Investigating the Security & Privacy Risks from Unsanctioned Technology Use by Educators

Easton Kelso
Arizona State University
Tempe, Arizona, USA
eakelso@asu.edu

Ananta Soneji
Arizona State University
Tempe, Arizona, USA
asoneji@asu.edu

Syed Zami-Ul-Haque Navid
Arizona State University
Tempe, Arizona, USA
snavid2@asu.edu

Yan Shoshitaishvili
Arizona State University
Tempe, Arizona, USA
yansho1@asu.edu

Sazzadur Rahaman
University of Arizona
Tucson, Arizona, USA
sazz@cs.arizona.edu

Rakibul Hasan
Arizona State University
Tempe, Arizona, USA
rakibul.hasan@asu.edu

Abstract

With the increasing digitization of teaching and learning activities, technology-generated data has become the target of attacks from external adversaries and abuse by technology providers. Researchers have investigated stakeholders' perceptions of security and privacy risks from technologies and how those risks are affecting institutional policies for acquiring new technologies. However, outside of institutional vetting and approval, there is a pervasive practice of using applications and devices acquired personally. It is unclear how these applications and devices affect the dynamics of the overall institutional ecosystem.

We address this gap through an online survey-based study targeting educators and administrators from K-12 and higher education institutions in the United States. Our study identified 494 unique applications used by educators, and examined the perceived and subsequent risks associated with integrating these technologies into an institution's ecosystem. The findings highlight a significant lack of privacy and security awareness among educators when selecting new tools, as well as widespread uncertainty regarding regulatory compliance. Additionally, institutional warnings and policies on unsanctioned app use appear to have limited effectiveness in changing educators' behaviors. To mitigate these challenges, we identified the need for institutions to provide clear guidelines, data privacy and security training, and vetted alternatives that meet the needs of educators while ensuring compliance. A collaborative approach between educators and administrators will be key to balancing automation and data privacy.

ACM Reference Format:
Easton Kelso, Ananta Soneji, Syed Zami-Ul-Haque Navid, Yan Shoshitaishvili, Sazzadur Rahaman, and Rakibul Hasan. 2025. Investigating the Security & Privacy Risks from Unsanctioned Technology Use by Educators. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3706599.3720254

CHI EA '25, Yokohama, Japan

ACM ISBN 979-8-4007-1395-8/25/04
https://doi.org/10.1145/3706599.3720254

1 Introduction

Technology use in the education domain, at both K-12 and higher education institutes (HEIs), has seen unprecedented growth recently, digitizing every aspect of teaching, learning, research, and administrative tasks [5, 7, 12, 24]. Simultaneously, there has been much effort from the research community to understand security and privacy risks as perceived by different stakeholders in this setting. For example, researchers investigated the factors affecting decisions to adopt tools by educators and administrators [3, 5, 21], rising security and privacy concerns of data subjects due to an increasing number of tools being deployed [2, 8, 9, 18, 25], how these tools are being audited and maintained to alleviate security and privacy risks [5, 12], as well as how institutional policies and other regulatory and computational measures aiming to minimize the use of collected data in privacy-invasive ways [10, 12, 18].

The security and privacy impacts of *unsanctioned technologies*—ones that are not institutionally procured, and thus escape auditing and are free from contractual obligations to limit data collection and use [11]—however, have not been investigated. Unsanctioned technologies may be ubiquitous as a plethora of apps and services can be used by anyone for teaching and learning-related activities, often free of cost [12]. Even paid apps in many cases can be personally acquired, for example using research grants or departmental funds, where they do not go through the institutional procurement and security audit process if the price is below a threshold [12], and thus they do not have a formal contract restricting data collection and use. This lack of a vetting process and contracts may lead to increased risks of leaking private data, as well as legal liabilities for the users or the institutions since many student records are protected under laws (such as FERPA [22]) that do not apply to other domains. Thus, investigating unsanctioned technology use in institutional settings and the associated data security and privacy issues need urgent attention.

This paper contributes to shedding light on this matter; specifically, it seeks to answer the following research questions: (1) RQ1: What unsanctioned technologies do educators (at K-12 or HEIs) use and why? (2) RQ2: How do educators perceive and experience security and privacy issues and risks of those apps and how those perceptions impact their use? and (3) RQ3: How do unsanctioned technologies impact the security and privacy posture of education institutes?

To answer these questions, we first conduct an online study ($N = 432$) involving educators at K-12 and HEIs to learn about their use of unsanctioned apps and personal devices, their perception and experience of associated security and privacy issues, their knowledge and understanding of institutional policy about unsanctioned technology use, as well as their efforts to minimize security and privacy risks. We identified 494 unique apps they use for various purposes related to teaching, learning, and research. We identify the absence of institution-provided alternatives, habituation, usability, and surprisingly, being 'forced' by school admins, among the primary reasons for unsanctioned app use. Major selection criteria they used include the apps' capacity to engage students and AI (Artificial Intelligence) features; security and privacy were rarely considered as a primary deciding factor. We also find that many participants continued to use apps despite distrusting them and even after observing privacy-invasive behaviors. Less than half of the participants knew the existence of institutional policy, and most of those who knew went against it to use unsanctioned apps.

We supplement these findings with another study surveying school administrators, IT support staff, and technology policy makers (N=24). The results concur with findings from the first survey, where admins acknowledged that educators often use unsanctioned apps and request their integration with institutional apps, which are sometimes accommodated. Participants also listed security and privacy incidents their institution faced because of unsanctioned app and device use; examples include a third-party app scraping institutional data, and increased security vulnerability due to educators forwarding emails to their private accounts.

Overall, our studies surface striking security and privacy issues, which might impact millions of students, arising from educators' unsanctioned educational technology use. We discuss the privacy, security, and compliance implications of our study results, and provide recommendations to improve this situation.

2 Related work

Technologies now manage nearly every aspect of academic activities [7, 9], with tech ecosystems constantly evolving with the availability of numerous mobile apps and extensions for other platforms (such as through marketplaces for Zoom [1] and Canvas [4]). This continuous digitization has led to security and privacy vulnerabilities: in 2023, data breaches at HEIs have cost an average of 3M USD [20].

Past research has studied the institutional use of technologies. Radway *et al.* investigated if and how universities conform to the Family Education Rights and Privacy Act (FERPA) while sharing directory information [18]. Chanenson *et al.* interviewed K-12 school officials and IT personnel to understand districts' use of technologies and how they manage student privacy and security [5]. Balash *et al.* surveyed university instructors to understand the prevalence of using online exam proctoring apps and why they are (not) adopted [3], while Shioji *et al.* investigated the same with a target audience of senior administrators [21]. Kelso *et al.* investigated how universities procure technology, their auditing process, and how they maintain institutional security posture. Paris *et al.* reported how loopholes in regulations and institutional contracts can be exploited to invade privacy [16] . However, the literature lacks studies on unsanctioned technology use and its impact on security and privacy, which is crucial for a more comprehensive understanding of educational institutes' security and privacy posture.

3 Study 1: Educator Survey

To understand the use of unsanctioned educational technologies and personal devices for teaching-related activities in education setting, we conducted an online survey from October to December 2024 targeting K-12 and HEI educators. The following sections detail the methodologies and findings of this study.

3.1 Methods

Survey design. We designed an online survey to capture the use of unsanctioned applications for teaching and grading-related activities. This survey included a mix of open-ended and multiple-choice questions, structured to gather comprehensive insights into app usage, institutional awareness, and data management practices.

After obtaining consent, participants were first asked to list at least three applications (for mobile, web browsers, or desktop computers) that they have used for teaching and grading-related activities and why. Follow-up questions explored participants' perceptions and experiences with their listed apps and their knowledge of institutional policies regarding unsanctioned application use. The survey concluded by asking participants about the data management practices of unsanctioned applications, specifically whether these apps provided the option to delete user data when discontinued and if participants had utilized this feature (full questionnaire can be found in Appendix A).

Data Collection. The survey was conducted using the Qualtrics platform [17]. We recruited participants through Prolific[1], a well-known platform for online recruitment and management of research participants. The study received Institutional Review Board (IRB) exempt status, as it posed minimal risk to participants.

Selection criteria ensured that participants were current or former educators teaching at K-12 schools, colleges, community colleges, or universities, with prior experience using unsanctioned apps for teaching, grading, or other academic activities during their tenure. Each participant was compensated $5 for completing the survey, approximately taking 10 minutes of their time.

Data analysis. After closing the survey, we cleaned and validated the data to ensure accuracy, consistency, and reliability. We then calculated descriptive statistics, such as percentages and counts, to identify key trends in participant responses to closed-ended questions.

For open-ended questions, three authors independently reviewed and systematically coded the responses, identifying major themes related to educators' motivations for using unsanctioned technologies, privacy and security concerns, and awareness of institutional policies. This multi-faceted analysis provided a structured understanding of educators' perspectives surrounding the use of unsanctioned technologies.

[1] https://www.prolific.com/

3.2 Results

3.2.1 Participants. We collected data from 450 participants and manually reviewed it to exclude 18 responses that were either autogenerated or gibberish. Autogenerated responses were identified based on the wording of answers, specifically if an answer was not in the first person perspective, or did not answer a question directly. For example, stating that "in many cases alternatives like [list of other technologies] are available." would be seen as autogenerated. This left us with 432 valid responses: 283 from K-12 educators and 149 from HEI educators. Our participants represented diverse demographics: 313 identified as female, 137 as male, and 5 as non-binary. The age distribution was as follows: 98 participants were under 30 (18–29), 269 were 30–50, and 89 were over 50. Regarding education, 18 had a high school diploma, 55 had a Bachelor's degree, 104 had a Master's degree, 23 had a doctorate, and the rest preferred not to answer. Discipline-wise, 28 participants taught STEM subjects, 290 taught non-STEM subjects, and 135 did not disclose their discipline.

3.2.2 Use of unsanctioned technology. Participants listed a total of 1,654 apps and services, with 494 being unique. Among these, participants K-12 and HEIs shared 88 applications. K-12 participants identified 284 unique apps, while HEIs identified 121 unique applications. The most popular personal use applications were Kahoot! (n=73), ChatGPT (n=69), Google Classroom (n=63), Canva (n=55), and Quizlet (n=50). For K-12 participants alone, top 3 were Google Classroom, Kahoot!, and a tie between ChatGPT and Canva, while HEI participants favored ChatGPT, Kahoot!, and Canvas.

A huge majority (n=375) stated that they use personal devices for teaching-related tasks. Among these, 114 participants used personal devices daily, while 139 used them several times a week. Moreover, 277 participants downloaded institutional documents (e.g., student data, grade books) onto personal devices. Of these, 137 reported that their devices had automatic cloud backups through personal accounts, potentially exposing institutional data to security risks.

3.2.3 Primary factors in app selection. Gamification was a key factor in app selection, with 30.4% of K-12 apps focused on helping students learn basics of reading, mathematics, and other general subjects. Classroom management tools also played a significant role among K-12 participants, comprising 12.2% of the apps. Participants emphasized their value, describing them as "a fun way to track classroom behavior" (P59) and noting they were "chosen for their ability to enhance classroom management and communication with both students and parents" (P83).

HEI educators used a range of tools, with 30.3% of their apps focused on tasks such as note-taking, sharing materials with students, and conducting research. AI-based applications made up 7.4% of their apps, reflecting the growing integration of AI in education. Educators stated that the use of AI "makes students want to learn, and motivates me" (P211) and "enhances my teaching of literature" (P210). In addition, specialized tools were commonly used, and one participant mentioned the need for apps to "shoot RAW images with a smartphone" (P151).

3.2.4 Reasons behind unsanctioned app use. In both K-12 and HEI contexts, the overwhelming majority (n = 387) mentioned "ease of use" or similar phrases as the primary reason to use unsanctioned apps, even when institutional alternatives were available. Accessibility (n = 281), student engagement (n = 279), and price (n = 212) followed closely as significant factors. Almost 70% of the participants who prioritized engagement (n = 279) were K-12 educators (n = 195), emphasizing that these apps "keep students very engaged" (P30). Familiarity with certain tools also played a role: 84 participants resisted school-provided options, noting they were accustomed to other tools due to previous careers, long-term use, and unwillingness to adapt to a new tool.

Within HEI setting, primary driver was the need for specialized tools unavailable through their institutions (n=61). Participants highlighted requirements for tasks such as "basic image editing" (P300) or accessing "reference apps for specific films and developer combinations" (P151). Research-related tools were also important, with educators seeking apps to "help with research papers" (P52) and tools for lab-specific needs, such as "coding observational data" (P37). Surprisingly, only seven participants cited "security" as a factor in their unsanctioned application choices, indicating that most respondents did not prioritize it as a primary selection criterion.

3.2.5 Security and privacy perceptions. As mentioned previously, while security and privacy were rarely top priorities in unsanctioned app selection, 218 participants acknowledged considering these issues for at least one unsanctioned app they listed, and 72 consistently evaluated security and privacy for all three apps they listed. On the other hand, a significant proportion—more than one-third (n = 176)—did not consider these aspects at all when choosing their apps. This highlights a complex relationship between perceived risks and actual behavior.

Despite limited consideration during selection, concerns about security and privacy issues emerged post-usage. 23 participants reported experiencing security or privacy breaches with at least one app, while 38 expressed concerns about apps' data collection practices potentially violating user privacy. Alarmingly, 43 participants believed that at least one app sold user data to advertisers, with one participant extending this belief to all three apps they listed.

Compliance awareness was mixed. All participants assumed FERPA [22] and HIPAA [23] applied to the apps they used, but their perceptions of compliance varied. For FERPA, 107 participants believed all three apps were compliant, 7 believed none were, and 237 thought at least one app was compliant. However, 71 participants were unsure of any app's FERPA compliance. For HIPAA, 81 participants believed all three apps were compliant, 10 believed none were, 182 believed at least one app was compliant, and 51 were unsure.

Trust in developers' ability to safeguard user privacy was similarly divided. 53 participants distrusted at least one app, and one distrusted all apps they used. 46 Forty-six doubted the competence of at least one app's developers to protect privacy, with one participant holding this belief for all their apps.

3.2.6 Institutional policy about unsanctioned app use. Surprisingly, only 86 of K-12 participants and 37 HEI participants were aware that their institution had a policy regarding the use of unsanctioned education technologies. Many of those aware of policies (n=22) admitted to using unsanctioned apps despite policy prohibitions, citing institutional shortcomings. P10 shared that "[my institution doesn't] provide a workable path to utilize new and emerging

technologies so [I] have to go against it." P8 agreed with P10 stating "we are not supposed to use any application that is [not] already approved, but many, like myself, ignore the rule."

107 participants reported receiving institutional warnings about the risks associated with unsanctioned app use. Among them, 33 mentioned that those warnings led to behavioral changes. The most common changes included discontinuing unsanctioned app use, switching to alternatives perceived as more secure, adopting 2FA, and exercising greater caution when sharing content with platforms.

3.2.7 Discontinuation and data deletion. 368 participants reported that they continue to use the three unsanctioned applications they mentioned in the survey. This includes 19 participants who experienced security or privacy issues with the apps, 33 who believed the apps collect data that violates users' privacy, 33 who stated the apps share data with advertisers, 47 who expressed distrust in the apps, and 41 who considered the app providers incompetent at protecting privacy. Eighty-five participants mentioned that they stopped using at least one app. Only nine of them said that the apps provided an option to delete data, and eight of them requested data deletion, while 60 participants were uncertain about the data deletion feature.

4 Study 2: Admin survey

To understand if and how the use of unsanctioned applications by educator leads to any security and privacy incidents, we conducted another online survey targeting administrators, IT personnel, data governance bodies, and technology policymakers from US-based educational institutes.

4.1 Methods

Survey design. Survey questions were created based on results from the first study (Section 3.2). We first asked participants if they recommended unsanctioned apps to educators, or received requests from educators to integrate such tools with other institutional tools. Next, we asked them to explain if there was any security and privacy incident at the institution due to educators using unsanctioned apps (see Appendix A) for the full questionnaire.

Data collection. This survey was administered on the Qualtrics platform. We recruited participants through direct emails and posting the study link on the EDUCAUSE platform [6] and two Reddit [19] groups: *k12sysadmin* and *k12cybersecurity*, as large-scale recruitment of participants from the target population is infeasible through online platforms such a Prolific. The study received IRB exempt status, as it posed minimal risk to participants.

Participants were compensated through an opt-in lottery for a chance to win a $20 gift card, a higher incentive compared to the educator survey due to the specialized nature of their expertise and the challenges in recruiting this demographic.

Data analysis. Data analysis for this survey followed much of the same steps as the educators survey (§ 3.1), except with the difference of only two authors reviewing all the material due to the small size.

4.2 Results

4.2.1 Participants. We collected data from 24 participants, identified with an 'A'. Among those, two were from K-12 institutions while the rest were from HEIs. Of those participants, 12 were actively in roles related to information security while the rest were in administrative roles at their institutions such as business manager, principal, or vice chancellor.

4.2.2 Use and integration of unsanctioned apps. Seven participants said that they had recommended unsanctioned apps to educators, supporting results from Study 1 (Section 3.2). Their recommendations come from needing "to meet niche demands that our institutional platforms cannot manage, or where educators are looking for free alternatives for their use or their student's use" (A4). These recommendations include common platforms such as "Canva, Slack, and ChatGPT" (A7).

On the other hand, all but three participants had received educators' requests for unsanctioned tools to be integrated into institutionally licensed tools. For example, A4 mentioned how they "have instructors wishing to integrate many tools such as polling, scheduling, citation software for use in classes". One administrator (A21) discussed how "almost at an individual level, everyone has their "solution" to teaching/learning "better" and brings it into the classroom with disregard" regarding how educators bring unsanctioned technology into classrooms.

Regarding fulfilling the integration requests, two participants said such requests are never accepted, others' responses varied from 'sometimes' to 'most of the time'. Twelve participants said such integrations go through an IT audit, others were unsure.

4.2.3 Security and privacy incidents. Nine participants indicated that they had experienced security and privacy incidents due to unsanctioned app use. A4 stated that they "have had third-party integrations scrape user data without being vetted and without contractual controls in place." Another participant (A12) stated challenges they faced in ensuring institutional security because "a significant subset of faculty were in the habit of auto-forwarding internal university email to personal email accounts. This was a problem for many reasons, the biggest being none of our phishing controls or detection would detect anything after such emails had transited outside our managed environment, including phishing attack successes and account compromise [...]". Without providing details, one participant (A19) mentioned an issue with *otter.ai* [15], that was integrated with *Zoom* video conferencing tool.

Several participants expressed worries about the impact unsanctioned apps can have on institutional security posture and legal compliance. Overall their top concern for the use of those technologies stems from the possibility of leakage of PII, "personal information collected and stored incorrectly" (A10). One participant (A11) explained how using unsanctioned technology "strips the controls [the institution] very intentionally design, build in and manage". A21 stated that "In the case of a classroom, [disclosure of information] can commonly meet the criteria for a FERPA breach exposing the institution to serious liabilities". Another participant (A16) pointed out how "instructors [may] not understand that the institution has laws that it must follow to protect its data... And sometimes integrations impact a security plan/posture and we just

can't use them." Concerns were also growing regarding the use of AI tools like ChatGPT. A20 mentioned how they "believe faculty are regularly using *free* AI tools with student data" which could lead to student data being leaked and put into those AI systems.

5 Discussion

This study sheds light on the nuanced challenges associated with educators' use of unsanctioned applications in educational settings. From security and privacy perceptions to institutional policy awareness and administrative roles, our findings highlight a complex interplay of factors that shape app usage behavior. Below, we discuss key themes and their implications.

5.1 Educators' Security and Privacy Awareness vs. Action

The findings reveal a striking paradox: while many educators acknowledge the importance of security and privacy (§ 3.2.5), these concerns rarely influence app selection or usage behavior. For example, 218 participants considered security and privacy for at least one app, yet more than a third ($n = 176$) did not factor these considerations into their decisions at all. Furthermore, even after experiencing breaches ($n = 23$), suspecting apps of poor data collection practices ($n = 38$), or believing apps sold user data ($n = 43$), many educators continued to use these apps. This behavior underscores a tendency to prioritize ease of use, engagement, and functionality (§ 3.2.4) over compliance and safety, highlighting a gap between perceived risks and actionable responses.

Compounding this issue is the widespread uncertainty surrounding regulatory compliance. Despite most participants assuming FERPA and HIPAA applied to the apps they used, many were unsure of their compliance status ($n = 71$ for FERPA, $n = 51$ for HIPAA). This lack of clarity not only compromises institutional data security but also demonstrates the inadequacy of current measures to educate and empower educators in *evaluating app security*. Institutions must focus on bridging this gap by offering secure alternatives that align with educators' needs while providing clear guidance and training on security and compliance.

5.2 Limited Effectiveness of Institutional Warnings

Only 107 of participants were aware of institutional warnings about the risks of unsanctioned app use, and among those, only 33 were influenced to change their behavior (§ 3.2.6). These numbers suggest that current warning mechanisms fail to translate awareness into meaningful action. Most educators, even when aware of institutional guidelines, prioritize practicality and familiarity over compliance.

This highlights the need for institutions to rethink their policy enforcement strategies. Instead of relying solely on warnings, institutions should adopt a proactive approach by educating educators on the risks associated with unsanctioned apps and offering clear, actionable alternatives. For example, providing training sessions on how to evaluate apps for compliance, encouraging the adoption of institution-approved tools, and implementing educator-friendly policies that balance security with flexibility could enhance adherence. Ensuring that warnings are both relatable and actionable will likely improve their effectiveness in fostering behavior change.

5.3 The Illusion of Control

While the ability to download unsanctioned apps may give educators a sense of flexibility and autonomy, it also creates an illusion of control, particularly regarding data security and deletion. Our study results highlight a significant gap in educators' understanding of app exit strategies (§ 3.2.7). Of the 85 participants who stopped using at least one app, only nine were aware of a data deletion option, and just eight requested data deletion. Meanwhile, 60 participants were uncertain about whether such options existed.

This lack of awareness demonstrates that educators are not currently equipped to safeguard institutional data effectively, especially when using unsanctioned apps. Without clear exit pathways, sensitive data may remain exposed to risks long after app use ends. This emphasizes the critical need for institutions to implement robust policies and educational initiatives that address not only app usage but also secure disengagement practices. Training educators on topics such as data retention, deletion policies, and privacy risks can help mitigate these vulnerabilities while reinforcing the importance of compliance.

5.4 Administration Challenges and Contradictions

Administrators are often on the frontlines of managing the consequences of unsanctioned app use, including security and privacy incidents. As evidenced by participant feedback (§ 4.2.3), some administrators have firsthand experience with data breaches, such as third-party integrations scraping user data (A4) or faculty autoforwarding emails outside managed environments, thereby bypassing institutional phishing controls (A12). These incidents underscore the broader institutional vulnerabilities posed by unsanctioned apps, particularly regarding the leakage of personally identifiable information (PII) and violations of FERPA and other legal requirements.

Interestingly, while many administrators expressed frustration with educators' use of unsanctioned apps, others acknowledged their own role in facilitating such practices. Some administrators even supported the integration of unsanctioned apps, validating educators' claims that they are occasionally encouraged to use these tools. This duality can create gray areas in policy enforcement and addressing this issue will require a collaborative approach between educators and administrators, while maintaining a common goal toward security. By involving both educators and administrators in developing guidelines and reviewing tools, institutions can create realistic and effective policies that balance security requirements with the practical needs of teaching, ensuring compliance while supporting classroom needs.

6 Study Limitations

While our study provides valuable insights into the use of unsanctioned applications and their consequences, several limitations should be acknowledged. First, the self-reported nature of surveys

introduces the potential for social desirability bias, where participants may provide responses they perceive as more acceptable rather than their true thoughts and behaviors [14]. Second, the inability to ask follow-up or clarification questions limits our ability to fully understand participants' reasoning and decision-making processes, requiring interpretation of their responses. Third, there is considerable variation in response depth, with some participants providing detailed explanations while others offering minimal information, which may affect the richness of qualitative insights.

To mitigate these limitations, we emphasized the anonymity of the survey to encourage honest responses and requested participants to provide detailed answers where possible [13]. Future research could address these challenges by incorporating qualitative methods such as interviews or focus groups to gain deeper insights into educators' perspectives and decision-making regarding unsanctioned technologies.

7 Conclusion

Our findings emphasize the urgent need for institutions to rethink their approach to unsanctioned app use. Educators' preference for these tools, despite associated risks, reflects a demand for functionality and engagement that institutional offerings often fail to meet. At the same time, administrators' experiences with security incidents reveal critical gaps in policy implementation and enforcement. Educational institutions must invest in creating educator-friendly, while secure alternatives and provide clear pathways for vetting and approving education tools. Moreover, fostering a culture of shared responsibility—where both educators and administrators collaborate to balance innovation with compliance—will be essential for addressing these challenges effectively.

References

[1] [n. d.]. Video Conferencing, Cloud Phone, Webinars, Chat, Virtual Events | Zoom. https://zoom.us/

[2] David G. Balash, Dongkun Kim, Darika Shaibekova, Rahel A. Fainchtein, Micah Sherr, and Adam J. Aviv. 2021. Examining the Examiners: Students' Privacy and Security Perceptions of Online Proctoring Services. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 633–652. https://www.usenix.org/conference/soups2021/presentation/balash

[3] David G. Balash, Elena Korkes, Miles Grant, Adam J. Aviv, Rahel A. Fainchtein, and Micah Sherr. 2023. {Educators'} Perspectives of Using (or Not Using) Online Exam Proctoring. 5091–5108. https://www.usenix.org/conference/usenixsecurity23/presentation/balash

[4] Canvas. [n. d.]. Canva. https://app.learnplatform.com/marketplace/.

[5] Jake Chanenson, Brandon Sloane, Navaneeth Rajan, Amy Morril, Jason Chee, Danny Yuxing Huang, and Marshini Chetty. 2023. Uncovering Privacy and Security Challenges In K-12 Schools. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–28. doi:10.1145/3544548.3580777

[6] Educause. [n. d.]. Educause. https://www.educause.edu/.

[7] Barbara Fedders. 2018. The Constant and Expanding Classroom: Surveillance in K-12 Public Schools. *North Carolina Law Review* 97, 6 (2018), 1673–1726. https://heinonline.org/HOL/P?h=hein.journals/nclr97&i=1722

[8] DeVan L. Hankerson, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, and Dhanaraj Thakur. 2021. *Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software*. Technical Report. https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/

[9] Rakibul Hasan. 2023. Understanding EdTech's Privacy and Security Issues: Understanding the Perception and Awareness of Education Technologies' Privacy and Security Issues. *Proceedings on Privacy Enhancing Technologies* 2023, 4 (Oct. 2023), 269–286. doi:10.56553/popets-2023-0110

[10] Rakibul Hasan and Mario Fritz. 2022. Understanding Utility and Privacy of Demographic Data in Education Technology by Causal Analysis and Adversarial-Censoring. *Proceedings on Privacy Enhancing Technologies* 2022, 2 (April 2022), 245–262. doi:10.2478/popets-2022-0044

[11] Easton Kelso, Ananta Soneji, Sazzadur Rahaman, Yan Shoshitaishvili, and Rakibul Hasan. 2024. Trust, Because You Can't Verify: Privacy and Security Hurdles in Education Technology Acquisition Practices. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1656–1670. doi:10.1145/3658644.3690353

[12] Easton Kelso, Ananta Soneji, Sazzadur Rahaman, Yan Soshitaishvili, and Rakibul Hasan. 2024. Trust, because you can't verify:privacy and security hurdles in education technology acquisition practices *(CCS'24)*. Association for Computing Machinery, New York, NY, USA. Place: Salt Lake City, USA.

[13] Susan McNeeley. 2012. Sensitive issues in surveys: Reducing refusals while increasing reliability and quality of responses to sensitive survey items. *Handbook of survey methodology for the social sciences* (2012), 377–396.

[14] Anton J Nederhof. 1985. Methods of coping with social desirability bias: A review. *European journal of social psychology* 15, 3 (1985), 263–280.

[15] OtterAI. [n. d.]. OtterAI. https://otter.ai/.

[16] Britt Paris, Rebecca Reynolds, and Catherine McGowan. 2022. Sins of omission: Critical informatics perspectives on privacy in E-Learning systems in higher education. 73, 5 (April 2022), 708–725. doi:10.1002/asi.24575 Number of pages: 18 Place: USA Publisher: John Wiley & Sons, Inc. tex.issue_date: May 2022.

[17] Qualtrics. [n. d.]. Qualtrics. www.qualtrics.com.

[18] Sarah Radway, Katherine Quintanilla, Cordelia Ludden, and Daniel Votipka. 2024. An Investigation of US Universities' Implementation of FERPA Student Directory Policies and Student Privacy Preferences. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery, New York, NY, USA, 1–35. doi:10.1145/3613904.3642066

[19] Reddit. [n. d.]. Reddit. https://www.reddit.com/.

[20] Natalie Schwartz. 2023. Data breaches cost higher education and training organizations $3.7M on average in 2023. https://www.highereddive.com/news/data-breaches-cost-higher-education-colleges/689499/.

[21] Elisa Shioji, Ani Meliksetyan, Lucy Simko, Ryan Watkins, Adam Aviv, and Shaanan Cohney. 2024. "It's been lovely watching you": Institutional Decision-Making on Online Proctoring Software. IEEE Computer Society, 18–18. doi:10.1109/SP61157.2025.00018 ISSN: 2375-1207.

[22] US Department of Education. [n. d.]. Family Educational Rights and Privacy Act (FERPA). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[23] Wikipedia. 2024. Health Insurance Portability and Accountability Act. https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act.

[24] Ben Williamson, Sian Bayne, and Suellen Shay. 2020. The datafication of teaching in Higher Education: critical issues and perspectives. *Teaching in Higher Education* 25, 4 (May 2020), 351–365. doi:10.1080/13562517.2020.1748811 Publisher: Routledge _eprint: https://doi.org/10.1080/13562517.2020.1748811.

[25] Tianyi Yang and Rakibul Hasan. 2024. Discovering Privacy Harms from Education Technology by Analyzing User Reviews. In *Proceedings of the 23rd Workshop on Privacy in the Electronic Society (WPES '24)*. Association for Computing Machinery, New York, NY, USA, 186–192. doi:10.1145/3689943.3695050

A Appendix

The complete questionnaires for the educator and administrator surveys are available at the following link: https://osf.io/d9c6a/?view_only=a062ad724be64a82ab6033c556fa271e.