Looking Forward: Privacy in 2021

EDUCAUSE Annual Conference
10/29/2020

Amelia Vance
Director of Youth & Education Privacy
avance@fpf.org
Reflecting on 2020 (so far...)

FUTURE OF PRIVACY FORUM
Why Does Privacy Matter During a Pandemic?

Tracking the Coronavirus at U.S. Colleges and Universities


214,000+ Cases  1,600+ Colleges
Why Does Privacy Matter During a Pandemic?

Because higher ed students, faculty, administrators, and broader communities keep saying it does
Three Types of Risk

■ Harm
Is the tool (or how your school / your students use the tool) safe, secure, private? (harms can be individual, organizational or societal)

■ Compliance
Is the tool (or how your school / your students use the tool) in compliance with federal, state or local regulations and policies?

■ Reputation
Regardless of the above, how is this perceived by the community?
Over history, privacy was often defined as control over information about you, with a distinction about private vs public information. But as lines blur between private and public and there is a limit to what individuals can actually control, a new theory of how to think about privacy was proposed by scholar Helen Nissenbaum.

“A right to privacy is neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information... finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g., education...)...”

-Helen Nissenbaum, Privacy in Context
Edge Cases

“The world is made of edges. Systems are large enough that ‘edge cases’ aren’t.”

- Lea Kissner, Chief Privacy Officer at Humu; Former Global Lead of Privacy Technology at Google

What are the student circumstances that we think of as “edge cases” that are likely in every school?

Source: Lea Kissner, Building for Trust, 2019 presentation
Examples of “Edge Cases”

- Students with invisible disabilities
- Students who are LGBTQIA with families that would harm or kick them out if they knew
- Students facing abuse at home
- Students who are undocumented, or whose families are undocumented
- Students who are homeless
- Students who may not have access to a computer, a tablet, or a phone
- Students who may not have access to the internet or may have metered or slow internet

Students don’t owe you disclosure of this information - so how can you protect their privacy without knowing it?
Exacerbated Potential Privacy Risks When Moving Online

- Amplifying the accessibility of information
- Revelation of information that impacts how others see them
- Information shared for one purpose and used for another purpose
- Surveillance effects
- Invasion into the solitude of the home
Potential Harms

- Can Break or Damage Trust - and therefore Adoption and Data Quality
- The Surveillance Effect
- Equity and the Digital Divide
- Students May be Less Likely to Seek Help
- Students May Drop Out
- Increase the School-to-Prison Pipeline
- Inappropriate Use by School Personnel
- The “Permanent Record”

What can be discovered about you from “innocuous” information? What privacy protections are needed to provide guardrails to new collections and use of data related to the pandemic?
Exacerbated Student Privacy Compliance & Liability Risks

- USED (FERPA+FSA Agreements)
- ADA
- GLBA and other security requirements (NIST 800-171)
- State AGs (state student privacy laws)
- HHS (HIPAA)
- Other judicial remedies (common law, 4th Amendment)
- FTC and companies
And sometimes it’s not really about privacy...

“Privacy was once misconstrued as being about hiding and secrecy. Now it’s understood to be something much more pressing: power dynamics between the individual, the state and the market. [Data protection] must seek to mitigate the inherent power imbalances between people — and those that collect, process and profit off their data.”

–Frederike Kaltheuner
Triaging Privacy

- Disclosure of COVID-19 diagnoses
  - FERPA’s health or safety exception
- Rapid switch to online learning
  - Awkward rollouts
  - Expanded decentralized adoption of noncompliant and non-privacy protective technologies
    - Expanded use of non-education products
- Even more difficult to track adoption and use
- “Zoombombing”
- Video and video recording issues
- More monitoring of students
- Policymaker concerns
Managing the Privacy Risks of Moving Education Online

- What are privacy risks when in-school learning transfers online?
  - Classes (synchronous vs asynchronous, recorded or not, video on or off, verifying participation/engagement)
  - Assessments
  - Office hours and mentoring
  - Counseling and trauma-awareness
  - Social experiences and community
Triaging Privacy 2.0

- Disclosure of COVID-19 diagnoses
- (Somewhat) unexpected continued online learning
- Back-to-"normal" with expectations, grades, and tests
  - With measuring engagement, proctoring software, and other technological ways of monitoring
- Tracking student and staff health, social distancing, and adherence to school coronavirus policies
- **Avoid or Accept**: If we make the very generous assumption that these technologies actually work as they claim, what are the criteria we can use to determine if the risk posed by these technologies is worth any benefits they might bring?
Newer Ways Students Are Monitored

- Wearables
- Facial Recognition
- Social Media
- Network
- Attendance & Engagement
- Security Cameras
- Wearables

Security
Cameras

Facial
Recognition

Attendance & Engagement

Social Media

Network
A school mandated that students wear a COVID-detecting ‘BioButton.’ They fought back

The BioButton was supposed to send them back to college safely. But concerns over the mandatory wearable's data collection practices led to a student petition—and a school reversal.

ExamSoft’s remote bar exam sparks privacy and facial recognition concerns

Researchers Raise Concerns About Algorithmic Bias in Online Course Tools
More Data & Tech = More Potential For Mistakes

Hofstra disables data tracking on temperature kiosks

EdScoop News @EdScoop_news · Aug 28
Hundreds of students’ COVID-19 test data left unprotected at University of Kentucky @universityofky hubs.ly/i/HOvCH8D0
It doesn’t have to be true to go viral…

Wolfgang 🇺🇦 🇦🇺 @Ouren · Mar 21
Everyone working remotely:

ZOOM monitors the activity on your computer and collects data on the programs running and captures which window you have focus on.

If you manage the calls, you can monitor what programs users on the call are running as well. It’s freaking up.

516  14.9K  41K

Zoom 🌐 @zoom_us · Mar 22
Hi, attention tracking feature is off by default - once enabled, hosts can tell if participants have the App open and active when the screen-sharing feature is in use. It does not track any aspects of your audio/video or other applications on your window.

Attendee attention tracking
As of April 2, 2020, we have removed the attendee attention tracker feature as part of our commitment...

support.zoom.us

63  103  987
But There Are Privacy-Protective Ways To Move Forward
But There Are Privacy-Protective Ways To Move Forward
Managing the Privacy Risks of Reopening Schools In-Person

- Data sharing
  - Does the school require disclosure of COVID-19?
  - Will your reopening plan require disclosure of preexisting conditions?
  - Will your school require documentation? (ex/ doctor notes, antibody test results, eventually vaccination status)

Opt-ins/out?

Minimizing discrimination: how could information be reused or abused?
Managing the Privacy Risks of Reopening Schools In-Person

- Tech (and research efficacy)
  - Biometric scanning to minimize touching
  - Contact-tracing apps and location tracking
  - Social distancing detectors and location tracking
  - Wearables

- Temperature checks
- Thermal imaging (may include AI/FR)
- Cough detectors
- Dogs as disease detectors

- Opt-ins/outs?
- Minimizing discrimination: how could information be reused or abused?
Some technologies are **inaccurate**. They don’t measure or detect what they claim to, or they do it poorly. The **consequences** can be life altering and even fatal.
Even when a system works perfectly accurately, it can still cause harm. The records that the system relies on can reflect previous discrimination, or the system can be applied in unjust ways.
Mitigating the Privacy Risks of Remote Learning

- Policy creation and expansion
  - Video/web conferencing
  - Monitoring
  - Assessments
  - Accountability
  - Discipline policies
- PD for educators
- Embedded privacy
- Cybersecurity
...Plus all the normal privacy issues in postsecondary education
Colleges scrapping spring break amid travel concerns during coronavirus pandemic

One school said spring break would "increase the risk of spreading COVID-19."

By Meredith Dello
September 29, 2020, 6:03 AM • 6 min read

BU to preserve class recordings for potential use in lawsuits

Cal State universities will stay online all year amid COVID-19 pandemic

The Post-Pandemic Evolution of Student Data Privacy

The critical importance of maintaining strong data privacy and governance policies and protocols has only increased with the shift toward a remote delivery model in higher education due to the COVID-19 pandemic.
Pandemic surge?
Continued virtual learning
More data collection and technology adopted when classes are back in-person
New Congress
New President? (or at least likely new appointees)
FERPA
Consumer privacy laws
Increased focus on cybersecurity from policymakers and enforcement agencies
A culture of privacy within schools means everyone who has access to students’ personal information is trained and know why and how to effectively and ethically collect, use, share, protect, and secure it.
Resources - Covid & Online Learning

- FERPA and Virtual Learning (1-page list of resources), U.S. Department of Education
- FERPA and Virtual Learning webinar slides and recording, U.S. Department of Education
- FERPA and Virtual Learning short video and Q&A on Remote Learning and Student Confidentiality, Utah State Board of Education
- Privacy Considerations in Higher Education Online Learning, New America OTI
- FERPA and the Coronavirus Disease 2019 FAQ, U.S. Department of Education
- COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus, Federal Trade Commission
- Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies, CoSN
- Cybersecurity Considerations in a COVID-19 World, CoSN
- 10 Key Steps to Establish Distance Learning Amid COVID-19, F3 Law

Subscribe to FPF’s monthly student privacy newsletter here
FPF Student Privacy Resources by Special Topic

- Student Privacy During the COVID-19 Era
- State Student Privacy Laws
- Train-the-Trainer Program
- Student Privacy Compass Blog
- Student Privacy Newsletter
- Student Privacy Reports
- Infographics
- Videos, Webinars, Presentations, & More!
FPF Issue Brief Series

- Increased Data Collection and Sharing
- Thermal Scans and Temperature Checks
- Wearable Technologies & COVID-19
- Location Tracking & COVID-19
- Online Monitoring & COVID-19
- ...& more to come!
Additional Student Privacy Resources

- Privacy Technical Assistance Center, US Department of Education
- An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies, Berkman Klein Center for Internet and Society
- Student Privacy Compass
- Protecting Privacy in Connected Learning Toolkit, Consortium for School Networking
- Forum Guide to Education Data Privacy, NCES
- Parents: Raise Your Hand and Ask Schools How They Protect Student Data, FPF
- Common Sense Media Privacy Evaluations
- Student Data Privacy Consortium Resource Registry
- Data in the Cloud: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era, National School Boards Association
- The Educator’s Guide to Student Data Privacy, FPF and ConnectSafely
- Student Data Privacy website and training videos, Utah state education agency
- California Data Privacy Guidebook, CCSESA, CITE, and F3 Law
- Predictive Analytics in Higher Education: Five Guiding Practices for Ethical Use, New America
Other Relevant FPF Areas of Privacy Expertise

- **AI and Machine Learning** (including algorithmic harms)
- **Biometrics** (including **facial recognition**)
- **De-identification**
- **Ethics** (including company-researcher partnerships, big data ethics, responsible data use during crises, and designing an ethical review process for research access to corporate data)
- **Health**

- **International** (particularly EU and Israeli privacy laws and requirements)
- **Location-tracking and advertising practices**
- **Mobility** (including connected cars)
- **Smart communities** (including integrated data systems)
- Both **International** and **U.S.** policymaker education through classes and highlighting exemplary privacy scholarship
Questions?

Amelia Vance
Senior Counsel and
Director of Youth & Education Privacy
Future of Privacy Forum
avance@fpf.org
@ameliaivance
www.studentprivacycompass.org