OPERATIONALIZING PRIVACY AND DATA SECURITY COMPLIANCE IN HIGHER EDUCATION

SCCE VIRTUAL HIGHER EDUCATION COMPLIANCE CONFERENCE
JUNE 1, 2020

Who we are:

Tres Cleveland
SHAREHOLDER
tcleveland@maynardcooper.com

Starr Turner Drum
SHAREHOLDER, CIPM, CIPP/E, CPP
sdrum@maynardcooper.com
The Importance of Geography

General Rule:
Individual’s residence = applicable law
General Privacy Principles

- Limited collection
- Purpose specification
- Use limitation
- Notice + Transparency
- Legal bases for processing
- Choice
- Data minimization
How to Think About Privacy Obligations

**What platform(s) are being used?** e.g., website, mobile application, remote instruction or proctoring platforms

**Who is being targeted and/or monitored?** e.g., administration, faculty, staff, students, members of students’ households

**Where are the targeted/monitored individuals located and where is their data going?** Remember the importance of geography.

**What information is being collected?** e.g., education records, directory data, IP address, video/audio recordings, biometric data

The requirements for disclosures, consent, scope of use, and third party sharing are all impacted by the answers to these questions.

---

Geography

<table>
<thead>
<tr>
<th>U.S. (except California)</th>
<th>INTERNATIONAL*</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sectoral (e.g., FERPA, GLBA, HIPAA)</td>
<td>• Omnibus</td>
</tr>
<tr>
<td>• Multiple inconsistent statutes</td>
<td>• One comprehensive privacy/data protection statute for public and private sectors</td>
</tr>
<tr>
<td>• Sensitive data = education records, financial, health</td>
<td>• Sensitive data aligns with equal protection</td>
</tr>
<tr>
<td>• Protected personal data context-dependent</td>
<td>• Broad scope of personal data</td>
</tr>
<tr>
<td>• Enforcement by federal and state regulators with other enforcement responsibilities (CA, too)</td>
<td>• Enforcement by single data protection authority</td>
</tr>
<tr>
<td>• No restrictions on international transfers</td>
<td>• Regulation of cross-border transfers</td>
</tr>
</tbody>
</table>
Scope of Applicability

**GDPR**
Applies to organizations:
- established in the EU, OR
- Offer goods and services to individuals within the EU, OR
- Monitor the behavior of individuals within the EU

**CCPA**
Applies to for profit entities doing business in California that:
- Have annual gross revenues in excess of twenty-five million dollars ($25,000,000); OR
- Annually buys, receives, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; OR
- Derives 50 percent or more of its annual revenues from selling personal information

**FERPA**
Applies to all schools that receive funding from the department of education

<table>
<thead>
<tr>
<th>GDPR</th>
<th>CCPA</th>
<th>FERPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controllers and Processors</td>
<td>No controller/processor distinction. Entities can be “businesses,” “third parties,” or “service providers.”</td>
<td>Educational Institutions and School Officials</td>
</tr>
<tr>
<td>Employees and B2B personnel captured</td>
<td>No employees, no B2b personnel for 2020</td>
<td>Only applies to eligible students</td>
</tr>
<tr>
<td>Rights = access, information, portability, deletion, rectification, restrict processing, object to automated processing</td>
<td>Rights = information, access, portability (sort of), deletion, opt out</td>
<td>Access and amendment rights</td>
</tr>
<tr>
<td>One month (+2 months, if needed) to respond to rights requests</td>
<td>45 days (+45 days, if needed) to respond to rights requests</td>
<td>45 days to respond to access request</td>
</tr>
<tr>
<td>No mechanism mandate for individual rights requests</td>
<td>Mandates mechanisms for consumer rights request submissions</td>
<td>Annual notice must include information about request mechanism</td>
</tr>
</tbody>
</table>
Recent Relevant Privacy Litigation

• United States v. Facebook, Inc.

• Everyone v. Zoom

• BIPA litigation and circuit split

• CJEU Schrems II decision announced for July 16, 2020

Privacy Compliance To Dos

✓ Data inventory and mapping
✓ Assess vendor data collection use and sharing and ensure appropriate privacy provisions are in place in vendor agreements
✓ Evaluate and update privacy notices and consents for students, faculty, staff, etc.
✓ Evaluate and update individual rights response process and procedures and include vendors in process where needed
✓ Evaluate and update record retention and deletion practices
DATA SECURITY

What is a data breach?
- Unauthorized access to or acquisition of certain types of information

What is sensitive data?
- Differs by geography. Can include proprietary/competitively sensitive data; intellectual property, health info, SSN, etc.

What are the risks?
- Fines/penalties
- Lawsuits
- Reputational damage
- Other financial costs
DATA SECURITY REGULATORY FRAMEWORK

- International laws (e.g., GDPR)
  - Have proactive security requirements and requirements to report breach to regulators within 72 hours
- FERPA
  - Schools must use “reasonable methods” to secure education records
- State Data Breach Notification Laws
  - 1 in every state
  - Apply according to the residence of the impacted individual
  - Some states have proactive security requirements

CIS TOP 20

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises
Users are an organization’s greatest threat.

- Attackers target PEOPLE.
- Social engineering is becoming increasingly sophisticated.
- Over 99% of emails distributing malware require human intervention for them to be effective.
- The pandemic has greatly exacerbated these vulnerabilities.

If you SEE something, 
SAY something.
VALIDATE all requests to send sensitive information or to transfer funds.

- Call the sender or other contact using a previously established, trusted phone number.
- Use dual controls for funds transfers.
- Beware of any change in wiring instructions, bank name, or payment method.
- Employees in HR, Payroll, Procurement, and Finance should receive special training.

Incident response tips:

- Have a plan.
- Follow the plan.
- Test the plan.
- Invoke and maintain the attorney-client privilege.
- Control and centralize communication and documentation.
- Messaging matters!
Recent Relevant Cybersecurity Litigation

- *In re: Equifax, Inc., Customer Data Breach Security Litigation*

- *In re: Target Corporation Customer Data Security Breach Litigation*

- *FTC v. Wyndham Worldwide Corp.*

Security Compliance To Dos:

- Bolster remote security protocols
- Evaluate and update Written Information Security Plan
- Assess and audit vendor security
- Test and update incident Response Plan (remote tabletop)
- Evaluate cyber insurance coverage and make sure it’s sufficient
Questions?