

DuaneMorris®

[www.duanemorris.com](http://www.duanemorris.com)

# Privacy and Security Challenges for Distance Learning

©2020 Duane Morris LLP. All Rights Reserved. Duane Morris is a registered service mark of Duane Morris LLP.

Duane Morris – Firm Offices | New York | London | Singapore | Philadelphia | Chicago | Washington, D.C. | San Francisco | Silicon Valley | San Diego | Los Angeles | Taiwan | Boston  
Houston | Austin | Hanoi | Ho Chi Minh City | Shanghai | Atlanta | Baltimore | Wilmington | Miami | Boca Raton | Pittsburgh | Newark | Las Vegas | Cherry Hill | Lake Tahoe | Myanmar | Oman  
Duane Morris – Affiliate Offices | Mexico City | Sri Lanka | Duane Morris LLP – A Delaware limited liability partnership

## Presenters



Michelle Donovan, Partner Duane Morris LLP  
619.744.2219 | [MHDonovan@duanemorris.com](mailto:MHDonovan@duanemorris.com)

# Recording Virtual Classrooms

## FERPA

“Education records” are (i) directly related to a student; and (ii) maintained by an educational agency or institution or by a party acting on behalf of the educational agency or institution.

### Recent Department Guidance:

Video recordings of virtual classroom lessons qualify as “education records” protected under FERPA only if they directly relate to a student and are maintained by the institution or by a party acting on their behalf. FERPA’s nondisclosure provisions may still apply to such video recordings even if they do not qualify as “education records,” if the video recording contains PII from student education records

# Recording Classrooms

## Other Legal Considerations

- Constitutional Right of Privacy - reasonable expectation of privacy
- Wire Tapping Laws

## Online Proctoring

- Collection of sensitive personal information
  - Drivers License
  - Biometric Data
  - Video recordings
- Part of student education record
- Surveillance and wire tapping issues

## EdTech Privacy Concerns

- Common Sense EdTech Privacy Report – only 20% met minimum standards
- Large Number of Startups
- Technology Companies Not Familiar with Highly Regulated Education Sector
- Adopting Technology Not Intended for Use in Education Sector
- Student Education Records

## What Laws Apply

- **FERPA**
- **Wire Tapping Laws**
- **California Consumer Privacy Act**
- **State Privacy Laws – Privacy Policies**
- **Breach Notification Laws**
- **Biometric Privacy Laws**



# FERPA

## School Official Exception

- Performs an institutional service or function for which the institution would otherwise use its own employees;
- Meets the criteria for being a school official with a legitimate educational interest in the education records or PII;
- Under the direct control of the institution
- Uses the education records or PII only for authorized purposes and does not redisclose the education records or PII to other parties



## Constitutional Right and Wiretapping

- If recording:
  - Notify individuals upfront if recording
  - Use recording indicator to show when recording
- Limit access, use and disclosure
- Accurate Privacy Policy

## California Consumer Privacy Act (CCPA)

- Privacy Notice Requirements
- Service Provider Requirements and Limitations
- Consumer Requests

## State Laws – Privacy Policies

- Requires commercial websites and online services to post a privacy policy that describes:
  - Categories of personally identifiable information (PII) collected
  - Categories of third parties with whom the you may share PII
  - Description for notifying users of material changes to policy
  - Effective date

### CalOPPA

- How you respond to a browser's Do Not Track signal or to other such mechanisms.
- The possible presence of other parties conducting online tracking on the operator's site or service

# Breach Notification and Biometric Privacy Law

- Sensitive Categories of Information
- Breach Notification Requirements in the Event of Breach
  - Who is Responsible For the Notice?
  - Who Pays?
  - Third party claims
  - Government Investigation
- Biometric – restrictions on collection, use and retention

## ASK

- What personal information is collected?
- How are they handling consent (if needed)
- How are they protecting the information?
- How long is the information kept?
- How is the information used by the company?
- How is the information shared with third parties?
- If shared, what are they doing to protect the data and ensure third party compliance with laws?

## Terms of Service

- Data Ownership
- Limit how data can be collected, used and maintained
- FERPA acknowledgement and warranty
- Information security requirements
- Breach and notification obligations
- Indemnification for breach or failure to comply with law
- What happens to the data if you switch providers and/or otherwise terminate use of services?
- CCPA service provider provisions if applicable

## 2020 Cybersecurity Risks

- **400% Increase in cyberattacks during pandemic**
- **Phishing Attacks**
  - 67% of all breaches last year
  - Social engineering to steal credentials
- **More Sophisticated and Targeted Ransomware Attacks**
  - Malicious software, or malware, that uses encryption to deny access to a computer system or data until a ransom is paid
  - Extraction and encryption
  - <https://ifap.ed.gov/electronic-announcements/090120TechSecurityAlertActiveRansomwareCampaignTargetingEDInst>



## Mitigating Risk

- Comprehensive Information Security Program
- Training and Building a Security Culture
- Multifactor Authentication

# Resources

## Department of Education

<https://ifap.ed.gov/fsa-cybersecurity-compliance>

<https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best>

<https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning-during-covid-19>

## NIST Guidelines

[http://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=918804](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=918804)

## EDUCAUSE

<https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program>