NEW AMERICA

October 2020

Privacy Considerations in Higher Education Online Learning

Chris Sadler

Acknowledgments

We would like to thank the Bill & Melinda Gates Foundation for its generous support of our work. The views expressed in this report are those of its author and do not necessarily represent the views of the foundation, their officers, or their employees.

About the Author(s)

Chris Sadler is the Education Data and Privacy Fellow at New America's Open Technology Institute.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Contents Cont'd

Introduction

When colleges and universities started shutting down in March of 2020 in response to the spread of COVID-19, they were forced to move from in-person or semi-digital environments to fully online in a matter of days. This led to one of the largest educational technology experiments in history, with the average institution needing to move more than 500 courses online.[1] Many colleges were already developing or expanding online education programs prior to the pandemic, but for others the move to online education is new. With the fall 2020 semester, some institutions have attempted to re-open for in-person classes or opted for a hybrid model of holding classes online while bringing some students back to campus, but many are primarily offering distance learning.[2]

The educational technology (ed tech) used for delivering online classes is serving an essential role in allowing schools to continue teaching under unusual conditions. However, the ongoing shift to remote learning is leading privacy professionals, faculty, students, and others to focus on both pre-existing and new privacy issues related to the technology facilitating online learning. Given the younger age of the students in K-12, educators have recognized for some time that the use of ed tech in secondary school education raises privacy concerns. The devices used for K-12 education are more likely than those used in higher education to be issued to students or accessible in the classroom, and researchers and privacy advocates have long been concerned about the use of these devices for surveillance,[3] school shooting prevention,[4] and other secondary purposes that raise privacy issues.

Until fairly recently, higher education institutions focused more on the cybersecurity aspect of data protection. It was not until 2018 that privacy first showed up on the top 10 list of information technology issues in EDUCAUSE's[5] information technology poll of institutions.[6] Privacy advocates and the media have brought greater attention to privacy in higher education in part due to the collection of student data for predictive analytics uses[7] and greater on-campus surveillance of students.[8] The increased use of remote learning, and the increasing amounts of student data they generate, will add to privacy concerns. There are clearly important questions about what happens to the data collected in the course of providing distance learning that institutions and ed tech companies need to answer.

Distance learning will likely be an important issue of discussion and scrutiny in higher education for some time. Schools will continue to rely on it as the pandemic continues, but there is also the potential for a longer-term shift to more distance education in the post-pandemic future. This paper offers an overview of privacy issues and concerns related to online learning in higher education.

Applicable Laws

Family Educational Rights and Privacy Act (FERPA)

The primary law regulating privacy in both K-12 and higher education is the Family Educational Rights and Privacy Act (FERPA).[9] FERPA provides students the right to access records an institution keeps on them, the right to request to have the records amended, and offers some control over the disclosure of personally identifiable information (PII) from education records. FERPA applies to all academic institutions receiving funds under applicable Department of Education programs.

FERPA is essentially technology neutral and does not address online learning specifically. Currently, there is no official FERPA certification program for assessing third-party ed tech compliance for higher education. Products and services may outline how they comply with FERPA, but ultimately every institution must perform its own assessment to determine how their use will affect the institution's ability to comply.

FERPA's definition of PII is more expansive than direct identifiers such as social security numbers or biometric features. It also includes semi-direct identifiers such as date of birth and mother's maiden name, as well as "other 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."[10] However, data that is anonymized ("de-identified") so that it does not contain personally identifiable data can be shared with any third party without consent.[11]

Generally, FERPA requires written consent from students attending a postsecondary institution before releasing educational records that contain PII. However, FERPA contains several exceptions to the consent requirement. The "school official" exception is the one most relevant to distance learning and use of ed tech vendors. This exception permits disclosures from student education records to school officials who have a "legitimate educational interest" in having access to a student's records. School officials in this capacity includes not only administrators and teachers, but also information technology personnel, and others.[12] This exemption permits the disclosure of PII from education records in the course of outsourcing to ed tech companies. Vendors can act as de facto school officials as long as the services or functions they provide are ones "for which the educational agency or institution would otherwise use its own employees." However, schools must retain direct control over how PII is used and

maintained, and they remain legally responsible for what happens to any data disclosures to ed tech companies.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA),[13] passed in 1999, largely reformed regulation of the financial services industry, but also included provisions relating to consumer financial privacy. The Federal Trade Commission (FTC) considers higher education institutions to be financial institutions subject to the GLBA if they participate in Title IV educational programs (that is, the school accepts federal financial aid for students). GLBA regulations include a privacy rule governing data privacy practices, but the FTC deems higher education institutions to be in compliance with the privacy rule if they are in compliance with FERPA. The Safeguards Rule of the GLBA, which is not covered by compliance with FERPA, concerns data confidentiality, but primarily from a standpoint of cybersecurity requirements. The Department of Education recently indicated that it will audit institutions for compliance with the Safeguards Rule of the GLBA.[14] Requirements for compliance include performing a risk assessment that addresses network and information system security controls, incident response, and security training of employees. Schools must implement a safeguard for each risk identified.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a state law passed in 2018 that gives California consumers new rights and additional controls over personal information that businesses collect and use. As of January 1, 2020, companies and institutions conducting business either in California or with the state's residents come under regulation by the CCPA.[15] With the increase in remote learning and the potential for more California residents attending schools based in other states, the CCPA is relevant to schools across the country. Most colleges and universities would seem to be unaffected, as the law only pertains to for-profit entities. However, schools' increasing use of for-profit vendors in providing distance learning may make the CCPA applicable. Whether a vendor falls under the purview of the CCPA is based on certain criteria. A business/vendor must either have an annual gross revenue of greater than $25 million, derive at least half their annual revenue from sales of personal information, or receive or share/sell personal information of 50,000 or more California residents (usually defined as a state taxpayer).

Notably, the CCPA contains a "right to deletion," which enables consumers to request that the institution delete any and all information collected. However, this requirement is preempted to the extent that FERPA (a federal law) requires

institutions which receive federal financial assistance collect, store, and disclose certain data. This means that institutions will need to assess what data they must necessarily store to comply with federal law. They will also need to determine what personal information they or their third-party vendors collect that is subject to erasure and other rights provided to California residents by the CCPA.

Other State Laws

In recent years, over 40 states have enacted laws governing how schools and their service providers collect, use, and protect student data.[16] Most of these laws solely cover K-12 student data, but some also govern how public and private higher education institutions use student data. For example, a Louisiana law covering both public K-12 and higher education institutions requires, among other things, deletion of personal data collected during the application process, and a prohibition on certain student analytics.[17] A few state laws, however, have been drafted solely to address higher education privacy and security, including a Virginia law which prohibits higher education institutions from requiring a student to disclose the log-on credentials of personal social media accounts.[18]

There are other general privacy laws that some states have enacted, such as data breach notification laws, that may also have privacy and security implications for educational institutions and the ed tech vendors they contract with in the course of providing online education.

Europe's General Data Protection Regulation (GDPR)

Europe's General Data Protection Regulation (GDPR) is a legal privacy framework adopted in 2018 that sets guidelines for collection and processing of personal information from individuals living in the European Union (EU). Higher education institutions may also need to comply with the privacy provisions in Europe's GDPR[19] if they provide online classes to individuals in the EU. Compliance may also be required if they accept applications from EU residents, have study abroad programs in the EU, interact with EU-based alumni, or collect or use data about EU residents. All of the personal data processed in providing an online course is subject to GDPR compliance. The GDPR provides rights and imposes restrictions on data processing under principles of purpose limitation and data minimization that require additional safeguards above and beyond what FERPA requires. For example, GDPR's definition of "personal data" is broader than FERPA, requiring protection of additional information such as IP addresses. These, and other GDPR-specific stipulations would need to be detailed in ed-tech vendor contracts that involve collecting data to ensure that GDPR requirements are being met on behalf of the institution.

Distance Learning Technologies

Higher education has slowly and steadily adopted distance learning over the past two decades. By the fall of 2018, 35 percent of all postsecondary students were enrolled in distance learning classes,[20] and just prior to the pandemic, 88 percent of all postsecondary institutions offered at least some completely online courses.[21] The technologies for providing remote learning have rapidly grown and transformed. There are now a multitude of ed tech tools used in higher education online programs: learning management systems like Canvas and Blackboard, lecture capture software such as Kalture, video conferencing platforms such as Zoom and WebEx, online exam proctoring tools such as ProctorU, and many others. Some schools also choose to outsource the partial or full provision of their distance learning programs to companies known as online program managers (OPMs). The following section provides an overview of the main technologies used for online learning and the privacy concerns they pose.

Learning Management Systems

Initially introduced in the late 1990s, learning management systems (LMSs) have become the central technology tool for colleges in creating, distributing, and managing educational content. They have seen a rapid transformation from their beginnings as simple web pages and content libraries, and they now provide a number of tools for course organization and delivery, collaborative interaction, measuring and assessing student learning, and other functions. In recent years, the LMS market has moved away from in-house LMSs to cloud-based solutions provided by companies such as Canvas.

In the past, many schools mainly used LMSs to support and supplement in-person classes, providing the ability to create structured course content, access reading materials, and administer quizzes, among other functions. LMSs are now often used for hybrid and remote learning as well. Most LMSs have functionality for providing virtual classrooms and online learning through various integrated tools. Many universities have leaned more heavily on these functions of their LMS platforms with the shift to online learning caused by the COVID-19 pandemic.[22]

LMSs, with their host of applications, often serve as large repositories of student data that institutions can use for analytic purposes. Increased remote learning will add new volumes of video and learning data captured in the course of online classes. As data continues to amass in LMSs, privacy risks increase, both from the potential for data breaches and the potential for misuse of data. Concerns have also been raised about what happens to these troves of data when LMS companies are sold.[23]

Videoconferencing

Videoconferencing tools are often essential to remote learning, enabling live classes and allowing students and teachers to communicate and collaborate virtually. Most LMSs have integrated videoconferencing capabilities,[24] but Zoom and other videoconferencing platforms are frequently being used as separate, supplemental tools during the pandemic as well.[25]

Video streams and recordings (as well as audio) from online learning may be considered education records under FERPA in certain circumstances. The video needs to be directly related to a student. This includes classes and other educational situations where students are on video asking questions, making presentations, or appearing in any other way that would make it possible to personally identify the student. This can be simply attending a videoconferenced class with the camera on.[26]

Video from classes are often recorded and saved so they can be rewatched by students later. This means that missteps, embarrassing moments, and other video data that students may not want others to see can be collected and stored. Turning on the camera for remote classes also means virtually allowing others into a student's home.[27] A great number of personal details can often be gleaned through the presence of other people, personal objects, photographs, and calendars. Without proper security and privacy controls, other parties could potentially access these recordings.

Students from high-risk populations, including undocumented immigrants, may face immediate threats to their safety as a result of images, videos, and other information collected in online classes. For example, remote students who are citizens of countries with censorship laws may face prosecution for comments made in online classes.[28] In addition to students, family members, and friends who happen to be captured on video (or audio) during a student's class could also potentially be at risk.

While FERPA does protect against sharing of video educational records with law enforcement without consent, there are exceptions. The "law enforcement" exception relates to records and surveillance video maintained by the school's "law enforcement unit" (those designated to monitor the safety of the school and enforce laws).[29] Under FERPA, these records are not considered educational records and can be disclosed without consent to law enforcement. Video data from online learning, while considered an education record under FERPA, may be disclosed to law enforcement only in the event of a "health or safety emergency"[30] or by judicial order or subpoena.[31] However, videos of online classes usually include images of multiple students, creating concerns that law enforcement could potentially misuse this data should they gain access to it, targeting vulnerable populations. This could possibly be done by mining videos using facial recognition tools.

In addition to the privacy risks from school or law enforcement access, entrance to live videoconferences by uninvited individuals is a high-profile problem that became apparent in the early days of the COVID-19 outbreak. Unauthorized entries into meetings and classes were frequently made by individuals, often for the purpose of disruption.[32] The prevalence of this occurring on Zoom popularized the term "Zoom-bombing."[33] Increased awareness of this issue has led to better security practices in using videoconferencing tools. Platforms have improved safeguards and security options, and users have learned to configure settings to make meetings more secure through password requirements, restricting screen sharing to host only, creating waiting rooms for new participants, and other changes. However, Zoom-bombing still remains a problem for schools.[34]

Online Program Management Companies

Creating a distance learning program has large costs in up-front development, data storage, and maintenance that many institutions do not want to take on themselves. Some colleges thus choose to outsource creating and administering their online learning courses to third-party contractors known as online program management companies (OPMs). As online learning continues during the pandemic and beyond, more and more schools will likely consider partnering with an OPM.[35]

Many OPMs provide a bundle of services that go beyond the implementation of online learning technology. They can also handle marketing, recruitment, and retention services for institutions. While some OPM contracts are fee-for-service based, others are revenue-based. Revenue-based agreements provide OPMs with sizable financial incentives to enroll students, as they often receive half or more of tuition revenue.[36] As OPMs serve multiple online college programs, personal information from student applications can be repurposed for marketing, raising potential privacy concerns. Contracts can permit student application information from one school to be used by the OPM to market another school to students that the OPM provides services for (and thus may have a financial incentive in increasing enrollment for). The value of this data to OPMs can be significant. In 2014, OPM 2U paid the University of California-Berkeley $4.2 million to use data from student applicants to market another school to those students.[37]

Institutions are facing increasing pressure from the higher education policy community to be more transparent about the terms of their relationships with OPMs,[38] including clarity about data privacy. A recent analysis of public colleges' contracts with OPMs conducted by the Century Foundation found that 32 percent had "vague and/or no protections on the use of students' data and information."[39] Schools often omit any mention of the role of OPMs in their online programs,

much less clear details of the privacy protections implemented under their auspices.[40]

Remote Proctoring

With an inability to have in-person exams during the shift to online learning, college use of remote proctoring software and services, like Proctorio and Examity, has surged.[41] These tools can work within existing LMSs, or as a stand-alone service.[42]

Proctoring tools can be invasive and capture large amounts of data. Audio and video of the student and the environment the student is taking the exam in is recorded, eye movements are tracked, mouse movements and other computer activity are recorded, and proctors can remotely access and control the student's computer.[43] Proctoring has become increasingly automated, requiring little human involvement. Facial recognition can be used to help authenticate the student's identity. The system then monitors the test taker for the duration of the exam, flagging suspicious or abnormal test-taking behaviors using advanced analytics.

If not fully automated, and a human proctor is required, remote proctoring is ordinarily done from an office, where supervisors can monitor the actions of the proctors. The lockdowns due to the COVID-19 pandemic, however, have forced many companies to allow their proctors to work remotely, raising additional privacy concerns regarding the lack of oversight of proctor behavior.[44]

When an online proctored test begins, students are usually required to show photo identification to their laptop camera.[45] Depending on the ID used, the proctor collects data such as name, signature, address, driver's license number, and passport number. Breaches or misuse of identification data that include citizenship or national origin information raise privacy concerns for both undocumented students and other groups at risk of discrimination, persecution, or law enforcement actions based on this information.

Like videoconferencing, there are many opportunities beyond the direct recording of the student for privacy leaks through objects in the test taker's environment that the camera may capture. The risk is greater in certain ways, as remote proctoring often requires the test taker to begin by showing the entire room that the test is being taken in. Also, unlike remote classes, where a student has the option of turning their camera off, during a remote proctored exam students must leave their camera on and stay in front of the camera for the full duration. Given that test taking can be a high-stress situation, embarrassing moments may be captured.[46]

Mobile Applications

Almost all LMS platforms have some ability to track the learning activity of students. Schools' primary stated aim of this tracking is to improve student retention and graduation rates. However, colleges are also increasingly tracking where students go. Institutions use students' phones to collect data on their location, citing a number of purposes, including monitoring attendance and tardiness,[47] mental health,[48] and for campus safety.[49] Many institutions have increased tracking for COVID-19 tracing purposes, sometimes through required downloads of tracking apps.[50] Some schools have also considered the use of wearable health monitoring devices.[51] Using technology for contact tracing may have benefits in expanding traditional manual tracing systems and providing rapid alerts to potentially exposed individuals, but it raises a number of privacy and civil liberties concerns.[52]

While schools mainly use networks of Bluetooth transmitters and wireless access points on campus to collect location information on students, with the continuing pandemic there may be an increased desire to track both on-campus and hybrid learning students—not only when they are on campus, but as they leave to go home or otherwise go off campus. While direct tracking by the institution is less of a concern with fully remote students, who are not required to use special tracking apps or devices during the pandemic, mobile apps may still be collecting GPS location data. Some schools have their own mobile apps[53] that provide campus-based maps and information, but may be used by remote students as well to access grades, class schedules, and other information, and thus schools could still potentially track these remote students' location. LMSs can include mobile apps as well that allow students to access educational materials and participate in online classes and class discussions. These and other third-party ed tech apps may collect location data, either for potential use by the institution or for marketing and advertising purposes.[54]

Predictive Analytics

Predictive analytics is the analysis of current and historical data through various statistical means and data mining tools to make predictions about future events. Higher education uses predictive analytics for a number of purposes, including identifying students most in need of advising services, developing adaptive and personalized learning programs, and managing enrollment and retention. In the past it was an involved process to export data from LMSs for analysis, but current LMS technologies often integrate data extraction and analytic tools.

Institutions are understandably interested in how students are adapting to the increased use of online learning. A poll conducted by EDUCAUSE in May 2020 found that demand from college administrators for analytics on student success increased 66 percent since the start of the pandemic.[55] The largest increase in

demand for data was for information related to students' usage of technology tools.[56]

The desire to make analytics increasingly precise creates an incentive for schools to collect greater amounts and more types of data, leading to surveilling students not only more intensely while learning, but also outside of a learning environment, for instance seeing how often students visit the library or a gym.[57] Analytics providers are also now beginning to use machine learning and other artificial intelligence approaches. These often require very large volumes of data to train the algorithms used, increasing the potential privacy harms of breaches. There is also concern that predictive analytics efforts will have a larger privacy impact on low-income students and students of color, groups that tend to have a higher percentage of the at-risk student populations that predictive analytics focuses on.[58]

Privacy Policies and Practices

Data Minimization and Retention

Declining costs of cloud storage have made it easier and cheaper to store data, and educational technology continues to enable greater ways to collect more and more data. This creates incentives for both institutions and ed tech providers to amass data for refining analytic tools and for potential use in future applications. The more prevalent use of remote instructional tools and services due to the pandemic will add increasing amounts of video, experiential learning and testing data, and other information about students collected in online learning environments that will be of potential value for colleges.

FERPA does not provide any specific requirements for minimizing the amount of data collected, or for retention or deletion of data, other than mandating that institutions retain records for compliance with any legal or policy requirements, such as an outstanding request for inspection. Schools may retain some data, such as student transcripts, indefinitely. However, when schools disclose PII to ed tech vendors, the FERPA requirement that the vendor protect the PII from unauthorized disclosure implies adequate destruction of data when no longer needed per Department of Education interpretation and guidance.[59] FERPA does not explicitly require institutions to establish any policies for data retention and deletion. It only specifies that when institutions choose to delete PII, they must use "reasonable methods." FERPA, however, does not provide details on such methods. Deletion may mean the overwriting or destruction of data using various means, but can also mean removal of PII through de-identification. De-identified information from education records is not subject to any further deletion requirements as, by definition, it is no longer PII under FERPA.

De-identification of data is the process of altering data, such as by removing or obscuring PII, to prevent it from being used to identify a person. De-identified data may be shared under FERPA without consent, and with any third party.[60] FERPA's requirement for successful de-identification is "a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information."[61] While FERPA does not specify methods for de-identification, the Department of Education's Privacy Technical Assistance Center has released some definitions of de-identification techniques and guidance.[62]

When organizations, including higher education institutions, share data with third parties, they often rely on de-identification as a privacy protection. However, in recent years, de-identification of data has been shown to be

problematic through studies demonstrating the ability to match anonymized data back to an individual ("re-identification").[63] Re-identification is often done using external databases to infer information about the anonymized data (known as linkage attacks). FERPA's standard of reasonably available information presents a challenge. It is difficult to assess what information someone may be able to use in any given re-identification attack. Anonymized datasets also cannot be taken back once released, so even if data is effectively de-identified based on current standards, future techniques and newly available information could remove those protections.

Ideally, institutions should have someone with data privacy expertise assess the techniques that they or their vendors are using to anonymize data, what other controls are in place, and whether the risks of re-identification are low enough. They should also be forward looking—taking advantage of new privacy technologies for anonymization as they become available. Differential privacy has emerged as one of the most promising de-identification techniques, as it can provide formal, mathematical assurances of privacy. Private companies such as Apple are using differential privacy, as is the Census Bureau for the 2020 Census.[64]

To fully protect students' privacy, institutions and their ed tech providers need to do more than comply with the bare minimum protections required by law. This should start with minimizing the amount of data they retain in the first place by only collecting data that has clear and necessary uses and developing policies for keeping that data only as long as it is needed. This includes clearly detailing what video and other online learning related data will be stored, and for how long.

Privacy Policies and Data Use

As colleges pass data privacy obligations on to vendors and partners in the provision of online learning, schools ultimately remain responsible for protecting students. As a first-order concern, schools should ensure that the distance learning technologies they use are compliant with FERPA and other laws as applicable. With the COVID-19 pandemic, technology companies have more frequently posted information about their products and privacy policies that explain how their use of student data complies with FERPA.[65] This may provide only part of the privacy picture, however. The detailed, full privacy policies of ed tech companies can be looked to in assessing actual privacy practices. Unfortunately, privacy policies are often lengthy, filled with jargon and legalese, and difficult to understand.[66] How companies will protect data privacy in practice is often hard to assess.

In the K-12 context, there has been some progress in holding ed tech companies accountable through tools such as Common Sense Media's privacy reviews of ed tech apps[67] and the Future of Privacy Forum and the Software & Information

Industry Association's Privacy Pledge,[68] a signed code of conduct for ed tech vendors. The FTC can bring civil enforcement actions against companies that sign the pledge and do not adhere to the commitments it outlines. While this pledge is targeted toward companies that provide ed tech designed for K-12 institutions, it includes signatories such as Blackboard and Canvas that provide their same platforms and tools with modifications for higher education as well.

While students and teaching faculty should carefully review the privacy policies of any remote learning ed tech they are considering using (or OPMs they are considering partnering with), assessing privacy policies should only be a first step for institutions. Schools need to fully understand what technical and administrative protections for data are in place, and ensure that ed tech companies meet both the requirements of the institution's stated privacy practices and their system security plan to ensure privacy is protected in all phases of data collection, use, and storage. Both privacy policies and vendor contracts should, at minimum, include terms covering what data will be stored, limitations on the use of data, how data will be protected, and when and how data will be deleted. There should be clear and transparent answers to questions about a company's data use practices: whether data is being used in secondary ways, especially uses other than the ways in which it is being explicitly used for; if any data being shared with third parties, and if so, for what purposes; whether data is being used to build any sort of profile on students, and if this profile is for non-primary or non-explicit uses; and under what terms and conditions data is shared with the government and with law enforcement. There should also be clear limits on data collection. Schools should ensure that the vendors they contract with minimize the amount of data they collect, only gathering and retaining information that has necessary, clearly stated purposes.

Institutions should also keep in mind that FERPA and other privacy laws provide a floor for privacy protection, not a ceiling. They can, and should, act in the best interests of their students and use their power as the customers of ed tech companies to enhance overall privacy. For example, unless institutions take steps to prohibit the practice, there is a risk that ed tech companies will seek to monetize student behavioral data as a funding stream, leading to extended surveillance of students' learning experiences.[69]

Conclusion

The COVID-19 pandemic presents unique challenges to students, faculty, and staff of colleges in forcing an unprecedented move to online course delivery and learning. To aid in the pandemic-led shift to online classes, a wide number of technology companies have offered free or discounted tools for distance learning. Many colleges quickly adopted new ed tech and made short-term contracts and agreements with vendors; faculty often cobbled together various tools and apps themselves to continue their classes virtually.[70] As online learning continues through the pandemic, it may lead to a longer-term shift to distance learning in higher education. However, as outlined in this paper, there are a number of privacy considerations and vulnerabilities in online learning that institutions should address.

Both institutions and ed tech companies need to be clearer about their policies and practices for collecting and using student data. A lack of transparency has been a particular problem in aspects of higher education online learning. Relationships between schools and OPMs are often unclear, including terms of data use and protections.[71] And there is often little transparency into how video and other data captured during online classes and proctoring of online exams will be used, who will be able to view it, and how securely and for how long it will be stored.[72] While it is perhaps understandable that colleges needed to quickly pivot to remote learning as the pandemic began, now is the time to ensure the technologies being used are protecting the privacy of student data. Schools may not only need to update their privacy policies and vendor contracts, but also their own privacy practices and principles to reflect increased reliance on online learning and new data sharing and data integration practices.

Notes

1 Richard Garrett, et al., *CHLOE 5: The Pivot to Remote Teaching in Spring 2020 and Its Impact, The Changing Landscape of Online Education*, 2020. https://encoura.org/project/chloe-5-the-pivot-to-remote-teaching-in-spring-2020-and-its-impact/

2 *The Chronicle of Higher Education*, "Here's Our List of Colleges' Reopening Models", https://www.chronicle.com/article/heres-a-list-of-colleges-plans-for-reopening-in-the-fall/

3 Frida Alim et al, *Spying on Students: School Issued-Devices and Student Privacy,* April 13, 2017. https://www.eff.org/wp/school-issued-devices-and-student-privacy

4 Todd Feathers, "Schools Spy on Kids to Prevent Shootings, But There's No Evidence It Works", *Vice,* December 4, 2019. https://www.vice.com/en_us/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works

5 A leading higher education nonprofit association focused on information technology issues.

6 Susan Grajek and the 2017–2018 EDUCAUSE IT Issues Panel, "Top 10 IT Issues, 2018: The Remaking of Higher Education", *EDUCAUSE Review*, January 29, 2018. https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education

7 Manuela Ekowo and Iris Palmer, *The Promise and Peril of Predictive Analytics in Higher Education: A Landscape Analysis*, New America, October 2016, https://www.newamerica.org/education-policy/policy-papers/promise-and-peril-predictive-analytics-higher-education/

8 Sophie Quinton and National Journal, "Are Colleges Invading Their Students' Privacy?", The Atlantic, April 6, 2015, https://www.theatlantic.com/education/archive/2015/04/is-big-brothers-eye-on-campus/389643/

9 Higher education lacks the additional notice and consent requirements of the Children's Online Privacy Protection Act (COPPA). COPPA generally requires companies collecting personal information online from children under age 13 to provide certain notices of their practices and obtain parental consent. However, schools can consent on behalf of parents to the collection of student data if the data is used solely for school-authorized educational purposes; https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

10 "Personally Identifiable Information for Education Records", U.S. Department of Education, accessed September 25, 2020, https://studentprivacy.ed.gov/content/personally-identifiable-information-education-records

11 See the discussion of de-identification below.

12 "Who Is A 'School Official' Under FERPA?", U.S. Department of Education, accessed September 25, 2020, https://studentprivacy.ed.gov/faq/who-"school-official"-under-ferpa

13 *California Consumer Privacy Act*. https://www.congress.gov/bill/106th-congress/senate-bill/900/text

14 Office of Management and Budget, *2019 Compliance Supplement*, July 1, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/07/2-CFR_Part-200_Appendix-XI_Compliance-Supplement_2019_FINAL_07.01.19.pdf

15 *California Consumer Privacy Act of 2018,* Cal. Civ. Code §§ 1798.100–1798.199, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

16 Future of Privacy Forum, *State Student Privacy La ws* (accessed August 20, 2020). https://studentprivacycompass.org/state-laws/

17 House Bill 718 (HB718), Louisiana State Legislature, La. Civ. Code §§ 17:3914, https://legiscan.com/LA/text/HB718/2015

18 Senate Bill 438 (SB438), Virginia State Legislature, Va. Civ. Code §§ 23-2.1:3, https://lis.virginia.gov/cgi-bin/legp604.exe?ses=161&typ=bil&val=SB438&submit=GO&ses=161&typ=bil&val=SB438&submit=GO

19 European Union. *Complete Guide to GDPR Compliance*, accessed September 1, 2020, https://gdpr.eu/

20 "Fast Facts: Distance Learning", *National Center for Education Statistics*, accessed September 3, 2020, https://nces.ed.gov/FastFacts/display.asp?id=80

21 D. Christopher Brooks, Susan Grajek and Leah Lang, "Institutional Readiness to Adopt Fully Remote Learning", EDUCAUSE, April 9, 2020, https://er.educause.edu/blogs/2020/4/institutional-readiness-to-adopt-fully-remote-learning

22 Richard Garrett, et al., *CHLOE 5: The Pivot to Remote Teaching in Spring 2020 and Its Impact, The Changing Landscape of Online Education*, 2020. https://encoura.org/project/chloe-5-the-pivot-to-remote-teaching-in-spring-2020-and-its-impact/

23 Jeffrey R. Young, "As Instructure Changes Ownership, Academics Worry Whether Student Data Will Be Protected", *EdSurge*, March 17, 2020, https://www.edsurge.com/news/2020-01-17-as-instructure-changes-ownership-academics-worry-whether-student-data-will-be-protected

24 Via open-source tools such as BigBlueButton, or through commercial videoconferencing platforms like Microsoft Teams, and Google Meet.

25 Richard Garrett, et al., *CHLOE 5: The Pivot to Remote Teaching in Spring 2020 and Its Impact, The Changing Landscape of Online Education*, 2020. https://encoura.org/project/chloe-5-the-pivot-to-remote-teaching-in-spring-2020-and-its-impact/

26 "When is a photo or video of a student an education record under FERPA?", U.S. Department of Education, accessed September 8, 2020, https://studentprivacy.ed.gov/faq/when-photo-or-video-student-education-record-under-ferpa

27 Instructors face this as well.

28 Karin Fischer, "Instruction Under Surveillance", *Chronicle of Higher Education*, September 30, 2020, https://www.chronicle.com/article/instruction-under-surveillance

29 "What Is A 'Law Enforcement Unit' Under FERPA?", U.S. Department of Education, accessed September 30, 2020, http://studentprivacy.ed.gov/faq/what-"law-enforcement-unit"

30 Schools are required to record "the articulable and significant threat" that formed the basis for the disclosure, and the parties to whom the information was disclosed. See "What Does "Articulable And Significant Threat" Mean?", U.S. Department of Education, accessed September 29, 2020. https://studentprivacy.ed.gov/faq/what-does-%E2%80%9Carticulable-and-significant-threat%E2%80%9D-mean

31 "FAQs on Photos and Videos under FERPA", U.S. Department of Education, accessed September 29, 2020, https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa

32 Tony Wan, "Holding Class on Zoom? Beware of These Hacks, Hijinks and Hazards", *EdSurge*, March 27, 2020. https://www.edsurge.com/news/2020-03-27-holding-class-on-zoom-beware-of-these-hacks-hijinks-and-hazards

33 Taylor Lorenz and Davey Alba, "'Zoombombing' Becomes a Dangerous Organized Effort", *New York Times*, April 3, 2020, https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

34 Alex Wigglesworth, "UCLA investigates 'Zoom-bombing' attacks during online classes", *Los Angeles Times*, October 10, 2020. https://www.latimes.com/california/story/2020-10-10/ucla-zoom-bombing-attacks

35 Alejandra Acosta, Clare McCann, Iris Palmer, *Considering an Online Program Management (OPM) Contract*, New America, September 15, 2020. https://www.newamerica.org/education-policy/reports/considering-online-program-management-opm-contract/

36 Stephanie Hall and Taela Dudley, *Dear Colleges: Take Control of Your Online Courses* (New York: The Century Foundation, September 12, 2019). https://tcf.org/content/about-tcf/tcf-analysis-70-university-opm-contracts-reveals-increasing-risks-students-public-education/

37 Margaret Mattes, *The Private Side of Public Higher Education* (New York: The Century Foundation, August 7, 2017). https://tcf.org/content/report/private-side-public-higher-education/?agreed=1

38 Kevin Carey, "The Creeping Capitalist Takeover of Higher Education," *Highline*, April 1, 2019, https://www.huffpost.com/highline/article/capitalist-takeover-college

39 Stephanie Hall and Taela Dudley, *Dear Colleges: Take Control of Your Online Courses* (New York: The Century Foundation, September 12, 2019). https://tcf.org/content/about-tcf/tcf-analysis-70-university-opm-contracts-reveals-increasing-risks-students-public-education/

40 Kevin Carey, "The Creeping Capitalist Takeover of Higher Education," *Highline*, April 1, 2019, https://www.huffpost.com/highline/article/capitalist-takeover-college

41 Colleen Flaherty, "Big Proctor", *Inside HIgher Ed*, May 11, 2020 https://www.insidehighered.com/news/2020/05/11/online-proctoring-surging-during-covid-19

42 And some schools simply use Zoom or other videoconferencing platforms for proctoring purposes. See Susan Grajek, " EDUCAUSE COVID-19 QuickPoll Results: Grading and Proctoring", *EDUCAUSE REVIEW,* April 10, 2020, https://er.educause.edu/blogs/2020/4/educause-covid-19-quickpoll-results-grading-and-proctoring

43 Monica Chin, "Exam Anxiety: How Remote Test-proctoring Is Creeping Students Out", *The Verge*, April 29, 2020, https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education ; And also limit the student's online access to specific IP addresses, prevent switching windows or accessing any other application, and block functions such as copying and pasting.

44 Drew Harwell, "Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance", April 1, 2020, Washington Post, https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/

45 Identity management tools may be used in conjunction with proctoring software to further verify that the student taking the exam is the one who's actually enrolled. Some of these tools use public records and other databases to cull identity questions relating to residential history and other characteristics that only the enrolled student would know.

46 Such as getting sick on camera, as per the story related in Harwell April 1, 2020 article.

47 Mará Rose Williams And Souichi Terada, "Invasive Or Helpful? Mu Using Students' Phones To Track If They Are In Class Or Not", *Kansas City Star*, January 21, 2020, https://www.kansascity.com/news/state/missouri/article239139523.html

48 Drew Harwell, "Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands", *Washington Post*, December 24, 2019, https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/

49 Douglas Belkin, "No Place to Hide: Colleges Track Students, Everywhere", *Wall Street Journal*, March 5, 2020, https://www.wsj.com/articles/the-many-ways-college-students-may-be-tracked-on-campus-11583354852

50 Kate Cox, "College Contact-tracing App Readily Leaked Personal Data, Report Finds", *Ars Technica*, August 20, 2020, https://arstechnica.com/tech-policy/2020/08/college-contact-tracing-app-readily-leaked-personal-data-report-finds

51 Lilah Burke, "Monitoring Vital Signs for COVID-19", *Inside Higher Ed*, August 11, 2020, https://www.insidehighered.com/news/2020/08/11/university-use-wearable-tech-track-covid-campus ; Of more relevance for on-campus or hybrid students, FERPA's "health or safety emergency" exception may allow disclosure of health related data without consent.

52 Koustubh "K.J." Bagchi, et al., *Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns*, Edmond J. Safra Center for Ethics, July 2, 2020. https://www.newamerica.org/oti/policy-papers/digital-tools-covid-19-contact-tracing-identifying-and-mitigating-equity-privacy-and-civil-liberties-concerns/

53 https://www.osu.edu/downloads/apps/ohio-state-app.html

54 Alfred Ng, "Education Apps Are Sending Your Location Data And Personal Info To Advertisers", *CNET*, September 1, 2020, https://www.cnet.com/news/education-apps-are-sending-your-location-data-and-personal-info-to-advertisers/

55 Kim Arnold, et al., "EDUCAUSE COVID-19 QuickPoll Results: Student Success Analytics", *EDUCAUSE*, May 28, 2020, https://er.educause.edu/blogs/2020/5/educause-covid-19-quickpoll-results-student-success-analytics

56 Kim Arnold, et al., "EDUCAUSE COVID-19 QuickPoll Results: Student Success Analytics", *EDUCAUSE*, May 28, 2020, https://er.educause.edu/blogs/2020/5/educause-covid-19-quickpoll-results-student-success-analytics

57 Drew Harwell, "Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands", *Washington Post*, December 24, 2019, https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/

58 Jeffrey R. Young, "Researchers Raise Concerns About Algorithmic Bias in Online Course Tools", EdSurge, June 26, 2020, https://www.edsurge.com/news/2020-06-26-researchers-raise-concerns-about-algorithmic-bias-in-online-course-tools ; Christine Bannan and Margerite Blase, *Automated Intrusion, Systemic Discrimination*, New America, October 8, 2020, https://www.newamerica.org/oti/reports/automated-intrusion-systemic-discrimination/

59 "Best Practices for Data Destruction", U.S. Department of Education, March 2019, https://studentprivacy.ed.gov/resources/best-practices-data-destruction

60 "Data De-identification: An Overview of Basic Terms", U.S. Department of Education, May 2013, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms.pdf ; Electronic Code of Federal Regulations: Title 34, Part 99--Family Educational Rights and Privacy, accessed September

16, 2020, https://www2.ed.gov/policy/gen/reg/ferpa/index.html

61 Electronic Code of Federal Regulations: Title 34, Part 99--Family Educational Rights and Privacy

62 "Data De-identification: An Overview of Basic Terms", U.S. Department of Education, May 2013, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms.pdf

63 Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review* 57 (August 2010): 1701-1777. https://www.uclalawreview.org/pdf/57-6-3.pdf

64 Chris Sadler, *Protecting Privacy in Data Releases: A Primer on Disclosure Limitation*, New America, February 24, 2020, https://www.newamerica.org/oti/reports/primer-disclosure-limitation/

65 See for instance, "FERPA Guide", Zoom, October 2020, https://zoom.us/docs/doc/FERPA%20Guide.pdf

66 Kevin Litman-Navarro, "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster", New York Times, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

67 "Ed Tech Reviews," Common Sense Education, accessed September 15, 2019, https://www.commonsense.org/education/search?contentType=reviews

68 Future of Privacy Forum and The Software and the Information Industry Association, *Student Privacy Pledge, 2020.* https://studentprivacypledge.org/

69 Alfred Ng, "Education Apps Are Sending Your Location Data And Personal Info To Advertisers", *CNET*, September 1, 2020, https://www.cnet.com/news/education-apps-are-sending-your-location-data-and-personal-info-to-advertisers/

70 Manisha Aggarwal-Schifellite, "Early responses indicate shift to online classes going well overall", *The Harvard Gazette*, March 26, 2020, https://news.harvard.edu/gazette/story/2020/03/professors-learn-to-adapt-and-innovate-with-online-classes/

71 Dian Schaffhauser, "2U Calls for Transparency in Online Program Management", *Campus Technology*, September 12, 2019, https://campustechnology.com/articles/2019/09/12/2u-calls-for-transparency-in-online-program-management.aspx

72 Rebecca Heilweil, "Paranoia about cheating is making online education terrible for everyone", *Recode*, May 4, 2020, https://www.vox.com/recode/2020/5/4/21241062/schools-cheating-proctorio-artificial-intelligence

NEW AMERICA