Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference

A Security Framework for Privacy Concerns in for e-Learning

[1]Adegbenro Dimeji, [2]Nwaocha Vivian, [3]Ogunlowo Tolulope & [4]Longe, Olumide Babatope
[1&2]Doctoral Programme in Cyber Security, African Centre of Excellence in Technology Enhanced Learning, National Open University of Nigeria, Abuja, Nigeria
[3]Society for Multidisciplinary & Advanced Research Techniques (SMART), Lagos, Nigeria
[4]Diaspora Liaison Lead – SMART, 5059 Cedar Drive, Columbus, Ohio, USA
E-mails: adegbenrodimeji@yahoo.com; onwaocha@noun.edu.ng; ogunlowotolulope97@gmail.com; longeolumide@acity.edu.gh;

ABSTRACT

This study aims on Right to Privacy on the Internet. The paper will unfold as follows. Influences on consumer privacy online, online consumer tracking; that is when online scenarios meet privacy expectations or complied with a privacy notice, and the importance of privacy notices in managing privacy online. This paper will also highlight consumer online privacy specifying ''the youth, parents, and online privacy' 'and the regulations in place to shape such policies. Will also unfold privacy in the digital age or the internet. This paper will again unfold UN general assembly on the right to privacy on the internet. The paper unfolds the potential consequences of revealing certain information online and analyzes if there are any differences between the motivations and attitudes of young people. Will again highlight on National Security Agency (NSA) surveillance which demands that Internet carriers be more forthcoming about their handling of personal information which must be intensified. Responding to this concern, this report evaluates the data privacy transparency of forty-three Internet carriers serving the public. This paper is to investigate the relationship between individual and societal determinants of online privacy concern (OPC) and behavioral intention of internet users. The study also aims to assess the degree of reciprocity between consumers' perceived benefits of using the internet and their OPC in the context of their decision-making process in the online environment.

Keywords: Security, Framework, Privacy, Internet, Data Privacy, Online, Consumers, Education.

Proceedings Citation Format
Adegbenro, D.R., Nwaocha, V., Ogunlowo, T. & Longe, O.B. (2023): Towards The Development of a Self-Diagnosing System for Ailments Using Predictive Modelling Machine Learning. Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. 31st May – 2nd June, 2023. Pp 183-192. https://www.isteams.net/ghanabespoke2023. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2023P18

1. BACKGROUND TO THE STUDY

In 2016 the issue of privacy entered the radar of social awareness because of the public outrage caused by the news about Cambridge Analytica. News outlets reported how the company used personal data leaked from Facebook and other platforms to influence the 2016 political campaigns of Brexit in the UK, and the presidential election in the USA. Almost in sync with these events, some rising voices started to warn us about the real depth of the issue and its impact.

The E-learning community is growing at a rapid pace and so are e-learners' privacy concerns. Considerable amounts of data about e-learners are being collected to provide personalized learning experiences. The collected data contain personal and sensitive information such as test scores, learning preferences, learning progress, questions asked in forums, conversations in chat rooms, and counseling sessions. As a result, there are natural concerns over privacy. It is desirable to offer sufficient privacy to ensure that e-learners have autonomy in their activities and personal spaces in this relatively public educational environment. Demchak and Fenstermacher have noted that privacy is directly related to the knowledge of the identity (Kim, 2021). We view identity as a dataset (e.g. name, biometric data element, behavioral pattern, etc.) that is used to model and thereby recognize an entity as distinct from others. An entity may be represented by many identity models including its own "true" identity (Miah, 2020).

Naturally, some models are partial, revealing some but not all information about the entity. Some models may be incorrect representing false information about the entity. Sometimes, a person may want to publish their own personal identity model, and sometimes they may want to keep it concealed. E-learning systems are different from many other online communities in that learners typically have more trust in the system (e.g. they are willing to part with private information readily, as they believe it will be used in evaluation), and have an extended working relationship with the system (e.g. they may work with the same forum system for many years as they progress through a program). While personalization has become very popular in today's adaptive e-learning systems, we feel that the learner's privacy and identity management issues have largely been ignored. Kobsa and Schreck have described the risks to privacy posed by the personalization (Zerka et al., 2020).

Online privacy issues are reflected in various activities, such as peer review, group collaborative work, and learners' evaluations. In doing peer reviewing and assessment, learners access online portfolios which contain sensitive information such as scores, project-related assignments, and self-reflection. The main issue regarding privacy in collaboration is learners' desire to control how they are perceived by other people (Patil & Kobsa, 2005).

2.1 LITERATURE REVIEW

Online privacy issues are reflected in various activities, such as peer review, group collaborative work, and learners' evaluations. In doing peer reviewing and assessment, learners access online portfolios which contain sensitive information such as scores, project-related assignments, and self-reflection (Meier, Schäwel, & Krämer, 2020). The main issue regarding privacy in collaboration is learners' desire to control how they are perceived by other people (Meier et al., 2020). When learners don't feel comfortable about sharing knowledge on social media websites or in the online environment, or if they don't recognize the value of knowledge gained through sharing in an online environment, they become resistant to such a learning platform. A safe learning environment is protected by guaranteeing learners' privacy (L. Li, Shen, & Han, 2021). (Sims, 2021) stated that in class or in online discussions, students reveal lots of personal and private information that might be questionable or even threatening to our boundaries and ethical responsibilities, which raises a question about how much students should share their personal information with the instructor.

Bondre, Pathare, & Naslund (2021) suggested that instructors can integrate the privacy criteria and learning expectations into the rubrics and focus on assessing students' learning outcomes to avoid being influenced by students' self-disclosed information. In collaborative work, it is important that the members trust and respect each other's privacy and that the instructors create a trust and privacy-guarded environment. We should develop norms about what information is to be shared and the steps taken to process and anonymize that information. We should also know that privacy issues are context-based, and information in one context might not be transferred to another without being associated it original context (Alexei & Alexei, 2021).

In learner assessment and evaluation, bias can occur due to differences in gender, ethnicity, and other factors. Social media websites such as Facebook, Twitter, and blogs provided flexible digital environments for learners to learn anywhere, anytime, on various online platforms. More and more instructors are starting to integrate such non-institutional learning platforms into their teaching. However, such an environment also raises challenges for learners, which causes resistance from learners. The challenges include learners' skillfulness and comfort in using new technology and their comfort level with digital identity, time that might be wasted on new technology, and concerns about the boundaries between social and professional identities (de Souza Rodrigues, Chimenti, & Nogueira, 2021).

2.1.1 Trust and Privacy Issues In E-Learning

Many assumptions about privacy in a traditional classroom do not apply to online learning whether it is an online offering of a course or an online community of practice. A traditional classroom represents a close group where learners get to know each other. Yet some information is private including precise grades or confidential conversations. In contrast, e-learners become acquainted with one another by means of looking into each others' profiles. A profile is a self-constructed identity model presented under some label, popularly known as a pseudonym. An e-learner may construct many such profiles depending on how they want to present themselves in many different contexts (Ivanova, Grosseck, & Holotescu, 2015). For example, an e-learner may want to position herself differently to her co-learner peers than to her instructors or might want to share more personal information with her project team than with the members of other project teams. Since each of the profiles consists of a different subset of personal information, they represent partial identities. To e-learners, privacy is about the autonomy of presenting themselves differently in different contexts (Liagkou, Stylios, & Petunin, 2019).

In a traditional classroom, learners do not enjoy the same freedom of presenting themselves so differently in different contexts as do e-learners. In a traditional classroom, an observer can easily construct an identity model of another learner. As a result, unlike e-learning, a self-constructed identity model of a learner may not be well accepted by another learner in a traditional classroom setting. However, the lack of privacy is compensated by a greater degree of trust in a traditional classroom (Meier et al., 2020). E-learners are often strangers whose interactions are limited to certain selected written communications (synchronous or asynchronous). Any private information is prone to misuse when shared with a stranger. It is also hard to engage in a trusting relationship with a stranger. With a certain degree of familiarity, one can form an opinion about another person's trustworthiness (Zhu, Yu, Riezebos, et al., 2016). While in a traditional classroom, physical presence works as the guarantor of authenticity, in e-learning a learner needs to worry about the authenticity of their peers or instructors. We observe the need for privacy and trust in the following popular learning activities (Valluripally, Gulhane, Mitra, Hoque, & Calyam, 2020).

3. THEORETICAL FOUNDATION AND RESEARCH MODEL

3.1 Privacy Concern and Educational Technology

Bandara, Balakrishna, & Ioras (2021) defined the need to protect people's rights in their landmark article, The Right to Privacy. Privacy refers to a person's ability to control others' access to personal information (Els & Cilliers, 2018). Privacy is violated when individuals cannot maintain their communication with social and physical environments. However, privacy concerns are not a new phenomenon; these incidents repeatedly evolve when an individual perceives a threat from an innovative information technology (I.T.) that develops the surveillance, storage, retrieval, and communication of personal information (Karagiannis, Papaioannou, Magkos, & Tsohou, 2020). With the rapid advancement of educational technologies, the exchange of students' information has become more convenient (de Souza Rodrigues et al., 2021).

E-learning service providers have better and more sophisticated ways to access and collect personal information; therefore, gaining a student's personal information has become more accessible (Conference & Icvl, 2020). As a result, privacy concerns about personal information accelerate tremendously among students as a considerable amount of personal information is interchanged, stored, and shared (Maguraushe, Da Veiga, & Martins, 2019). Different countries introduced privacy guidelines and standards to guarantee students' personal information is fully protected (Liagkou et al., 2019). Despite these attempts, many educators and pupils are still reluctant to use the potential benefits of an e-learning environment due to privacy concerns. According to the study findings by (Anwar, 2020), people who were more concerned about their online privacy than others also shared slightly less personal information and had substantially more negative attitudes toward information sharing (between-person level). Thus, an inclusive interception of the privacy dynamics concerning the digitization of personal information in adopting an e-learning environment can only be achieved by looking at the factors that influence students' attitudes toward e-learning environment use (Alharthi, Spichkova, & Hamilton, 2019).

3.2 Proposed Conceptual Model

We modify a conceptual model for creating security subsystems previously introduced by (Alqurashi, 2019). Though this model did not focus on e-learning issues, it can be extended to it. Such an approach is not new. For example, (Karagiannis et al., 2020) used the D&M model of information systems success to generate their own model to assess e-learning systems success. Similarly, (Ioannou, Tussyadiah, & Miller, 2021) proposed another model based on multiple previous works of (H. Li, Yoo, & Kettinger, 2021). The reason for that is that the model mirrors the National Institute for Standards and Technology's (NIST's) system development lifecycle model (SDLC). The purpose of all NIST models is to ensure that they are generic enough to be extended to different areas (Hong, Chan, & Thong, 2021). The modified model is presented in Figure 1. A brief description of each factor along with individual propositions that set the stage for future research are presented next.

3.3 Data Evaluation

The use of data in organizations usually follows certain guidelines that may reflect consistent procedures and practices of the IT team, especially the database administrator (DBA). Organizational DBMS hold data for thousands of users and these data fall into different forms. As universally understood, the integrity of data (completeness and correctness) is essential to building a robust useful database. Consequently, the security of these data should always be considered a part of its integrity. We believe that an institution that offers e-learning programs must adopt robust measures to protect restricted, confidential or sensitive participants' data against loss or improper use by unauthorized internal or external parties. A data management policy can help in this regard. That policy should articulate procedures and practices for data protection. One assumes that the DBA and the database team follow universally-effective practices for data design and management.

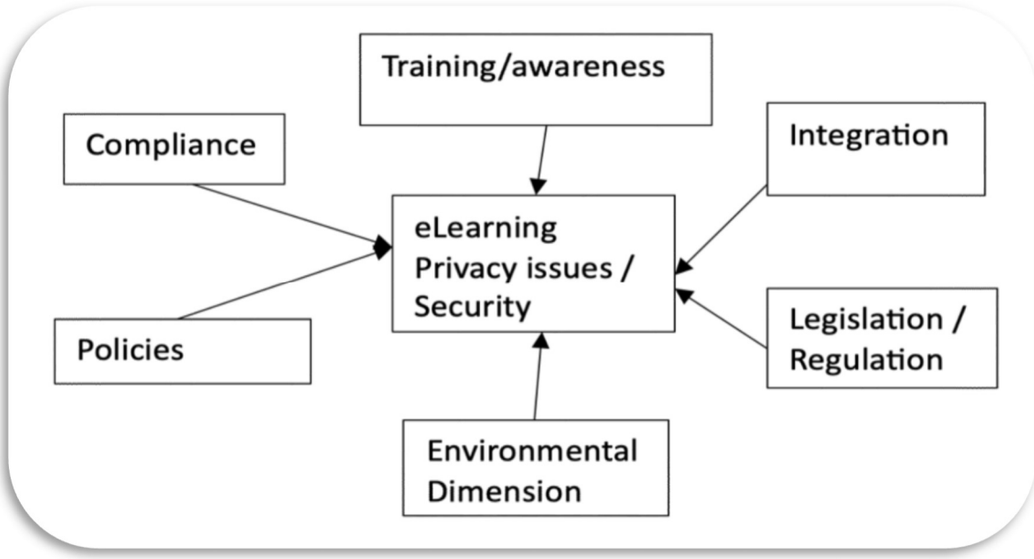

Fig 1: Privacy issue eLearning conceptual framework

3.4 Policies

We work on the premise that organizations continue to seek improvements and all their activities are designed to help achieve these improvements. Accordingly, policies are created, refined, and implemented to help attain organizational strategic goals. When policies are initiated and adopted, the security and privacy of the stakeholders must be addressed in these policies. While developing security policies for e-learning, many factors should be considered: 1) the student's home environment, 2) the student's use of technology, and 3) the teacher/facilitator of the interaction. For educational institutions, their practice of using technology should be clearly stated as a measure of protection for the well-being of the participating student. Additionally, the integrity of the experience (plagiarism/cheating).

3.5 Legislation/Regulation

Most organizations try to implement relatively good security plans, protections, and response capabilities. However to plan for the future, even a well-prepared entity needs to understand the driving forces that will require it to change its security planning, protections, and response. Compliance and regulations are probably the most important set of driving forces for organizations today. To be in compliance organizations invariably need to substantially improve their security. This is especially true in the areas of documentation and identity management (Zhu, Yu, & Riezebos, 2016). Examples of laws include data breach notification requirements such as California's SB 1386. Some deal with privacy protection, e.g. the European Union (EU) Data Protection Directive of 2002, and the US Gramm-Leach-Bliley Act (GLBA).

Universities are faced with compliance not just due to federal (e.g. Federal Requirement 4.8) regulations, but also under guidelines laid down by accreditation agencies such as the Southern Association of Colleges and Schools (SACS). SACS expects that each institution documents procedures that assure that the security of personal information is protected in the conduct of assessments and evaluations and in the dissemination of results. Institutions are also required to have a written procedure for protecting the privacy of students enrolled in distance and correspondence education courses or programs.

3.6 Architecture

This can be an overwhelming challenge for eLearning. The nature of online course delivery prompts many areas for concern with respect to security. The infrastructure of the institution and architecture of security should be designed to address the following: • Defining user roles (students and instructors) and their identity and login (Els & Cilliers, 2018); Course content and user manipulation (content addition, modification, deletion, and use) ability; and • Access channels. As a part of online course delivery, using a learning management system (LMS) has become common and frequent. Many of these will be addressed via agreements (or understanding) of what the institutions will provide and what the instructor's obligations will be.

For example, it is commonly understood that the instructor will be the designer/manager of the course. He/she will be the only one who can add, modify, or delete content (Liagkou et al., 2019). In the student role, the participating audience will have access based on what the instructor allows them to do using the different features in the LMS. Defining the parameters for secure access and protection of intellectual property must be addressed in the architecture. Therefore, we posit P4: Well-designed security architecture will enhance the security and privacy of the e-learning technologies (Alqurashi, 2019).

3.7 Integration

The wide array of enterprise systems in the market poses a challenge to organizations with respect to legacy and current existing systems. It is assumed that if an organization were to mix and match systems, these systems must integrate well to serve the different functions of the organization. For an academic institution that offers e-learning courses, the same holds true. The LMS and its security features must mesh well with that institution's current security plan and standards. The importance of information systems integration lies in the control and flexibility that integration affords the organization (Conference & Icvl, 2020).

With today's technological affordances, different DL stakeholders can benefit from IS integration as it presents a complete approach to the learning experience (Alier, Casany, Severance, & Amo, 2020). Today's organizations started to notice the need for systems that support their rapidly changing environments (Zerka et al., 2020). Academic institutions are learning new approaches to managing themselves like business entities. Because of so many surrounding conditions, higher education is changing into different business models (Maqsood & Chiasson, 2021).

The new business model includes investments in DL. That allows for new funding resources to accommodate the shrinking public resources. How is information systems integration relevant here? As tertiary institutions adapt, information technology tools will be needed to support the changing environment with respect to needs and infrastructure. In the previous section, we presented architecture as an essential driver for security in DL. The architecture of information systems almost always includes integration. Therefore we posit: P5: A complete and correct integration of information systems will enhance security and privacy of learning technologies (Sims, 2021).

3.8 Training

Most directives pertaining to security and privacy are captured in the security policy, and the standards. However, they will not be effective if no one knows about them and how an organization expects them to be implemented. For security to be effective, everyone from senior management on down to the rest of the staff must be fully aware of the importance of enterprise and information security (L. Li et al., 2021). A security-awareness program is geared toward an individual audience to ensure that each group understands its particular responsibilities, liabilities, and expectations. Security training should happen periodically and continually. Various methods should be employed to reinforce the concepts of security awareness. Things like banners, employee handbooks, and even posters can be used as ways to remind university employees and students about their duties and the necessity of good security practices.

At this juncture based on our research, training pertaining to e-learning courses is relegated to effective teaching of a distance course. It does not directly relate to the security awareness (Alqurashi, 2019). For example, SACS questions each institution's ability to make training in technology available to faculty members teaching distance education courses. As universities continue to evolve toward hybrid and pure online teaching environments, security and privacy issues will need to be communicated and assessed. Therefore, we posit P6: Security training, education, and awareness programs will enhance the security and privacy of e-learning technologies (Els & Cilliers, 2018).

3.9 Risk Analysis

An effective risk analysis should integrate the security program objectives with a university's business objectives and requirements. The more the university and security objectives are in alignment, the more successful the two will be. The analysis will help a university draft a proper budget for a security program and its constituent security components. Once an organization knows how much its assets are worth and the possible threats they are exposed to, it can make intelligent decisions about how much money to spend protecting those assets (Tsai, Whitelock-Wainwright, & Gašević, 2020).

SACS guidelines state that an institution has an ethical responsibility to take reasonable steps to provide a healthy, safe, and secure environment for all campus constituents, as it will contribute toward more effective risk management. Risk management/analysis according to SACS can be carried out through a review of an institution's safety plan, crisis communications plan, and other health and safety procedures. However, once again, in the eLearning technology realm, specifics are lacking in terms of required guidelines.

4. DISCUSSION

It is undeniable that distance education has become an essential part of higher education. The framework included data evaluation, policies, legislations/regulations, architecture, integration, training, and risk analysis. The conceptual framework within this research relies on the premise that information privacy and security span all of the five components. Thus, we adopted (Meier et al., 2020) model because of its wholesome premise to protect the organization's various aspects. Said model diligently seeks the integration of privacy and security as fundamental feature into each of the five components.

The seven pillars aim to encompass and relay the essential importance of privacy and security in any information system. They acknowledge that their model has intentional redundancy because "…one's view of a component differs when considering how it relates to the business process, security governance, and/or privacy governance subsystems.

5. IMPLICATIONS, FUTURE RESEARCH, AND CONCLUSION

This research used a known security and privacy model and extended it to e-learning based on previous practices of similar modes. E-Learning has become a fixture in higher education; therefore, its security becomes an important matter that should be properly treated. We conveyed that a wholesome risk analysis should be conducted to identify vulnerabilities and challenges. Accordingly, policies and procedures are charted based on the findings to ensure compliance. In addition, an assessment of resources and training needs will be necessary as well. Accordingly, educating and preparing the stakeholders to counter these risks will become easier. An effective e-learning environment depends on stakeholders who understand the importance of security and behave responsibly within it.

This study also shows that privacy issues in some areas are not addressed comprehensively and clearly, nor are they informed to the practitioners. Higher education institutions need to train instructors and practitioners about privacy issues, particularly in an online learning environment. There should be “an urgent move to educate online behaviors in all school levels, and professional training.

Sharing knowledge publicly is becoming more and more important. However, it is equally important to respect and protect learners’ privacy, especially in an online learning environment when privacy issues are more complex and nuanced compare with privacy issues in a physical learning environment. Some instructors may stop some good practices such as openly sharing knowledge among peers when such practice makes students feel that their privacy has been violated. It is a balance between respecting students’ privacy and convincing students to step outside of their private zone to share knowledge openly with their peers.

Privacy is contextual, it is difficult to have a universal privacy policy that can be applied everywhere. Privacy concerns are context-based and may change over time within different groups of the community. New privacy issues need to be identified and some privacy contracts may need to be revised and tailored to a new group of the community or a new context.

REFERENCE

Alexei, A., & Alexei, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *Article in International Journal of Scientific & Technology Research*, *10*(3), 128–133. Retrieved from www.ijstr.org

Alharthi, A. D., Spichkova, M., & Hamilton, M. (2019). Sustainability requirements for eLearning systems: a systematic literature review and analysis. *Requirements Engineering*, *24*(4), 523–543. https://doi.org/10.1007/s00766-018-0299-9

Alier, M., Casany, M. J., Severance, C., & Amo, D. (2020). Learner Privacy, a pending assignment. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*, 725–729. https://doi.org/10.1145/3434780.3436635

Alqurashi, E. (2019). Predicting student satisfaction and perceived learning within online learning environments. *Distance Education*, *40*(1), 133–148. https://doi.org/10.1080/01587919.2018.1553562

Anwar, M. (2020). Supporting Privacy, Trust, and Personalization in Online Learning. *International Journal of Artificial Intelligence in Education*. https://doi.org/10.1007/s40593-020-00216-0

Bandara, I., Balakrishna, C., & Ioras, F. (2021). the Need for Cyber Threat Intelligence for Distance Learning Providers and Online Learning Systems. *INTED2021 Proceedings*, *1*, 9312–9321. https://doi.org/10.21125/inted.2021.1947

Bondre, A., Pathare, S., & Naslund, J. A. (2021). Protecting Mental Health Data Privacy in India: The Case of Data Linkage With Aadhaar. *Global Health: Science and Practice*, *9*(3), 467–480. https://doi.org/10.9745/ghsp-d-20-00346

Conference, I., & Icvl, V. L. (2020). Data Privacy Aspects of E-learning (1) Trakia University – Stara Zagora , Faculty Technics and Technologies - Yambol , 38 “ Graf Ignatiev ” str , Yambol - 8602 , Bulgaria E-mail : kamenkk [at] abv . bg Abstract, *2*(May 2018), 291–296.

de Souza Rodrigues, M. A., Chimenti, P., & Nogueira, A. R. R. (2021). *An exploration of eLearning adoption in the educational ecosystem*. *Education and Information Technologies* (Vol. 26). Education and Information Technologies. https://doi.org/10.1007/s10639-020-10276-3

Els, F., & Cilliers, L. (2018). A privacy management framework for personal electronic health records. *African Journal of Science, Technology, Innovation and Development*, *10*(6), 725–734. https://doi.org/10.1080/20421338.2018.1509489

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics*, *168*(3), 539–564. https://doi.org/10.1007/s10551-019-04237-1

Ioannou, A., Tussyadiah, I., & Miller, G. (2021). That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure. *Journal of Travel Research*, *60*(7), 1510–1526. https://doi.org/10.1177/0047287520951642

Ivanova, M., Grosseck, G., & Holotescu, C. (2015). Researching data privacy models in eLearning. *2015 International Conference on Information Technology Based Higher Education and Training, ITHET 2015*, *00*(c). https://doi.org/10.1109/ITHET.2015.7218033

Karagiannis, S., Papaioannou, T., Magkos, E., & Tsohou, A. (2020). Game-Based Information Security/Privacy Education and Awareness: Theory and Practice. *Lecture Notes in Business Information Processing*, *402*(November), 509–525. https://doi.org/10.1007/978-3-030-63396-7_34

Kim, S. S. (2021). Motivators and concerns for real-time online classes: focused on the security and privacy issues. *Interactive Learning Environments*, *0*(0), 1–14. https://doi.org/10.1080/10494820.2020.1863232

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. *Journal of Management Information Systems*, *38*(1), 222–245. https://doi.org/10.1080/07421222.2021.1870390

Li, L., Shen, Y., & Han, M. (2021). Perceptions of information systems security compliance: An empirical study in higher education setting. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 6226–6231. https://doi.org/10.24251/hicss.2021.751

Liagkou, V., Stylios, C., & Petunin, A. (2019). Handling privacy and concurrency in an online educational evaluation system. *Baltic Journal of Modern Computing*, *7*(1), 86–98. https://doi.org/10.22364/bjmc.2019.7.1.07

Maguraushe, K., Da Veiga, A., & Martins, N. (2019). A conceptual framework for a student personal information privacy culture at universities in Zimbabwe, *12*, 143–128. https://doi.org/10.29007/wts6

Maqsood, S., & Chiasson, S. (2021). Design , Development , and Evaluation of a Cybersecurity , Privacy , and Digital Literacy Game for Tweens, *24*(4).

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, *8*(2), 291–301. https://doi.org/10.17645/mac.v8i2.2846

Miah, M. (2020). Blockchain Technology in Peer-to-Peer eLearning: Opportunities and Challenges. *2020 Proceedings of the EDSIG Conference Virtual Conference*, 1–13. Retrieved from https://www.researchgate.net/publication/345148488_Blockchain_Technology_in_Peer-to-Peer_eLearning_Opportunities_and_Challenges

Sims, L. (2021). *Effective Digital Learning*. *Effective Digital Learning*. https://doi.org/10.1007/978-1-4842-6864-3

Tsai, Y. S., Whitelock-Wainwright, A., & Gašević, D. (2020). The privacy paradox and its implications for learning analytics. *ACM International Conference Proceeding Series*, 230–239. https://doi.org/10.1145/3375462.3375536

Valluripally, S., Gulhane, A., Mitra, R., Hoque, K. A., & Calyam, P. (2020). Attack Trees for Security and Privacy in Social Virtual Reality Learning Environments. *2020 IEEE 17th Annual Consumer Communications and Networking Conference, CCNC 2020*. https://doi.org/10.1109/CCNC46108.2020.9045724

Zerka, F., Barakat, S., Walsh, S., Bogowicz, M., Leijenaar, R. T. H., Jochems, A., … Lambin, P. (2020). Systematic Review of Privacy-Preserving Distributed Machine Learning From Federated Databases in Health Care. *JCO Clinical Cancer Informatics*, (4), 184–200. https://doi.org/10.1200/cci.19.00047

Zhu, Z. T., Yu, M. H., & Riezebos, P. (2016). A research framework of smart education. *Smart Learning Environments*, *3*(1). https://doi.org/10.1186/s40561-016-0026-2

Zhu, Z. T., Yu, M. H., Riezebos, P., Weber, R. H., Alqurashi, E., Herrington, A., … Hajiyev, J. (2016). An Instructional Design Framework for Fostering Student Engagement in Online Learning Environments. *Distance Education*, *9*(1), 1–14. https://doi.org/10.1080/10494820.2020.1863232