welcome and Introductions
▶ 8:15 – 9:00am: Michael Hawes, U.S. Department of Education
▶ 9:00 – 9:30am: Case Study
▶ 9:30 – 10:00am: Break
▶ 10:00 – 10:30am: Amelia Vance, Future of Privacy Forum
▶ 10:30 – 11:00am: Rachel Rudnick, University of Connecticut
▶ 11:00 – 11:30am: Case Study
What is your top privacy concern?
Types of Risk

- An actual security or privacy risk
- Risk of not being in compliance
- Perception risk

Credit: Jim Siegl, Fairfax County Public Schools, Virginia
Today’s (Rough) Agenda

- 8:00 – 8:15am: Welcome and Introductions
- 8:15 – 9:00am: Michael Hawes, U.S. Department of Education
- 9:00 – 9:30am: Case Study
- 9:30 – 10:00am: Break
- 10:00 – 10:30am: Amelia Vance, Future of Privacy Forum
- 10:30 – 11:00am: Rachel Rudnick, University of Connecticut
- 11:00 – 11:30am: Case Study
Protecting Student Privacy

Higher Education Privacy Laws and Security Issues

Higher Education Privacy Bootcamp
EDUCAUSE
October 31, 2017

MICHAEL HAWES
Director of Student Privacy Policy
Office of the Chief Privacy Officer
U.S. Department of Education

United States Department of Education
Privacy Technical Assistance Center
Presentation Overview

- ED’s role in protecting student privacy
- FERPA 101
- Recent guidance from ED
- Current privacy and security issues in Higher Ed
- Questions
The U.S. Department of Education’s Role in Protecting Student Privacy

• Administering and enforcing federal laws governing the privacy of student information
  • Family Educational Rights and Privacy Act (FERPA)

• Raising awareness of privacy challenges

• Providing technical assistance to schools, districts, and states

• Promoting privacy & security best practices
What is Privacy?
Privacy

• “the state of being free from intrusion or disturbance in one's private life or affairs” (Random House)

• Many components of privacy:
  - Information Privacy
  - Bodily Privacy
  - Territorial Privacy
  - Communications Privacy
Privacy Principles:

- Authority and Purpose
- Accountability
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation

NIST Special Publication 800-53, Appendix J
www.nist.gov
IT Security:

• “Measures and controls that protect an [information system] against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of [information systems] and data.” (Vacca, ed. 2009, Computer and Information Security Handbook)

• Focused on protecting the:
  • Confidentiality;
  • Integrity; and
  • Availability of information systems
• Confidentiality
• Integrity
• Accountability, Audit, & Risk Management

• Use Limitation
• Data Minimization & Retention
• Transparency

• Individual Participation & Redress
• Authority & Purpose
• Data Quality

Privacy

IT Security

• Availability
Family Educational Rights and Privacy Act (FERPA)

- Applies to all institutions receiving Federal funds under any program administered by the Secretary of Education
- Gives eligible students the right to access and seek to amend their education records
- Protects personally identifiable information (PII) from education records from unauthorized disclosure
- Requires written consent before sharing PII – unless an exception applies
**FERPA Definitions**

**Personally Identifiable Information** (PII) is information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

**Education Records** are any records directly related to the student that are maintained by, or on behalf of, an educational agency or institution.
Directory Information Exception

• Students don’t attend school anonymously.
• Allows schools to release certain information without consent. A few examples:
  • name, address, telephone listing, electronic mail address;
  • date and place of birth;
  • photographs;
  • weight and height of athletes;
  • degrees & awards received, etc.
Directory Information Exception

• Schools/Districts must designate the data elements they consider to be Directory Information.

• Common uses:
  • Yearbooks
  • Concert programs
  • Telephone directories

Students have a right to opt-out of disclosures under the Directory Information exception!
School Official Exception

Schools or LEAs can use the School Official exception to disclose education records without consent to a third party if the third party:

• Performs a service/function for the school/district for which it would otherwise use its own employees
• Is under the direct control of the school/district with regard to the use/maintenance of the education records
• Uses education data in a manner consistent with the definition of the “school official with a legitimate educational interest,” specified in the school/LEA’s annual notification of rights under FERPA
• Does not re-disclose or use education data for unauthorized purposes
Health or Safety Emergencies Exception

• Disclosure is necessary to protect the health or safety of the student or others.

• There is an articulable and significant threat to the health or safety of a student or other individuals.

• Appropriate parties typically means local, State, or federal law enforcement, trained medical personnel, public health officials, and parents.

• Must be related to an actual, impending, or imminent emergency.

• School makes determination on case-by-case basis.
Parents of Dependent Students

A school may choose to disclose, without the students consent, a student’s education record to that student’s parent if the student is a dependent for IRS tax purposes.
Judicial Orders & Subpoenas Exception

- School may disclose PII from education records necessary to comply with a judicial order or lawfully issued subpoena.
- School must make a reasonable effort to notify the eligible student of the order or subpoena before complying with it in order to allow the eligible student opportunity to seek protective action.
- Some judicial orders and subpoenas are exempt from FERPA’s notification requirement.
FERPA: Financial Aid Exception

Education records may be disclosed in connection with financial aid for which the student has applied or which the student has received, if the information is necessary for such purposes as to:

a) Determine eligibility for the aid;
b) Determine the amount of the aid;
c) Determine the conditions for the aid;
d) Enforce the terms and conditions of the aid
Studies Exception

Allows disclosure of PII from education records for studies that are “for or on behalf of” schools, school districts, or postsecondary institutions, if:

• The studies are for the purpose of
  • Developing, validating, or administering predictive tests; or
  • Administering student aid programs; or
  • Improving instruction; and

• There is a written agreement with the individual/organization performing the study that meets certain requirements.
Written Agreements—Studies Exception

• Written agreements **must**
  • Specify the purpose, scope, and duration of the study and the information to be disclosed, and
  • Require the organization to
    • use PII only to meet the purpose(s) of the study
    • limit access to PII to those with legitimate interests
    • destroy PII upon completion of the study and specify the time period in which the information must be destroyed
Data Governance, Online Services, and Predictive Analytics

• Increase in data silos at IHEs and the importance of Data Governance

• Guidance on Protecting Student Privacy while Using Online Educational Services (2014) and Model Terms of Service (2015)

• Be mindful of privacy and ethics when using predictive analytics in higher education
WIOA Guidance

Joint Guidance on Data Matching to Facilitate WIOA Performance Reporting and Evaluation

• Jointly issued by U.S. Departments of Education and Labor (August 2016)
• Provides information to assist State agencies, educational institutions, and service providers in performance reporting and evaluation requirements under the Workforce Innovation and Opportunity Act (WIOA)
Student Medical Records

Dear Colleague Letter on
Protecting Student Medical Records

• Issued by the Department’s Chief Privacy Officer (August 2016)
• Outlines legal protections relating to student medical records in the context of litigation between the institution and the student.
HIPAA
Guidance on FERPA and Reverse Transfer

FERPA and Reverse Transfer (SUNY Letter)

• Issued by the Family Policy Compliance Office (January 2016)
• Details various methods for disclosing student transcript information to promote Reverse Transfer and the awarding of Associate’s Degrees to students who have transferred to four-year institutions.
Integrated Data Systems

Integrated Data Systems and Student Privacy (2017)

• Provides an overview of the legal issues relating to participation in an integrated data system.
• Provides best practice recommendations for improving data governance and transparency in IDS.
Using Financial Aid Information for Research and Evaluation


• Explains the overlapping laws that protect student financial aid information.
• Answers questions on how financial aid information may be used for program evaluation and research purposes.
Data Breaches in Education

Source: Identity Theft Resource Center
Top Causes and Vulnerabilities

1. Phishing / Malware
2. Hacking / Intrusion
3. Lost or Stolen Hardware (Poor Storage)
4. Mistakes – errant emails, attachments, etc.
5. Third Party Vendors / Service Providers
## Post-secondary Data Breaches

<table>
<thead>
<tr>
<th>School</th>
<th>Method</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Berkeley</td>
<td>Hackers breached an unpatched security flaw in the Berkeley Financial System</td>
<td>80,000</td>
</tr>
<tr>
<td>North Carolina State University</td>
<td>Phishing scam resulted in access to university email account containing PII</td>
<td>38,000</td>
</tr>
<tr>
<td>Rockhurst University</td>
<td>Phishing scam resulted in the theft of employee IRS W-2 forms</td>
<td>13,000</td>
</tr>
<tr>
<td>University of Calgary</td>
<td>Ransomware attack on university email server</td>
<td>All university staff. UC payed the hackers $15,000 to unlock their servers</td>
</tr>
</tbody>
</table>

*Average cost to institutions per record across all sectors - $154.00*
“Instances of data breaches...continue to proliferate and reinforce the need for focused action...”

FSA requires institutions to comply with the Gramm-Leach-Bliley Act.

Institutions of higher education are required to ensure the security and confidentiality of customer records and information.
• Under GLBA, postsecondary institutions must:
  • Develop, implement, and maintain a written information security program;
  • Designate the employee(s) responsible for coordinating the information security program;
  • Identify and assess risks to customer information;
  • Design and implement an information safeguards program;
  • Select appropriate service providers that are capable of maintaining appropriate safeguards; and
  • Periodically evaluate and update their security program.

• The Department is incorporating the GLBA security controls into the Annual Audit Guide, and will require the examination of evidence of GLBA compliance as part of institutions’ annual student aid compliance audit.
Looking Ahead
PTAC Service Offerings

http://studentprivacy.ed.gov/

- Help Desk ([privacyTA@ed.gov](mailto:privacyTA@ed.gov))
- Training (CBT, webinar, or onsite)
  - FERPA 101
  - Data Sharing under FERPA
  - Data Security Best Practices
- Data Governance, Policy, and Architecture Reviews (online or onsite)
  - Data Governance
  - Data Security Architecture
  - Breach Response Preparation
- Data Sharing MOU Assistance

United States Department of Education
Privacy Technical Assistance Center
Questions?
Today’s (Rough) Agenda

▶ 8:00 – 8:15am: Welcome and Introductions
▶ 8:15 – 9:00am: Michael Hawes, U.S. Department of Education
▶ 9:00 – 9:30am: Case Study
▶ 9:30 – 10:00am: Break
▶ 10:00 – 10:30am: Amelia Vance, Future of Privacy Forum
▶ 10:30 – 11:00am: Rachel Rudnick, University of Connecticut
▶ 11:00 – 11:30am: Case Study
Case Study 1: Data Breach
Suggestions

• Think about each of the roles needed in your organization (e.g., public information officer, data system leadership, attorney, auditors, etc.).

• The full extent or impact of a data breach is rarely known up front. Do your best to anticipate what might happen, but don’t get ahead of yourself.
District Data Breach Exercise

Each team will develop two key products:

1. **Public and Internal Communications/ Messaging** – Develop the message(s) you will deliver to your staff, students, other state agencies, the media, and the public.

2. **Response Plan** – Outline how the university will approach the scenario and what resources you will mobilize. Describe who will compose your response team. Identify goals and a timeline for your response.
Background and Scenario

• You are employed by Port Foozle University, a large school with 23,000 students enrolled.

• The university contracts with a very large software company, whose name starts with “Micro-“ and doesn’t end with “trademark violation”, to provide a suite of applications to employees and the student body.

• One of the applications this company provides is called “Shelve“ which allows for the sharing of media and documents to foster collaboration and productivity.
Background and Scenario (cont)

• “Shelve” permissions are tightly controlled, with only very few IT administrators authorized to have rights to view all documents currently uploaded.
• Yesterday afternoon, the University’s IT helpdesk received an interesting call: A observant student had noticed that some of the documents that they had access to on Shelve were not their own and not from any other place they currently had access.
• IT Helpdesk Workers were able to replicate the issue, and reported that they were able to access hundreds of student documents that were marked as “discoverable” using Shelve.
• Some of the documents contained Social Security numbers and other student PII.
• The Network Admin immediately suspended all student access to Shelve.
• University administration has ordered that you further investigate and begin prepping a response...
More Information is Uncovered

• Upon initial review, your team discovers that approximately 6,500 documents were made discoverable by anyone inside the university.
Okay, What Now?

1. Gather with your team.
2. Go over the background and scenario carefully. What do you know? What don’t you know?
3. Begin considering your approach to a response. Elect a team member to take notes.
4. We will regroup in 7 minutes. Be prepared to report how you are planning your response.
Port Foozle University Data Breach Exercise

7 Minutes
Questions to consider...

• Is there evidence of an actual breach?

• Do you have any legal responsibilities at this point?

• How do you respond to the findings? Acknowledge? Remain mute? Aggressively investigate?
Time to Regroup!

Let’s discuss each group’s approach to a response.
One of your staff just received word that the Port Foozle Register, the local paper, has just run a story on their website reporting that FAFSA forms from University students have been made publically available and can be freely downloaded.
Scenario Update

• How does this change your response?
• How you respond to your leadership?
• What information do you plan to provide?
• What are the assumptions you are making about the situation?
• Are you working on your resume?
Port Foozle University Data Breach Exercise

7 Minutes
Time to Regroup!

Let’s discuss each group’s approach to a response.
If It Hasn’t Come Up Already…

• How can you prevent this in the future?
  • Do you currently have data security policies and procedures in place?
  • Do you have a central number for someone to call should they have questions about the privacy and security of their child’s data?
  • Do you have FERPA Training implemented in any way?
  • Have your reporting obligations changed?
CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887
privacyTA@ed.gov
https://studentprivacy.ed.gov
(855) 249-3073
Today’s (Rough) Agenda

- **8:00 – 8:15am:** Welcome and Introductions
- **8:15 – 9:00am:** Michael Hawes, U.S. Department of Education
- **9:00 – 9:30am:** Case Study
- **9:30 – 10:00am:** Break
- **10:00 – 10:30am:** Amelia Vance, Future of Privacy Forum
- **10:30 – 11:00am:** Rachel Rudnick, University of Connecticut
- **11:00 – 11:30am:** Case Study
Today’s (Rough) Agenda

- 8:00 – 8:15am: Welcome and Introductions
- 8:15 – 9:00am: Michael Hawes, U.S. Department of Education
- 9:00 – 9:30am: Case Study
- 9:30 – 10:00am: Break
- 10:00 – 10:30am: Amelia Vance, Future of Privacy Forum
- 10:30 – 11:00am: Rachel Rudnick, University of Connecticut
- 11:00 – 11:30am: Case Study
Federal Laws and Actions

▶ FERPA
▶ There were several student data privacy bills introduced in Congress in 2015 and a FERPA re-write may pass in 2018. One bill has been re-introduced in 2017 so far.
39 States Have Passed 123 Laws Since 2013

- Law regulating SEAs and/or LEAs
- Law regulating both SEAs/LEAs and Third Parties
- Law regulating Third Parties
- Bill introduced since 2013 but none passed
Overview

▶ Over the last five years, states have enacted over 100 laws governing how schools and their service providers collect, use, and protect student data.
▶ Most of these laws cover information collected from students in elementary, middle, and high school settings.
▶ A handful of laws also govern how private and public institution of higher education use student data.
Unintended Consequences

- Has been a huge problem throughout this debate
- Words matter
  - Definitions
  - Vague language
- Fear-based policies
- Privacy problems with privacy legislation
- The need for input
- Penalties
Interesting Trends

- Governance
- Transparency
- Contracts
- Opt-In or Out Requirements
- Device and social media privacy
- Audits
- Training
- Penalties (financial and criminal)
State Laws

- Of the 106 state laws passed on student privacy since 2013, only 26 are applicable to higher education;
  - 12 regulate higher education substantively;
  - 14 only briefly mention higher education.
14 Laws that Briefly Mention Higher Education

- 2 require a state board to include a review of data systems in higher education in a comprehensive study,
- 10 permit K-12 schools, state boards, or state agencies to transfer information to institutions of higher education within the state longitudinal data system (SLDS),
- 1 dealing with training higher education employees in student data protection, and
- 1 that allows the state board of education to apply its data protection rules differently to institutions of higher education than it does to K-12 schools.
12 Laws that Substantively Regulate Higher Education

- 5 laws permit institutions of higher education to disclose certain student without facing any liability;
- 4 prohibit institutions of higher education from selling student information or requesting social media account information from students and penalizing them for refusing to provide it;
- 1 law places an affirmative duty on institutions of higher education to delete any student data they obtained through admissions; and
- 1 law provides postsecondary students with both a privacy and property right to their electronic communications on their school’s network.
Comparing Laws

- Most laws that discuss higher education either do not differentiate between private or public institutions of higher education (16 laws) or only apply the law to state schools (4 laws).
- This reflects a perceived inability by state legislators to govern private institutions of higher education.
Lack of Laws

- Misuse of data may be a concern because minors have less control over the information that is collected from them and how it is used.
- Primary and secondary education is mandatory while attending college or a university is optional.
- There are many more private (both secular and parochial) institutions in higher education than in K-12 schools.
Breaches

- 75% of the data breaches reported between 2010-2016 disclosed higher education records and only 25% impacted K-12 students.
- One possible explanation of this gap in regulation could be overreliance on general state data security laws to protect higher education students.
State Data Breach Laws

- However, some data breach state laws specifically exclude higher education institutions from security and breach requirements.
Student Privacy Bills and Research

▶ In 2014, 7 laws passed in 7 states included at least one provision targeted at researchers.

▶ In 2015, 53 bills in 21 states and 6 laws passed in 5 states included at least one provision targeted at researchers.

▶ In 2016, 47 bills in 19 states and 4 laws passed in 4 states (and an additional 2 laws passed in 2 states that were carried over from 2015) included at least one provision targeted at researchers.
In total, 19 states since 2014 have passed laws that included at least one provision targeted at researchers.
What is Driving These Laws?

- "What is education research, and why do I care about it?"
- "Researchers are able to get access to student data and use it for whatever they want."
- "Parents should always be allowed to opt their child out of research that will not directly improve their child's education or help their child in some direct way."

Beyond IRBs
Questions?

- www.fpf.org
- facebook.com/futureofprivacy
- @futureofprivacy
Today’s (Rough) Agenda

▶ 8:00 – 8:15am: Welcome and Introductions
▶ 8:15 – 9:00am: Michael Hawes, U.S. Department of Education
▶ 9:00 – 9:30am: Case Study
▶ 9:30 – 10:00am: Break
▶ 10:00 – 10:30am: Amelia Vance, Future of Privacy Forum
▶ 10:30 – 11:00am: Rachel Rudnick, University of Connecticut
▶ 11:00 – 11:30am: Case Study
WHAT DOES PRIVACY LOOK LIKE IN HIGHER EDUCATION?

(Seeing it from the view of one Higher Ed Privacy Officer)

Rachel Krinsky Rudnick, JD, CIPP/US
University of Connecticut
The Rules...

- FERPA
- HIPAA (hybrid?)
- GLBA
- GDPR
- Red Flags Rule (ID theft prevention, management)
- State laws
- PCI-DSS
- Breach management/notification
- Human Subjects, Export Controls, Research Compliance
- Balancing FOI (open records laws, sunshine laws)
- University policies
... best practices

Be a good human

What if it was my data?
Do you have a designated Privacy Officer?

- What is a Privacy Officer?
- Privacy vs. Information Security
- Privacy Office?
- Centralized function vs. embedded?
- Just part of someone’s job?
Where should Privacy report?

- Compliance
- Legal
- IT
- Audit
- Provost
- Registrar
- President / Board (!)
- Nowhere? Everywhere?
Models to consider

- Compliance/Regulatory function vs. Program
- Centralized vs. distributed (embedded)
- Big picture comprehensive program vs. regulation-by-regulation
- Reactive vs. Proactive approach
What is Privacy?

Photo credit: https://blogs.orrick.com/trustanchor/
An (user-friendly) oversimplification...

- Privacy is the WHAT
- Security is the HOW
What does a Privacy Officer do?

Some days it feels more like this:
Role of Privacy Officer

• Knowledge of (ever evolving) rules
• Oversee program
• Serve as privacy resource/subject matter expert
• Write (and possibly enforce) policies
• Review/draft contract language
• Assist/provide guidance to faculty, staff, students, constituents
• Investigate concerns/complaints
• Educate/Conduct training
• Breach management
• Internal/external communication
• Create and maintain relationships/partnerships
• Be a team player \( \rightarrow \rightarrow \rightarrow \text{committees, committees, committees} \)
it’s evolving...
It takes a village: Partnerships

Photo credit: http://smurfs.wikia.com/wiki/Smurf_Village
Partnerships & Collaboration with Stakeholders

- **ISO** → (i.e., Privacy is the What; Security is the How)
- **Legal** → many PO’s are attorneys, but still need assistance (contract language, interpretation, overlapping legal regimes)
- **Audit**
- **Risk Management**
- **Senior Management** (buy-in, Elevator Speeches)
- **Functional Offices** (Registrar, Bursar/Financial Aid, Research Compliance/Sponsored Programs, HR/Payroll, Health-related units)
- “**Compliance Cowboys**” – liaisons to support your efforts; train the trainer
Tools

- Data Inventories
- Records Retention & Information Management strategies
- Privacy Impact Assessments (PIA)
- Maturity Modeling
- Nymity’s comprehensive approach
- Beg, borrow and steal from colleagues (inside your university, and peers outside)
External resources

- HE-CPO group (supported by EDUCAUSE)
- IAPP
- Law firms
- Vendors (webinars, free tools)
- NACUA/AACRAO
- FERPA|Sherpa
So you want to be a Privacy Officer?


Today’s (Rough) Agenda

- 8:00 – 8:15am: Welcome and Introductions
- 8:15 – 9:00am: Michael Hawes, U.S. Department of Education
- 9:00 – 9:30am: Case Study
- 9:30 – 10:00am: Break
- 10:00 – 10:30am: Amelia Vance, Future of Privacy Forum
- 10:30 – 11:00am: Rachel Rudnick, University of Connecticut
- 11:00 – 11:30am: Case Study
Case Study 2

You are the Privacy Officer at a major public research university. You learn that a new, comprehensive set of privacy and data security regulations has been passed that may or may not apply to a subset of constituents with your campus. You read through the rules that have been enacted, realize that the terminology being used to describe the data to be covered, the rights of individuals whose data you hold and the monitoring, reporting obligations and data management (including information security) requirements are very different than what have applied to your university in the past. The penalties for non-compliance are significant and could cost your university tens of millions of dollars if a data breach were to occur, or if a complaint is filed with the enforcement entity created by the new regulations and that entity were to find your university non-compliant.
Case Study 2 (continued)

You dig a little deeper and realize that there likely are constituents of your university whose personally identifiable information may be covered by this new regulatory scheme, but you don’t have a good handle on what data you hold on those individuals, where it is stored, who can access it or how long you maintain it. Money is tight at your university as your state’s budget, and therefore its allotment to your university, keeps shrinking. You will need to figure out how to navigate the new rules and formulate a game plan and implementation strategy. No one has stepped up to take the lead at your university yet, but you know the risks of not getting this right are big and much of the new regulation focuses on data privacy and information management. You also know that it is likely that, even without asking senior management, leading the response and implementation initiative will fall on your shoulders. The regulations go into effect in 6 months.
Questions

■ What do you do first? How do you get started?
■ How do you go about determining the scope of the new regulation’s application to your university?
■ Where will you go to find out more information about the rules, how they apply and how to approach them?
■ Who do you reach out to in order to decide how to approach your university’s response and preparation?
■ Who will your partners be as you figure this all out?
■ What pitfalls do you expect as you lead up this initiative?
Time to Regroup!

Let’s discuss each group’s approach to a response.
Questions?

- www.fpf.org
- facebook.com/futureofprivacy
- @futureofprivacy