# Privacy Trust Framework for Evaluation of Security Breaches in Digital Learning Environment – Research in Progress

**[1]Adegbenro, D.R., [2]Nwaocha, V. &[3] Longe, O.B. & [4]Okunoye, A.O.**
[1&2&3]Doctoral Programme in Cyber Security
African Centre of Excellence on Technology Enhanced Learning
National Open University of Nigeria, Abuja, Nigeria
[3]Faculty of Computational Science & Informatics, Academic City University, Accra, Ghana
[4]Williams College of Business, Xavier University, Cincinnati, Ohio, USA.
**E-mails:** [1]dimeji.adegbenro@aun.edu.ng ; [2]onwaocha@noun.edu.ng; [3]olumide.longe@acity.edu.gh; okunoye@xavier.edu
**Phone:** +2348026257856; +2348082595455; +233595479930, +15137453052

## ABSTRACT

Our research focus is to identify privacy concern as a factor that influence learners trusts in online learning environments. We intend to elucidate and provide a framework that can assist institutions and instructors who design and implement e-learning platforms and online courses to address these concerns. The essence of the proposed framework is to serve as an evaluation tool for assessing security breaches in digital learning environments using appropriate theoretical.

**Keywords:** Privacy, Trust Framework, Evaluation, Security Breaches, Digital Learning Environment

**Proceedings Reference Format**
Adegbenro, D.R., Nwaocha, V., Longe, O.B. & Okunoye, A.O. (2021): Privacy Trust Framework for Evaluation of Security Breaches in Digital Learning Environment Proceedings of the 27th iSTEAMS Multidisciplinary Innovations & Technology Transfer (MINTT) Conference. Academic City University College, Accra, Ghana. June, 2021. Pp 355-362 www.isteams.net/ghana2021.
DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2021/V27P31

## 1. INTRODUCTION

The use of information and communication technologies has greatly changed how learning experiences are conceived and deployed. Together with cloud computing, the widespread use of different digital devices enables learning possibilities not previously considered. Students can now access a multitude of learning opportunities, engage with apps that concentrate on a particular subject, enhance their virtual world experience, increase reality and communicate with others through social networks (World Economic Forum, 2020). In a learning environment, the progression of technology progresses along with the ability to record events that occur. It is also possible to capture and store every interaction and resource accessed. As a result, privacy issue needs to be urgently addressed since information and communication technologies is now the new normal for learning due to COVID-19 Pandemic. Human dignity is preserved, sovereignty is granted, and communication barriers are reduced. When our online activities generate a trove of data that can be easily collected, processed, and disseminated at scale using technological means, our privacy is at risk.

These risks are present in every aspect of online interaction, including learning environment. Professor Jim Greer was one of the first opinion leaders to raise concerns about online learning privacy, as well as data privacy in general. Determining how much information the environment can enable others to see is a major problem in promoting privacy in e-learning. According to evidence, some people will feel more comfortable disclosing more information about their online activities than others. Individuals' confidence in the positions they play is strongly related to their willingness to release personal information. For example, students are more likely than others to reveal personal details to certain groups (instructors, tutorial assistants, and friends) than to other (classmates and strangers). As a general rule, each person must feel that his or her privacy is protected and will not be infringed upon.

Institutions and organizations at various levels are now adopting electronic learning option even though most of these institutions are not prepared for online learning options but they have no option but to adapt to the changing situation due to the risk of having physical classes due to COVID-19 pandemic. In order for institution to continue learning activities they have to provide adaptable and scalable option to deliver instruction virtually via on-line and remote platforms. Some also adopted blended learning as an option in environments where data delivery and network conditions makes it challenging to go fully online (UN, 2020). These trends have also penetrated the African learning landscape with the advent and introduction of e-learning to facilitate distance learning and support conventional classroom activities especially during the COVID-19 era. Today's e-learning platforms provide the opportunity for remote learning, innovation and enhanced learning environments that are student-driven (Diaz, Golas, & Gautch, 2010), but with these new opportunities comes other challenges such as trust and privacy as it relates to the volume of data stored by the participants

## 2. RELATED WORKS

While many of the tools and technologies adopted in these efforts provides the needed platform to facilitate teaching and learning, privacy of information, trust and security have remained largely uncaptured by these technologies (Steiner, C., Kickmeier-Rust, M.D., and Albert, 2015) . Antecedently, e -learning technologies have focused on algorithmic and technological designs, delivery of course contents, pedagogies and instructor and student level interaction without much consideration given to privacy concerns (El-Khatib, Korba, Xu, & Yee, 2003). Given the increasing adoption of e-learning from the African perspective and the volume of student information that will be migrated online, trust and privacy protection has become an important component that must be considered in order to make diffusion and adoption of e-learning platform scalable. As users of e-learning facilities become more aware of the risks of information disclosure, institutions adopting e-learning will need to do more to assure trust and privacy in e -learning platforms (Wang, 2014; EdTech, 2020).

According to Anwar and Greer (2012), Concerns have been raised on the use of tracking systems on teachers and learners as well as the use of CCTVs to monitor examination conducts. "Privacy and trust are equally desirable in a learning environment. Privacy promotes safe learning, while trust promotes collaboration and healthy competition, and thereby, knowledge dissemination" Are designers and tutors ready for trust related and privacy related issues in online learning environment? (Ramona Juanjo 2019). The need also exists to evolve methodologies and models that can be adopted to evaluate security breaches in learning environments.

Furthermore, Greer's work touches on all three primary ideas in different ways. In addition, his work offers a distinct viewpoint on the relationship between identity and appearance and privacy. In his work, privacy is defined as the ability of a user to decide the circumstances under which their personal information is displayed. Irving Goffman's concept of privacy is the inspiration for this concept. The restriction theory of privacy stresses the need of restricting others' access to one's personal data. The control theory of privacy recognizes the importance of having control over one's data. The fundamental critique of control theory is that having complete control over all information is an unrealistic goal, especially since our online presence exposes us to a variety of observers.

### 2.1 Research Gaps

Our research has therefore based on existing literature identified heightened privacy concern as a factor that influence learners trusts in online learning environments and sets out to address these gaps. Furthermore, we intend to elucidate and provide a framework that can assist institutions and instructors who design and implement e-learning platforms and online courses to address these concerns. Our Framework will further assist in evaluating security breaches in digital learning environments using appropriate theoretical lens (Mary Frances, Patrick & Xeturah, 2019).

### 2.2 Research Questions

The research questions that emanate from the foregoing are:

1. How can privacy, trust, and personalization be supported in an online learning environment
2. To what extent are privacy, trust, and personalization desired in e-learning environments?
3. What are the most common trust and privacy issues with existing online learning platforms, and how can they be addressed?
4. Are designers prepared to incorporate trust and privacy into the design of e-learning environments?

### 2.3 Aims and Objectives

The proposed aim of our research is to develop a Framework that integrate Trust and Privacy into e-Learning Environments by contextualizing the peculiarities of the African Learner. The same framework will then be used to evaluating security breaches in digital learning environments

To achieve the aims above, the following specific objectives will be pursued:

i. An analysis of the strengths of existing privacy and trust model in an e-Learning environment will be carried out
ii. We will design a privacy preservation and trust model to mitigate Privacy issues in digital learning environments by contextualizing the specific parameters that impact on trust and privacy from an African perspective
iii. Develop a data framework for the design in (ii)

### 2.4 Relationship Among Privacy, Trust, Security, And Personalization

Trust and privacy are intertwined constructs: the more we trust, the more information about ourselves we are willing to reveal [Teltzrow and Kobsa, 2004, Briggs et al., 2004]. Trust is a prerequisite for self-disclosure because it reduces the perceived risks of revealing private information [Steel, 1991]. [Rezgui et al., 2003] offer a reputation management system for monitoring the reputation of online services and attributing high reputation to services that do not cause any “leakage” of private information. As a consequence, reputation-based trust may be used to online service privacy management. Chellappa and Sin further establish, through an empirical investigation, that online consumers' privacy concerns are inversely connected with the elements that establish confidence in the vendor providing personalized services [Chellappa and Sin, 2005]. People are unlikely to divulge personal information to an untrustworthy party.

People may be wary about data collection if they believe their personal information may be exploited. Friedman et al. further argue that online transaction trust is directly linked to privacy concerns [Friedman et al., 2000]. In the Internet world, trust brings with it the risk of privacy invasion, identity theft, and personal reputation damage. The distinction between privacy and security must be understood. When it comes to privacy, security may be both a friend and a foe. Security is viewed as a technological problem, but privacy is viewed as a social responsibility. The connection is that security technologies may provide procedures for ensuring privacy. [Dourish and Anderson (2006)] [Dourish and Anderson (2006)] [Dourish and Anderson (2006)]. Access control and authentication can be used to achieve privacy through security. Information privacy refers to a person's capacity to regulate the use and distribution of personal information about oneself, as well as who has access to such information [Cavoukian, 2002]. While access control and authentication can protect against direct disclosures, they can't protect against disclosures based on inferences formed from the disclosed data [Sweeney, 2002]. When authentication is not required to obtain a sufficient level of security, privacy may be jeopardized [Kent and Millett, 2003].

Majority of people are unaware of the privacy and security implications of the authentication methods they are compelled to employ in dealings with commercial and government entities. As a result, individuals may act in ways that jeopardize their personal privacy and/or threaten the authentication systems' security. The notion of separating knowledge about conduct from knowledge about identification, as proposed by Demchak and Fenstermacher (2004), might help to alleviate the conflict between privacy and security [Demchak and Fenstermacher, 2004]. According to Andersson et al., a privacy and security solution can lead to a trust solution [Andersson et al., 2005].

The secure and anonymous communication channels aid in the establishment of fundamental trust by ensuring that no data is spilled to attackers and that the user does not reveal their network address or position. Only once the other party has supplied adequate proof of its trustworthiness and once an agreement on a data handling policy and responsibility has been reached does Access Control authorize data sharing. It increases a user's confidence in the security of their personal information. In Pair to Pir networks, trust models, on the other hand, have lately emerged as a significant security risk management technique (e.g., in the identification of rogue nodes [Kumar, 2006]

### 2.5 Privacy, Personalization, Security, and Trust in E-learning

From academia to industry to cyber communities, the sphere of e-learning has grown. Today's online has undergone a significant transformation from the so-called Read-Web to a Read-Write-Web focused on participation and personalization. As a result, e-learning has evolved into a personal learning center where information is reused and remixed to meet the requirements and interests of individual students. Apart from formal or corporate learning, informal learning occurs frequently in personal networks or communities of practice, where members of a learning community both support and compete with one another, resulting in effective and relevant knowledge production. Personalization of learning refers to the delivery of a learning experience tailored to the learner's preferences [Dagger et al., 2003].

As a result of the variety of learning materials, varied cognitive capacities, varying levels of prerequisites, and different learning styles, Borcea et al. consider customization as a requirement in e-learning [Borcea et al., 2005]. Collaboration is a crucial element of learning, whether it takes place in a classroom or online. In e-learning, common goals and reciprocal advantages are identified and pursued through cooperation, according to Mason and Lefrere [Mason and Lefrere, 2003]. Collaboration reduces duplication of work and encourages creativity. According to Allan and Lawless, online cooperation can induce stress, which is connected to the collaborators' reliance on one another and their level of mutual trust [Allan and Lawless, 2003]. Trust is essential for efficient cooperation, whether it is synchronous (e.g., chat, conferencing) or asynchronous (e.g., email, blogs, threaded conversations). In a collaborative setting, privacy awareness is even more vital. “Impression management” [Patil and Kobsa, 2003] is the fundamental worry about privacy in collaborative work situations. Because users engage with other users or user groups in a collaborative environment, numerous sorts of information about them accumulate over time [Franz et al., 2006].

The majority of e-learning advances have concentrated on course creation and delivery, with little or no regard for privacy and security as essential components. Students are more aware of the privacy consequences of their online actions, and some countries have lately passed privacy legislation. The core criteria for corporate e-learning are privacy and data protection, especially when tailored systems that adapt to sensitive learner personal data are implemented. Furthermore, businesses do not want rivals to understand the specifics of the training offered, since this might jeopardize their strategic goals. In e-learning, privacy is defined as the capacity of a student to manage the circumstances in which their personal information is shared with others [El-Khatib et al., 2003].

Privacy standards are obviously vital for e-learning, as Borcea et al. point out, because they produce an impartial environment [Borcea et al., 2005]. A learner should be allowed to act anonymously or using several partial identities. The separation of activities allows learners to be unfettered and study without feeling rushed. Apart from this separation, we require deliberate linkage of information by the owner of information in order for them to establish reputation. Tutors and writers may only be acknowledged in one class in order to receive an unbiased evaluation. Simultaneously, one of the most essential goals of e-learning is to support each unique user during the learning process. Collecting and evaluating information on a specific learner is a necessity for providing good help. Because an e-learning program is designed to aid students, it cannot operate in complete anonymity [Borcea et al., 2005].

### 2.6. Philosophical Underpinnings

The positivist, interpretivist and critical research are main paradigm (Orlikowski & Baroudi, 1991). The positivist paradigm is a kind of school of thought that embraces objective genuineness which is in a single form and it’s solid. Positivist are known for approaching a research through a deductive approach. The term deductive approach starts with the worldwide/general believe of a phenomenon then narrows down to the situation in particular. Deductive approach poses hypothesis and test them. The testing of the hypothesis will give rise to the confirmation of the principle viewed by the researcher. Despite the allegation on the positivist philosophical assumption it is hard to avoid (Schrag, 1992). A descriptive study will be done which is influenced by the positivist paradigm. This study will use statistical proposition and quantitative technique in the quest to know the nature of connection between the independent and dependent variable (Lee, Hubona, & Lee, 2015)

Interpretivist: Is another school of thought which believes in the presence of multiple reality (Walsham, 1995). An interpretivist doesn't just relies on the actions exhibited, he tries to understand the motive that drives the action (Walsham, 2006). Interpretivist uses an inductive approach unlike the positivist which uses a deductive approach to investigate its study. Interpretivist position concerning epistemology and ontology is that reality is relative and multiple (Hudson and Ozanne, 1988). According to (Uduma & Waribugo Sylva, 2015), multiple interpretive reality depends on other systems for meanings; this makes it difficult to interpret in terms of reality. Knowledge acquires from interpretive research is socially constructed rather than it's been determined objectively and perceived (BOER, 2005). Interpretivist researcher always tries to avoid complicated structural frameworks adopted in positivist research, and interpretive usually adopts a flexible research structure that can modify as the research goes intense (Uduma & Waribugo Sylva, 2015). Critical research: is another school of thought in research which strives to critique the status quo, through exposure of the believes in the social system there by transforming the social condition (Mingers, 2013)

## 3. METHODOLOGY / RESEARCH DESIGN

This study seeks to adopt the positivist paradigms as it best suits this study been that it intends to seek out fact from the social phenomenon of being value free. (Ononiwu, 2015). The approach that have been found suitable for the positivist paradigms is the quantitative and deductive approach (Riege, 2003). This study will adopt a positivist research approach and a quantitative method. An in-depth review of theoretical frameworks, conceptual frameworks and relevant IS theories as it applies to the research will be done.

### 3.1 Mode of Data Collection

Online survey will be used to issue out questionnaires to the populace. The response will be analyzed using a Structural Equation Modelling. The analysis will be carried out to find answer to the research questions and create knowledge discovery relevant to the research from data collected.

## REFERENCE

1. Ononiwu, C. (2015). Mechanisms For Emergent Usage Of Adaptive Information Systems: A Critical Realist Case Of E-Financial Systems In South Africa. *University Of Cape Town*.
2. Ononiwu, C., Brown, I., & Carlsson, S. (2018). Theory Choice In Critical Realist Information Systems Research. *Association for Information Systems*, *8*, 1–28.
3. EdTech Series (2020): *Education During COVID-19 Crisis: Opportunities and*
4. *Contstraints of Using EdTech in Low Income Countries.* https://edtechhub.org/coronavirus/edtech-low-income-countries/
5. Mary Frances Rice , Patrick R. Lowenthal & Xeturah Woodley (2019): *Distance education across critical theoretical landscapes: touchstones for quality research and teaching.*
6. *Distance Learning Education*. Taylor and Francis. Pages: 319-325. https://www.tandfonline.com/toc/cdie20/current
7. Rivera, J & McAlister, M (2001): "*A comparison of student outcomes & satisfaction between traditional & web based course offerings,*" in Proceedings of the 2001 Information Resources Management Association International Conference, 2001, pp. 770-772
8. Ramona Maile Cutri & Juanjo Mena (2019): *A critical reconceptualization of facultyreadiness for online teaching Pages: 361-380*. Published online: 03 Aug 2020. https://www.tandfonline.com/toc/cdie20/current
9. Susan Stephan (2017): *Embracing Engagement Through Technology in Online Legal Education; Distance Learning* Vol 14 Issue 3 2017
10. Susan Stephan (2017): *Trust- Related Privacy Factors in E-Learning Environments*; Distance Learning Ye Diana Wang (2013): \ 345-359 | Received 30 Dec 2013, Accepted 19 Jun 2014,
11. Published online: 20 Oct 2014 https://www.tandfonline.com/doi/abs/10.1080/01587919.2015.955267 United Nationa (2020): *Policy Brief on Edi=ucation During COVID 19* sg_policy_brief_covid-19_and_education_august_2020
12. UNESCO (2020): *Distance learning strategies in response to COVID-19 school closures*. https://unesdoc.unesco.org/ark:/48223/pf0000373305?posInSet=2&;queryId=N-8ea77989-29de-4ff3-997c-eaddc678be5b
13. World Bank (2020): *Remote Learning, EdTech & COVID-19.* https://www.worldbank.org/en/topic/edutech/brief/edtech-covid-19
14. World Economic Forum (2020): *The COVID-19 pandemic has changed education forever*. This is how. https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/ Vol 14 Issue 4
15. Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267-284.
16. Engelfriet, E., Jeunink, E., Maderveld, J. (2015). *Handreiking Learning analytics onder de Wet bescherming persoonsgegevens. SURF report*. https://www.surf.nl/kennisbank/2015/learning-analyticsonder-de-wet-bescherming-persoonsgegevens.html
17. Sclater, N., & Bailey, P. (2015). *Code of practice for learning analytics*. Available at: https://www.jisc.ac.uk/guides/codeof-practice-for-learning-analytics

18. Open University UK (2014). *Policy on Ethical use of Student Data for Learning Analytics*. Available: http://www.open.ac.uk/students/charter/sites/www.open.ac.uk.students.charter/files/files/ecms/web-content/ethical-useof-student-data-policy.pdf
19. Slade, S., & Prinsloo, P. (2015). *Student vulnerability, agency and learning analytics: an exploration. Journal of Learning Analytics, Special Issue on Ethics and Privacy*
20. Steiner, C., Kickmeier-Rust, M.D., and Albert, D. (2015) . LEA in Private: *A Privacy and Data Protection Framework for a Learning Analytics Toolbox*, *Journal of Learning Analytics, Special Issue on Ethics and Privacy.* systems using blockchain technology. *Proceedings - 2019 International Conference on Advanced Communication Technologies and Networking, CommNet 2019*, (July). https://doi.org/10.1109/COMMNET.2019.8742375
21. Hassan, N. A., Aziz, N. S. N. A., & Shaikh, T. (2020). Application of biometric recognition for patient management system. *International Journal of Current Research and Review*, *12*(21), 90 94. https://doi.org/10.31782/IJCRR.2020.122128
22. Kautz, K., Jensen, T. B., Halim, H., Yusof, M. M., Prabhu, S. M., Balasubramanya Murthy, K. N.,
23. Tracy, K. (2020). Analysis of identity management systems using blockchain technology. *ISSE 2020 - 6th IEEE International Symposium on Systems Engineering, Proceedings*, *11*(1), 1–13.
24. https://doi.org/10.1080/ Luecking, M., Fries, C., Lamberti, R., Stork, W., Albuali, A., Mengistu,T., … Rl, U. (2018).
25. Biometric technology for fighting fraud in national health insurance: Ghana's experience. *19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks,*
26. *WoWMoM 2018*, *3*(July), 89–96. https://doi.org/10.1109/WoWMoM.2018.8449762
27. Mafarage, A., Bieda, A., Gray, S. L., Hassan, N. A., Aziz, N. S. N. A., Shaikh, T., … Becker, J. (2020).
28. Kinship , Familial Searching and Biometrics. *The Grants Register 2021*, *7*(1), 90–94. https://doi.org/10.2139/ssrn.2226594
29. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, *115*, 619–640. https://doi.org/10.1016/j.future.2020.10.0070960085X.2020.1814989