Data Privacy & Higher Education:
A Look at the Changing State and Federal Landscape in 2015

Matthew Johnson & Stephanie Cason
April 27, 2015
2015 NASASIPS Annual Conference

What We'll Cover Today
- Overview of Privacy Obligations
- State Legislative Activity
- Federal Legislative Activity
- Data Security Concerns
- Authentication and IAM Issues

Overview of Privacy Obligations
## Sources of Requirements

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act of 1996 (Hipaa)
- FTC
- State Laws

## FERPA

- 40 years old.
- Enforcement only through Dept. of Education (no private right of action). Only penalty is loss of federal funding by a school.
- Largely focused on parental/student access to records, but also addresses privacy.
- Significant “loopholes” – Directory Information largely exempt.
- No collection or use limitations.

## HIPAA

- Applies to “Covered Entities” - Health care providers, health plans, health care clearinghouses
- Protects “individually identifiable health information”
  - Health status, health care received, payment
  - Disclosures only as allowed by rules or if authorized in writing
- Must identify and protect against reasonably anticipated threats to security or integrity of information
- Enforced by complaints to HHS
  - Penalties of $100 to $50,000 per violation, up to $1.5 million per year
- Less stringent state laws are preempted, but more stringent state laws will be enforced
FTC
- Fair Credit Reporting Act
  - Generally applies only in the context of credit reporting
- Child Online Privacy Protection Act
  - Limits on collecting personal information from children under 13
- Gramm-Leach-Bliley
  - Financial products and services
- General fair trade practices jurisdiction
  - Basic requirement to do what you say you will do
- Adopted best practices in 2012

General State Laws
- Breach notification laws in 47 states, D.C., Guam, Puerto Rico, Virgin Islands
  - Define covered information and entities
  - Define breach
  - Specify timing, method and target of notification
- Online privacy
  - Privacy policies (California, Connecticut, plus 16 other states as to government sites)
  - False and misleading statements (Nebraska, Pennsylvania)
- Employee communications
  - Monitoring notices (Connecticut, Colorado, Delaware, Tennessee)
21 States Passed Significant Student Data Privacy Bills in 2014

- **2014**
  - 110 bills introduced in 36 states.
  - 24 bills signed into law.
- **January-March 2015**
  - 138 bills introduced in 39 states.

General themes:
- Security
- Transparency
- Collection
- Use

April 2015 – National Association of State Boards of Education
- “Regulating Student Data Privacy: Don’t Throw the Baby out with the Bathwater”
The Student Online Personal Information Protection Act ("SOPIPA") applies to operators of websites, online services, or mobile applications used or designed for K-12 school purposes (defined broadly). Does not apply to similar services for postsecondary purposes (yet). Open question: Does it apply to college application assistance services? Prohibits targeted advertising using personally identifiable information (PII) from students or creating a profile of students using PII unless for a K-12 school purpose. Prohibits the sale of PII or disclosure of PII unless in furtherance of the school purpose.

Recent State Legislative Activity

California
- Applies to operators of websites, online services, or mobile applications used or designed for K-12 school purposes (defined broadly).
- Does not apply to similar services for postsecondary purposes (yet).
- Open question: Does it apply to college application assistance services?
- Prohibits targeted advertising using personally identifiable information (PII) from students or creating a profile of students using PII unless for a K-12 school purpose.
- Prohibits the sale of PII or disclosure of PII unless in furtherance of the school purpose.

California (cont'd)
- Security and Deletion Requirements
  - Required to maintain reasonable security procedures and practices and protect against unauthorized access, use, modification, disclosure, or deletion.
  - Must delete information in operator’s possession if school district requests.
- Effective January 1, 2016
- So far in 2015, 10 states have introduced legislation based on SOPIPA.

Recent State Legislative Activity

Florida
- Senate Bill 188
  - Limits the type of PII that public institutions (K-12 and postsecondary) may collect about students.
  - Prohibits collection of information regarding the political affiliation, voting history, religious affiliation, or biometric information (including fingerprint) of a student or member of a student’s family.
**Recent State Legislative Activity**

**Rhode Island**
- **Senate Bill 2095**
  - Prohibits educational institutions (public or private) from requesting access to a student’s (or applicant’s) social media account.
  - Students may not be disciplined for refusing to “friend” a school official (including athletic coaches).
  - Does not prohibit institutions from taking disciplinary action (or refusing admission) based on information that is publicly available.

---

**Federal Legislative Activity**

- Dept. of Education “Model Terms of Service”
  - Nominally designed for K-12 schools.
  - Provides a list of “best practices” for agreements with third parties in the ed tech space.
  - Does not change the law or regulations.
  - Goes beyond minimum legal requirements.
Messer/Polis Bill
- Based on California’s SOPIPA, but not as strict.
- Some exceptions for postsecondary or employment related activities.
- Would not preempt state law.
- Enforcement through the FTC.
- Bipartisan and White House support, but still a challenging political environment.

Federal Activity

FERPA Amendment?
- Senate Bill introduced last session (Hatch/Markey)
- House action possible in 2015
- Possible Changes
  - Majority of FERPA untouched for decades – time to modernize
  - Data security expectations
  - Closer look at marketing and promotional uses
  - Third parties possibly liable for violations
  - Revised penalties
  - Major hurdles to clear.
  - HEA reauthorization.

Federal Activity

Voluntary Student Data Privacy Pledge
- www.studentprivacypledge.org
- Focused on K-12, but some postsecondary implications.
- 127 Signatories (as of April 1, 2015)
- Can it be enforced?

Other Activity
Industry and government efforts
- FFIEC guidance, Digital Signature Guidelines, EV certificates, etc.
- M-04-04 (U.S.), IATF (Canada), etc.
- Distance learning requirement
- Must have “processes in place... (to establish) that the student who registers in a distance education... program is the same student who participates” in the program (34 C.F.R. 602.17)

Commercial Adoption of Multi-factor
- Twitter
  - In May 2013, Twitter announced that it was “introducing a new security feature to better protect your Twitter account: login verification. This is a form of two-factor authentication. When you sign in to twitter.com, there’s a second check to make sure it’s really you. You’ll be asked to register a verified phone number and a confirmed email address.”
- Evernote
  - In March 2013, Evernote suffered a breach of its systems; fraudulent identity credentials played a part.
  - In May 2013, Evernote rolled out an updated system with two-factor authentication, initially for its premium users; utilizes SMS messaging.
  - The company said it will “continue the roll out to our larger user base” after getting feedback from the premium users.
Stakeholder Scope and Relationships?

- Risk management
  - Relationship between liability assumption and control capability
  - How to manage and contract for new risks (transaction velocity, pattern changes)
  - How to manage current risks (e.g., identity fraud)
- Geographic requirements
  - Legal enforceability and local dispute resolution capabilities
- Support
  - Provisioning
  - Lifecycle management
  - Helpdesk/call center integration & escalation

PROACTIVE AND REACTIVE CONSIDERATIONS

Data Security and Liability Concerns

Liability and Contract Issues

- Risk management
  - Relationship between liability assumption and control capability
  - How to manage current risks?
  - How to manage new risks?
- Issues introduced by Federated Identity
  - Legal enforceability and local dispute resolution capabilities
  - Relationships with technology and service providers
  - Relationships with employees, business partners, and others
- Support
  - Provisioning
  - Lifecycle management
  - Helpdesk/call center integration & escalation
Selected Litigation Examples

- **Experi-metal v. Comerica (2012)**
  - The bank actually utilized a form of "true" multi-factor authentication. Through a phishing attack, the fraudsters obtained the EMI’s username, password and token number, and logged in immediately upon capturing them.
  - Once a legitimate online banking session was established, they initiated approximately 57 wire transfers over a six-hour period totaling $1.9M.
  - Judge ruled for business stating "[t]he trier of fact is inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier."

- **Choice Escrow and Land Title v. BankcorpSouth Bank (2012)**
  - Counterclaims by a bank against a commercial customer have been dismissed in a case where hackers accessed the customer’s account and drained it of over $400,000. In the original action, Choice Escrow brought suit against BankcorpSouth Bank alleging that BSB failed to provide commercially reasonable security by having only password protection on Choas’s account.

- **PATCO v. People’s United Bank (Ocean Bank) (2012)**
  - PATCO alleged that Ocean Bank’s online security was not commercially reasonable under Article 4A of the Uniform Commercial Code (UCC).
  - All of the transactions were “uncharacteristic” in that they sent money to numerous individuals to whom PATCO (1) had never before sent funds; (2) were for greater amounts than PATCO’s ordinary third-party transactions; (3) were sent from computers that were not recognized by Ocean Bank’s system; and (4) originated from IP addresses that were not recognized as valid IP addresses of PATCO,” the ruling said.
  - The court found that Ocean Bank was not monitoring its transactions for fraud nor notifying customers before a suspicious transaction was allowed to proceed - both capabilities that it did possess within its security system.

Selected Litigation Examples (cont’d)

- **Practical Considerations**
  - Risk reduction
    - Establish secure method for doing initial l&A; balance needs against privacy obligations and risks
    - Carefully negotiate contracts with all entities involved in deploying an identity management solution to distance education participants
    - Consider how to leverage any existing federated identity solutions
  - Standard “blocking and tackling”
    - 1. Create Governance Structure That Addresses IAM
    - 2. Prioritize Information Assets and Analyze Risk
    - 3. Create Security Protection Plan Tied to a Technology Acquisition Strategy
    - 4. Request Regular Updates and Adjust Accordingly
    - 5. Test Response Plan
    - 6. Maintain Appropriate Insurance Coverage
    - 7. Provide Regular Cybersecurity Training
Resources

FERPA
Regulations:
FERPA - http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=11975031b82001bed902b3e73f33e604&rgn=div5&view=text&node=34:1.1.1.33&idno=34
Distance Learning - http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=d47a835cb32d5c5042ac596901473db3&rgn=div8

HIPAA
HHS HIPAA page: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

State data breach laws

Governance
NIST Cybersecurity Framework
http://www.nist.gov/cyberframework

Questions?