2023

The Importance of Data Privacy and Security During Emergency Remote Learning

Emma Antobam-Ntekudzi

The Importance of Data Privacy and Security During Emergency Remote Learning

EMMA ANTOBAM-NTEKUDZI

The COVID-19 pandemic forever changed the world. The virus' rapid spread forced federal and local governments to enact quarantine mandates. On March 11, 2020, the Center for Disease Control and Prevention (CDC) (2022) announced COVID-19 as a pandemic. Two days later the United States declared an official nationwide emergency. Institutions were required to shut down and persons deemed non-essential participated in quarantine. Remote working became the standard, thus affecting all aspects of individual lives and institutions, especially education. Primarily in-person universities and colleges across the world scrambled to address the COVID-19 health concerns, comply with local shutdown rules, and attempt to continue providing an education to millions of students. Having no other option, faculty and other instructors were apprehensively thrust into the world of solely online teaching and learning (Paris et al., 2021). Instructors became resourceful in their techniques to quickly provide content online for their students. Unfortunately, this massive shift left little room to assess student information privacy and security concerns in a new non-traditional online environment. Easy-to-use and free teaching tools were adopted without these considerations. After two years, institutions can reflect on compromises made to data privacy and security in response to the COVID-19 crisis, particularly since a fully online presence opened some institutions to hacking vulnerabilities. Moving forward, students, instructors, administrators, and information technology staff should have a seat at the table when outlining privacy and security policies, during educational technology tool selection, and ensuring safe online learning.

Traditional Online Learning vs. Emergency Remote Learning

Online learning is not a new phenomenon. Prior to the pandemic, online learning existed as part of various distance learning programs (Shearer et al., 2020). For years, colleges and universities that are established as online institutions offered a modality of learning to students who preferred a remote education. It can be referred to by other names such as blended learning, mobile learning, and distributed learning (Nørgård, 2021). This form of teaching requires all aspects of a course to be available digitally. Depending on the parameters of each course, a class can be held asynchronously or synchronously. Students depend on access to technology devices to attend weekly classes, participate, and complete coursework. In this modality, face-to-face in-person engagement with classmates and/or the professor is usually non-existent. However, in-person components can be at the discretion of the instructor. Professors may meet with students during office hours in person and/or require group projects where students possibly gather in person to complete assignments. Online learning programs may include courses that follow a hybrid model, encompassing the blending of online and offline, formal, and informal (Nørgård, 2021) teaching and learning. Such established online learning programs support lifelong learning because of their flexibility for students who encounter a multitude of social and personal challenges that reduce the ability to succeed in a traditional face-to-face learning environment (Nørgård, 2021). Distance learning constituted a niche learning modality (Shearer et al., 2020) prior to the pandemic. COVID-19 brought this style of teaching and learning to the forefront where it was adopted rapidly (Kim, 2020) and under duress.

The term online learning is sometimes used to describe the kind of teaching and learning enacted in reaction to the COVID-19 pandemic. However, the rushed response, unpreparedness of instructors, and desperation of higher education institutions to resume their courses culminated in emergency remote learning (Karakaya, 2020). Traditional online learning includes established theory, pedagogy, assessment, conceptual frameworks, best practices, and defined terms (Nørgård, 2021). In addition to this, there is abundant literature on teaching and learning online (Ibacache et al.,

2021). Emergency remote learning is different because of the nature in which it arises (Karakaya, 2020). It is a temporary solution that provides an opportunity for continuity of education over a certain amount of time. Traditional online learning is not designed for provisional purposes. Understandably, the accelerated push to move everything online was not accompanied by proper support (Walsh et al., 2021). A lack of formal online teaching training for instructors accustomed to teaching predominantly in-person contributed to poor implementation of courses, particularly in the early stages of the pandemic. Limited training in universal design further weakened the quality of these online courses (Nørgård, 2021).

Teaching online was unfamiliar for a major portion of instructors (Ibacache et al., 2021) and face-to-face institutions. Some educational technology was already implemented in face-to-face classes pre-pandemic and used widely. An example of this is the learning management system (LMS) Blackboard. Unless a course was fully online prior to the pandemic, Blackboard was often used as supplemental to in-person teaching. It functioned as a central location for housing required materials, allowing for assignment submission, sharing announcements from the professor, and providing a location for communication outside of the in-person classroom. A major feature and benefit of traditional face-to-face courses remained the in-person interaction and courses were developed around the understanding of this modality. Upon COVID-19's arrival, the lack of time to train instructors did not allow for formal pedagogical teaching in online course development. Many were forced to figure out how to convert all face-to-face courses to 100% online within 24 hours. Assessments designed for in-person courses needed modification; instructors were still required to fulfill the learning outcomes of an academic department in this unfamiliar modality.

Technical Side of Security

The use of online tools to aid in the dissemination of emergency remote learning highlights the resilience and dedication of instructors during a health disaster. However, a discussion of privacy and security is necessary when educational technology or tools, not designed for education, are adopted. Instructors use educational tools adopted by the institution with the assumption they have been vetted in some form. The understanding is that a license between the vendor and institution exists. When individual instructors decide to seek and use tools not supplied by the institution, especially during an emergency, there is less chance that security and privacy outlines are investigated. For instance, cloud computing is important for online learning (Ali, 2021) and is embedded into some educational technology. Tools such as Dropbox, Google Drive, and OneDrive are popular cloud storage options used by colleges and universities. Users' personal and professional information is maintained in these spaces. This can pose a risk to security and privacy if licenses or terms of service with vendors do not provide clarity on data ownership, or they may include language that releases vendors from liabilities (Paris et al., 2021). Instructors who adopt Google Drive may not investigate the service's privacy/security policies. It is important to consider to whom the information belongs (the individual, the third-party vendor, or the institution), with whom it is shared, and what happens to the data once the contract is terminated (Gelpi, 2020). Institutions and instructors should be aware of whether the cloud vendor provides support (Dennen & Burner, 2017) in instances where data is breached.

Student Privacy

As instructors worked through emergency remote learning, the ability to create an online community in the classroom became a challenge. Some turned to well-known mobile applications such as WhatsApp to aid classroom communication, further collaborative work, and maintain engagement with the course (Tarisayi & Munyaradzi, 2021). Though such applications are familiar to students and perhaps used personally, questions should be raised regarding their security in a formal learning setting. Applications usually contain click-wrap agreements (Gelpi, 2020) that request

access to a user's contacts. It will also allow the individual the opportunity to deny or accept the application for download. Policies outlined within click-wrap terms are vague regarding the use of data or no information is provided on whether the data is destroyed (Paris et al., 2021). In addition to this, if an instructor has required students to use the application, there is no consent on the part of the student. Even with the existence of a digital agreement and request, it is in the best interest of the student to agree otherwise their success in the course could be jeopardized.

Student concerns about privacy and security may limit participation and negatively impact trust (Kim, 2020). There is little to no guaranteed protection when using free online tools. Applications and free tools are susceptible to hacking when used on unsecured devices (Kim, 2020). Information technology departments at colleges may implement firewall protections, but this primarily works when a student or instructor is on campus using the college's Wi-Fi. COVID-19 forced instructors and students to remain off-site while engaging in teaching and learning. This required the use of internet access that is likely not protected, such as data for personal devices and public or home Wi-Fi. There are varying studies that reveal differences in student perceptions of their data security. One study found that students were not concerned if professors and institutions utilized their data for research and education purposes (Vu et al., 2019). Institutions and instructors can guarantee students that they mean to use their data for approved purposes, but they cannot guarantee this is being done by third-party vendors. Regardless of student perceptions on this topic, being transparent and trying to improve privacy can impact student satisfaction (Williams et al., 2019). This applies not only to the classroom but also to college services.

The use of video conferencing tools raises concerns about not only privacy protections but also surveillance issues. Traditionally, those from marginalized groups have experienced forms of surveillance in their communities and are not usually afforded the same levels of privacy as those of dominant identities (Paris et al., 2021). Institutions that serve Black Indigenous People of Color (BIPOC) populations must be aware of how privacy intrusion can harm those from marginalized communities. Perceived surveillance can re-traumatize vulnerable students. Therefore, visitors or guests to an online class should be announced to students prior to their arrival. Instructors can impair trust when visitors are allowed into an online session and left unidentified. Instructors using the Zoom Video Communications conferencing platform must ensure protocols are in place for situations known as Zoom-bombing, where uninvited users take advantage of weak security protocols (Elmer et al., 2021). In 2020, a lawsuit filed against the Zoom Video Communications company alleged that it "sold user data to Facebook" (Brooks, 2020). The company's CEO used this opportunity to address security lapses that created an environment for Zoom-bombing to occur easily (Brooks, 2020). Since the latter half of 2020, instances of Zoom-bombing reduced due to the reaction from the company. Although, it remains important for instructors using this platform to be vigilant and make concessions with students who exercise privacy rights. Students who wish to maintain a camera-off participation style during synchronous online learning should not be penalized with a negative participation grade. Students who choose to reveal their faces on camera and full names should be provided with assurances that this identifiable information will not be exploited (Kim, 2020). Compromised student privacy can be detrimental to student learning (Vu et al., 2019).

FERPA

Institutions have the option to officially designate a widely used and necessary third-party tool, like Zoom or Blackboard. This allows the vendor access to sensitive information in a limited capacity (Gelpi, 2020). Even with the school's official designation, vendor agreements must still indicate which party receives direct control and maintenance of education records, images, and recordings. The responsibility is on the institution or instructor to ensure that an adopted educational tool is following the Family Educational Rights and Privacy Act (FERPA). FERPA, enacted in 1974 (CDC, 2018), was designed to give parents and eligible students over 18 control of their education records. It prohibits the release or disclosure of personally identifiable information without written consent, although there are some entities that can legally obtain student educational records without consent and under specific circumstances (U.S. Department of

Education, 2021). These include other schools to which a student will transfer, police authorities, disclosures in response to a subpoena, and accrediting organizations (U.S. Department of Education, 2021). FERPA provides basic guidelines for protection and is part of the conversation around ethics in data analytics in education. FERPA cannot cover all privacy and security needs, particularly when this is overlooked during an emergency. There are difficulties to creating universal policies that can address every issue (Chang, 2021). Vendor agreements/terms may gain unlawful ownership or dissemination of information via loopholes in FERPA compliance (Paris et al., 2021). The key is to move beyond FERPA compliance and understand the unique security and privacy needs of an institution's student body.

Issues of privacy violations exist outside of data interruption and vague vendor licenses. Instructors may choose to use social media tools in their courses as a way to foster a class that is more engaging and attractive. Students' familiarity with social media makes integrating the tool into coursework simple. This is helpful during emergency remote learning when students are forced into a modality they did not originally choose. Nonetheless, not all students will feel safe sharing details with instructors and classmates. The use of social media in a formal learning context can blur the lines between personal and professional (Dennen & Burner, 2017). Some students may not be willing to share, for educational purposes, details such as photos socializing or certain posts from family and friends. Allowing a professor and classmates to "follow" one's Facebook page for the duration of a course could be awkward and uncomfortable (Dennen & Burner, 2017). Students are often at the mercy of the course's requirements, and if the incorporation of social media is necessary for achievement in the course, then a student does not have a choice. Emergency remote learning removed many opportunities for students to have a say in their educational options. Instructors should be open to providing students with some agency within the course. This can encourage students to appreciate the level of control they possess despite the uncontrollable circumstances of a health crisis.

Risks with Online Tools

Ultimately, institutions must reflect on whether their delivery of emergency remote learning, which began in 2020 and continues in some form currently, complied with FERPA (Gelpi, 2020). Universities are encouraged to exercise care when choosing a tech vendor for educational purposes (Williams et al., 2019). However, the hurried response to COVID-19 forced the adoption of tools that were not originally created for educational purposes but used for the classroom. The widespread use of such tools by individual instructors did not allow for an institution to monitor the technology being implemented in each classroom. Moreover, institutions were unable to offer speedy resources to make this massive shift less stressful for instructors. Utilizing free online tools made online instruction bearable despite the risks to privacy and security. There are instances where personal data is routinely exposed while using an online tool. These include creating a user account and saving work to commercial cloud storage. Downloading browser extensions are sometimes required for an online product to function on a personal computer or laptop. This can open a device to malware which may compromise a user's data and the device itself (Varshney et al., 2018). Instructors and students using video conferencing tools allow their faces, voices, and full names to be shared and recorded without the knowledge of where a recording is stored or what happens to it after a semester concludes. Such activities, associated with free online tools, can risk exposing student and instructor data. Traditional educational technology tools are not exempt from this concern. Institutions must outline specifics when it comes to vendor agreements and terms of service to minimize the exploitation of their students and instructors. Instructors should take precautions and verify policies outlined on terms of service pages when choosing certain tools for classroom use.

Data Breaches & Lawsuits

Higher education institutions continuously faced data breaches and challenges prior to 2020. However, this increased as

emergency remote learning became the standard during the COVID-19 pandemic. Attacks to data security and privacy may come in the form of covert, deliberate theft and misuse of data from free online tools. Google is relied upon by many but remains a major data privacy and security offender. The company tracks user searches to personalize the user's experience. Google collects data and provides a limited ability for registered users to prevent the sharing of their information (Goodson, 2012). Google's suite offers a host of services used by students and instructors for both personal and professional purposes. Its ability to surveil online activity allows it to successfully sell its audience preferences to advertisers (Kang & McAllister, 2011). This strategy threatens the privacy of its users and exposes sensitive information to outside vendors. In addition to this, policies adopted focus more on maintaining Google's rights to user information (Kang & McAllister, 2011). This has led to lawsuits and settlements by the company regarding user data. In 2016, lawsuits were filed by the University of California system, specifically the Berkeley and Santa Cruz campuses, in which Google was accused of procuring student emails without consent from Google's Apps for Education suite (Riddell, 2016) and sharing them with advertisers. This case underscores the limited accountability and oversight to which Google is subjected. According to the lawsuit, Google scanned student information for years until the company formally announced that it "permanently removed all ad scanning" (Brown, 2016) from its education email service. Google continues to grow as a provider of technology in K-12 and post-secondary schools. The well-known browser Google Chrome is popular and used regularly by students and instructors. However, Google Chrome is no stranger to lawsuits that highlight the company's harvesting of data regardless of a user choosing to opt out (Nayak, 2022). As of today, Google declared a ban, beginning in late 2023, on allowing advertisers to track consumers in Chrome (Nayak 2022).

Hacking is another threat to student data. Since 2005, over 1,850 data breaches in education have been recorded nationwide, with 65% occurring in universities and colleges (Cook, 2021). Many of those breaches are the result of malware, spyware, and ransomware. All three attacks allow a third party to gain access to data (Grama, 2014) without consent and/or place data at high risk. This type of hacking can cause a myriad of serious problems for users. Stored data becomes compromised by exploiting weaknesses such as poor passwords, unsecured networks, or negligent security protocols (Beaudin, 2015). Whether the information is stored in a user account for an online tool or on an actual device, both locations are vulnerable once hacking has taken place.

Colleges and universities suffer tremendously when targeted by such mass data breaches. Institutions face monetary losses, suffer reputational consequences, and may experience reduced student enrollment (Grama, 2014). As a result of emergency remote learning during the COVID-19 pandemic, schools nationwide experienced a high number of breaches in 2020, with 2.99 million student records affected (Cook, 2021). The influx of students and instructors hurriedly working online placed more data in jeopardy. In 2020, Kansas City's Metropolitan Community College faced ransomware attacks often (Lubinski, n.d.) with the social security numbers, medical, and banking information of 630,000 former, current, and prospective students exposed (Cook, 2022). The well-known historically Black college and university (HBCU), Howard University, suffered ransomware attacks that locked its networks for days (Ngo, 2021). This forced online and hybrid classes to be canceled. The college continues to work with FBI and city officials regarding appropriate protection against cyberattacks. Unfortunately, some colleges are unable to recuperate their losses or recover altogether. Lincoln College, in Illinois, experienced a ransomware attack that took months to rectify (Holt, 2022). The COVID-19 pandemic caused severe reductions in student enrollment, recruitment, and fundraising. Consequences from the pandemic coupled with the ransomware attack overwhelmed the college. The 157-year-old institution could not survive and shut its doors on May 13, 2022 (Holt, 2022). Other institutions face security breaches from widely used online software. Stanford, the University of Colorado, the University of Miami, and the University of California system campuses Berkeley, Davis, and Los Angeles used the file-sharing program/service known as Accellion. In 2021, a data breach in the program resulted in the online publishing of student data from the aforementioned colleges (Wu & Catania, 2021).

Recommendations

Emergency remote learning should be safe. Now, in the third year of the pandemic, aspects of this type of learning continue to re-shape higher education moving forward. University students and instructors are slowly returning to a form of in-person teaching and learning. Simultaneously, a significant percentage of course offerings at various institutions may remain online for the foreseeable future. Other institutions might simply be interested in maintaining a robust online presence through growing their online courses. Since 2020, there have been trainings and guidelines developed to offer help to instructors when using specific tools adopted during the pandemic. For example, The City University of New York (CUNY) (2020) created a website primarily for instructors providing Zoom guidance to ensure security and privacy. Regarding video participation, CUNY (n.d.) has organized a chart comparing the privacy options among the four tools used with video capability: Zoom, Teams, Blackboard, and Webex. This can be helpful for instructors when deciding which video conferencing tool is best to use for their students. Beyond the institutional level, there are handbooks for online course development. The Online Consortium (2020), in partnership with the Association of Public and Land-grant Universities and Every Learner Everywhere, created a faculty playbook. Its goal is to aid instructor readiness regarding online teaching. It provides information, resources, tips, and best practices, emphasizes equity, and identifies course design components to follow. It could serve as a much welcomed handbook for instructors still learning about effectively delivering courses in an online modality.

Free, easy-to-use tech tools for education have allowed instructors to stay connected with students, especially since the start of the COVID-19 pandemic. There is an emphasis on collaboration and sharing in an online environment, but this should not be at the cost of privacy (Chang, 2021). The protection of safe learning is ensured when the student's privacy can be guaranteed. Online course development trainings can help instructors build online courses with privacy and security in mind. Instructors can incorporate privacy criteria into the syllabus and create collaborative assignments that allow anonymizing information (Chang, 2021). Transparency helps in creating trust between the instructor and students; therefore, being open about the safety protocols to students should be encouraged. Students have a right to know how their information will be used, if at all, who will see it, why it is needed, where it will be stored, and how it will be destroyed (Vu et al., 2019). Instructors should be trained in FERPA policies and learn about policies beyond that. The U.S. Department of Education's (2014) "Protecting Privacy While Using Online Educational Services: Requirements and Best Practices" document should be updated, but it remains relevant. It covers information for instructors and institutions to follow for protecting student privacy. It reminds readers to be aware of state and institutional policies and encourages caution when using click-wrap consumer applications.

Since the start of the pandemic, institutions have more cause to negotiate beneficial agreements with third-party vendors. Even if a provider is designated as a "school official", the terms of service must be specific regarding the level of control over collected information (Gelpi, 2020). Contracts should be able to ensure that information collected is stripped of identifiers (Gelpi, 2020). An agreement may outline what data is permitted for collection and compensation for the institution if the terms are breached. The ownership of personal and identifiable data should be defined with protocols in place that do not leave student information exposed when a contract is terminated (Gelpi, 2020). Agreements should include language on the destruction of student data upon the termination of a contract. At a very basic level, FERPA compliance (Paris et al., 2021) should be followed by an agreement with third-party vendors. Institutions can help instructors by periodically providing FERPA workshops and making available contracts with educational technology vendors for instructors to view. Faculty will continue to utilize easy-to-use free online tools for educational purposes. Rather than enforcing certain tools over another, institutions can create a list of teaching tools their faculty currently use, provide terms of service information for each, and offer a rating system designed to describe how well the tool indicates its protections of data and privacy. This will allow faculty to access terms of service information that might be difficult to find for some online tools. Institutions can encourage students and instructors to become involved in conversations about their privacy and security concerns, particularly in an emergency remote

learning environment. Engaging both parties will allow institutions to notice the gaps in their local policies for safety in online learning.

Incorporating Multiple Voices: Collaborative Policy Building

Creating safe learning policies in response to emergency remote learning is best conducted collaboratively. There are many individuals within higher education that should have a voice in what they would like protected. Generally, instructors, staff, and students remain in the dark regarding the privacy and security of their data. It is important for all groups affected to come together and decide what kind of privacy and security issues should be addressed beyond that which FERPA covers. Four groups are identified below as stakeholders in creating privacy and safety policies. Collaborative policy building can begin with conversations surrounding the topic. The questions below are designed to help facilitate a discussion on safety and privacy in an online environment.

1. Teaching faculty, instruction librarians, and instructional staff is a group of people who do not have the title of faculty but engage with students and create content for teaching and learning in the classroom: As facilitators and designers of courses, instructors can be made aware of the terms of service or agreements for specific tools and assess whether they are best to use or how to use them to ensure safe online learning.

a. What matters to you most in the privacy and security of education data that is personal, sensitive, and identifiable?
b. What do you know about FERPA? What do you know about the institution's data security and privacy guidelines?
c. How do you design your course with these principles in mind?
d. What are the educational technology tools that you use for your classroom?

2. Students comprise the group that is meant to be protected; therefore, including them in creating policies for online classroom privacy and safety is imperative. Students may trust the institution and instructor are making the right decisions and following FERPA policies when using third-party vendors and free online tools. Regardless of this trust, an understanding of what to identify as most important in an agreement can be helpful.

a. Have you been made aware of FERPA or the institution's guidelines regarding your rights in the classroom?
b. What are some educational tools that you have used in your classes?
c. What are some of your privacy and security concerns with those tools and with learning online?
d. How can the university help bring awareness to students about privacy protections and safe online learning?

3. Information technology department staff, specifically those in charge of educational technology tools. This group is in the best position to evaluate the privacy and security needs required of technology tools in the classroom. This group is also well-equipped to train students and instructors on understanding the importance of privacy and security protocols, FERPA guidelines, and other safeguards in online learning.

a. What are some important factors instructors and students should identify when reviewing the terms of service for a free online tool/application?
b. How might education for instructors and students on data privacy and security impact the college community?
c. What is this department's role, if any, in choosing educational tools for campus-wide use?
d. How does your department investigate and resolve data breaches or other data security issues?

4. University/College Administrators control the decision-making for the institution. This includes decisions on educational technology tools used campuswide. Administrators can support the privacy and safety concerns of

instructors and students while working with IT department representatives to create proper safety policies for the institution. Individuals in this group have access to university funds and create the campus-wide budget. Funding can be expanded to include the purchasing of effective safety mechanisms for online teaching tools used by instructors.

a. Describe the process, from beginning to end, of acquiring educational tech tools for instructor use campus-wide.
b. What are the factors that are involved in deciding to adopt an educational tool?
c. How do information privacy and safety play a role in these decisions?
d. Does the college work with outside local or state cybersecurity divisions? How would this collaboration benefit or hinder the protection of student data?
e. What campus-funded online teaching and learning professional development programs exist for instructors?

Conclusion

The scramble to place material online and continue classroom activities became a priority, with no time to consider data privacy and security protection. Universities and colleges focused on maintaining educational services for students throughout the beginning of the pandemic. Overnight, instructors were placed in challenging situations, without guidance on how to transfer all in-person classes to fully online. A few years into the pandemic and instructors have improved their online teaching, become more familiar with distance learning pedagogy, and have more resources, supported by the administration, to aid in online course development. It is time to review vendor contracts hastily accepted and investigate the terms of service for free online tools and social media adopted during the pandemic. This is a great moment for institutions to explore existing and new data privacy and security issues that have arisen with the majority of classes taking place online. Administrators, IT staff, instructors, and students have an opportunity to come together and create local policies that directly address privacy and safety. Online learning for traditionally face-to-face universities and colleges will continue while the pandemic endures. For this reason, it is important to tackle and share knowledge about data protections for students to ensure emergency remote learning is successful and safe.

References

Ali, M. B. (2021). Multi perspectives of cloud computing service adoption quality and risks in higher education. In M. Khosrow-Pour (Ed.), *Handbook of research on modern educational technologies, applications, and management* (pp. 1-19). Information Resources Management Association. http://doi.org/10.4018/978-1-7998-3476-2

Beaudin, K. (2015). College and university data breaches: Regulating higher education cybersecurity under state and federal law. *Journal of College and University Law*, 41(3), 657.

Brooks, K. J. (2020, July 17). *Zoom says it will fix security holes that video hackers have exploited.* CBS News. Retrieved August 22, 2022, from https://www.cbsnews.com/news/zoom-video-conferencing-feature-freeze-security-flaws/

Brown, E. (2021, October 27). UC-Berkeley students sue Google, alleging their emails were illegally scanned. *The Washington Post.* Retrieved August 22, 2022, from https://www.washingtonpost.com/news/grade-point/wp/2016/02/01/uc-berkeley-students-sue-google-alleging-their-emails-were-illegally-scanned/

Center for Disease Control and Prevention. (2018). *Family Educational Rights and Privacy Act (FERPA).* https://www.cdc.gov/phlp/publications/topic/ferpa.html

Center for Disease Control and Prevention. (2022). *CDC museum COVID-19 timeline.* https://www.cdc.gov/museum/timeline/covid19.html

Chang, B. (2021). Student privacy issues in online learning environments. *Distance Education*, 42(1), 55–69. https://doi.org/10.1080/01587919.2020.1869527

City University of New York. (2020). *Zoom security protocol.* https://www.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/cis/it-resources-for-remote-work-teaching/Zoom-Security-Protocol.pdf

City University of New York. (n.d.). *Video participation privacy options.* Remote Learning & Work. https://www.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/cis/it-resources-for-remote-work-teaching/Video-Participation-Options.pdf

Cook, S. (2022, January 21). *US schools leaked 28.6 million records in 1,851 data breaches since 2005*. Comparitech. Retrieved August 22, 2022, from https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/

Dennen, V. P., & Burner, K. J. (2017). Identity, context collapse, and Facebook use in higher education: Putting presence and privacy at odds. *Distance Education*, 38(2), 173–192. https://doi.org/10.1080/01587919.2017.1322453

Elmer, G., Neville, S. J., Burton, A., & Ward-Kimola, S. (2021). Zoombombing during a global pandemic. *Social Media + Society*, 7(3), 1–12. https://doi.org/10.1177/20563051211035356

Gelpi, A. (2020). Ensure FERPA compliance in online provider agreements. *Campus Legal Advisor*, 20(11), 1–5. https://doi.org/10.1002/cala.40272

Grama, J. (2014). *Just in time research: Data breaches in higher education.* EDUCAUSE. https://library.educause.edu/resources/2014/5/just-in-time-research-data-breaches-in-higher-education

Goodson, S. (2022, April 14). *If you're not paying for it, you become the product*. Forbes. Retrieved August 22, 2022, from https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/

Hodges, C. B., Moore, S., Lockee, B. B., Trust, T., & Bond, M. A. (2020). *The difference between emergency remote teaching and online learning*. EDUCAUSE. https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning

Holt, K. (2022, May 9). *A US college is shutting down for good following a ransomware attack*. Engadget. Retrieved August 22, 2022, from https://www.engadget.com/lincoln-college-ransomware-attack-shut-down-covid-19-164917483.html

Ibacache, K., Rybin Knoob, A., & Vance, E. (2021). Emergency remote library instruction and tech tools. *Information Technology and Libraries*, 40(2), 1–30. https://doi.org/10.6017/ital.v40i2.12751

Kang, H., & McAllister, M. P. (2011). Selling you and your clicks: Examining the audience commodification of Google. *tripleC: Communication, Capitalism & Critique*, 9(2), 141–153. https://doi.org/10.31269/triplec.v9i2.255

Karakaya, K. (2020). Design considerations in emergency remote teaching during the COVID-19 pandemic: A human-centered approach. *Educational Technology Research and Development*, 69(1), 295–299. https://doi.org/10.1007/s11423-020-09884-0

Kim, S. S. (2021). Motivators and concerns for real-time online classes: Focused on the security and privacy issues. *Interactive Learning Environments*. https://doi.org/10.1080/10494820.2020.1863232

Lubinski, A. (n.d.). MCC Kansas City victim of cyberattack. *Courier Tribune*. Retrieved August 23, 2022, from https://www.mycouriertribune.com/schools/higher_education/mcc-kansas-city-victim-of-cyberattack/article_cf9b29f2-de35-11ea-9cd8-4312b8110d16.html

Nayak, M. (2022, February 28). *All the ways Google is coming under fire over privacy: Quicktake*. Bloomberg. Retrieved August 22, 2022, from https://www.bloomberg.com/news/articles/2022-02-28/all-the-ways-google-is-coming-under-fire-over-privacy-quicktake

Ngo, M. (2021, September 7). Howard University hit by a ransomware attack. *The New York Times*. Retrieved August 22, 2022, from https://www.nytimes.com/2021/09/07/education/howard-university-ransomware.html

Nørgård, R. T. (2021). Theorising hybrid lifelong learning. *British Journal of Educational Technology*, 52(4), 1709–1723. https://doi.org/10.1111/bjet.13121

Paris, B., Reynolds, R., & McGowan, C. (2021). Sins of omission: Critical informatics perspectives on privacy in e-learning systems in higher education. *Journal of the Association for Information Science and Technology*, 73(5), 708–725. https://doi.org/10.1002/asi.24575

Riddell, R. (2016, May 18). Google sued by 890 students over unlawful data mining allegations. *Higher Ed Dive*. Retrieved August 22, 2022, from https://www.highereddive.com/news/google-sued-by-890-students-over-unlawful-data-mining-allegations/419368/

Shearer, R., Aldemir, T., Hitchcock, J., Resig, J., Driver, J., & Kohler, M. (2020). What students want: A vision of a future online learning experience grounded in distance education theory. *American Journal of Distance Education*, 34(1), 36–52. https://doi.org/10.1080/08923647.2019.1706019

Tarisayi, K. S., & Munyaradzi, E. (2021). A simple solution adopted during the Covid-19 pandemic: Using WhatsApp at a university in Zimbabwe. *Issues in Educational Research*, 31(2), 644–659.

U.S. Department of Education. (2014). *Protecting student privacy while using online educational services: Requirements and best practice*. https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

U.S. Department of Education. (2021). *Family Educational Rights and Privacy Act (FERPA)*. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Varshney, G., Bagade, S., & Sinha, S. (2018). Malicious browser extensions: A growing threat: A case study on Google Chrome: Ongoing work in progress. 2018 *International Conference on Information Networking* (ICOIN), 188–193. https://doi.org/10.1109/ICOIN.2018.8343108

Vu, P., Adkins, M., & Henderson, S. (2019). Aware, but don't really care: Student perspectives on privacy and data collection in online courses. *Journal of Open, Flexible and Distance Learning*, 23(2), 42–51.

Walsh, L. L., Arango-Caro, S., Wester, E. R., & Callis-Duehl, K. (2021). Training faculty as an institutional response to COVID-19 emergency remote teaching supported by data. *CBE–Life Sciences Education*, 20(3), ar34. https://doi.org/10.1187/cbe.20-12-0277

Williams, D., Kilburn, A., Kilburn, B., & Hammond, K. (2019). Student privacy: A key piece of the online student satisfaction puzzle. *Journal of Higher Education Theory and Practice*, 19(4), 115–120. https://doi.org/10.33423/jhetp.v19i4.2206

Wu, D. & Catania, S. (2021, April 3). Hackers leak Social Security numbers, student data in massive data breach. *The Stanford Daily*. Retrieved August 22, 2022, from https://stanforddaily.com/2021/04/01/hackers-leak-social-security-numbers-student-data-in-massive-data-breach/