3-2023

Protecting Students: Data Privacy in the African Union

Etienne Vallée
Boise State University

Yu-Chang Hsu
Boise State University, hsu@boisestate.edu

Publication Information

Vallée, Etienne and Hsu, Yu-Chang. (2023). "Protecting Students: Data Privacy in the African Union". *TechTrends, 67*(2), 203-206. https://doi.org/10.1007/s11528-023-00834-0

Protecting Students: Data Privacy in the African Union

Etienne Vallée
Boise State University

Yu-Chang Hsu*
Department of Educational Technology
Boise State University
Boise, ID
hsu@boisestate.edu

Abstract

The adoption by the African Union of its Convention on Cyber Security and Personal Data Protection in 2014 represented a step forward to protect personal data and to ensure that data remain private and secure. This is especially important for students, who often have no autonomy in the educational technology they use. Students cannot choose why data and information is collected, nor how it is used. In this paper, the importance of data privacy in general is explored, along with a particular focus on educational data privacy. The legal implications for the protection of data privacy in Africa are then examined. In addition, the history and features of the African Union's Convention on Cyber Security and Personal Data Protection are reviewed. Finally, a summary regarding the areas that must be improved to ensure strong protection of data and privacy to support African students' educational needs is provided.

Keywords: African Union, data privacy, data protection, education

Disclosures

Funding: This is not a funded study.

Conflict of Interest: The authors declare that they have no conflict of interest.

Introduction

The Internet has fueled economic and educational development across the globe (Abdulrauf & Fombad, 2016). Information and data have become assets that can be collected, analyzed, and even traded (Prinsloo & Kaliisa, 2022), and ownership and control of data has become a business model (Komljenovic, 2022). Companies rushed into the educational market, collecting data and developing algorithms and applications deemed vital by institutions to deliver services to their students. However, as data and personally identifiable information became more granular, entities like the European Union (EU) and California reacted and imposed data privacy structures, especially in the realm of education (Prinsloo & Kaliisa, 2022). Laws and regulations in the EU and California, to name two examples, now govern how and why data can be collected and used, and include pathways to deletion (Office of the Attorney General, 2022). Several areas of the globe, including Africa, continue to lack effective data privacy protections, undermining the corresponding rights of citizens and students.

This article first explores the importance of data privacy, with a focus on educational data privacy. It then examines legal implications for data privacy in Africa. Lastly, it reviews the history and features of the African Union's Convention on Cyber Security and Personal Data Protection (CCSPDP), followed by reporting on areas needing improvement to ensure strong protection of data and privacy to support the educational needs of students in Africa.

Importance of Educational Data Privacy

Today's educational experience is replete with companies and services that collect data and information on users in exchange for specific benefits, but many questions arise. Who owns the collected data? Who controls the data? Who can access the data? These concepts remain nebulous both for students seeking education and for the institutions providing education (Komljenovic, 2022). Students contribute vast amounts of data in order to participate in educational activities without knowing exactly what happens to that data and what rights they have in accessing, correcting, or altogether deleting this information (Prinsloo et al., 2022).

Initiatives like the EU's General Data Protection Regulation (GDPR) give citizens more control over their data (Komljenovic, 2022). Similar laws have been adopted around the world, such as Brazil's *Lei Geral de Proteçao de Dados* (General Data Protection Law) and the California Consumer Privacy Act (Simmons, 2022). In most of Africa, however, data privacy and protection remain lax, and regulations are nonexistent, rarely enforced, or overly permissive (Prinsloo & Kaliisa, 2022).

This new digital frontier raises concerns about the exploitation of African educational data in a way that resembles neocolonialism and its mercantile approach of value extraction (Komljenovic, 2022; Prinsloo & Kaliisa, 2022) to the benefit of corporate offices located outside Africa (Prinsloo et al., 2022). Digital data bears an effective exploitation and storage cost of zero, allowing it to be duplicated and easily shared with the click of a button while providing marginal to no economic benefit (Komljenovic, 2022).

Legal Implications of Data Privacy for Africa

Two legal trends over data privacy regulations compete with each other. In the first trend, public education laws, which are open to public scrutiny, are migrating towards contractual laws, where data are commercially sensitive or proprietary and thus not available for public review (Komljenovic, 2022). In the second trend, data privacy is becoming a customary norm in international law, creating legal obligations for all states to apply this norm within their own borders, regardless of national legislation or data privacy treaties (Abdulrauf & Fombad, 2016).

Contractual laws frame an efficient trading marketplace. However, unlike physical assets, where property rights remain with the object, digital assets can be sold and purchased multiple times, with the owner receiving payment for each transaction, and remaining valuable over time (Komljenovic, 2022). And unlike commodities, where high prices lead others to enter the marketplace, intellectual property rights and copyrights limit the participation of other players (Komljenovic, 2022). Students interact with contractual laws when they must use institutional platforms to receive the benefits of an education. Students have no options but to agree to the terms of service and the commercial use of their data beyond their own control.

The second trend affecting data privacy is the application of customary norms, internationally recognized obligations that arise from the establishment of international practice, instead of deriving from adopted treaties (Legal Information Institute, 2022). Currently, no binding international treaties deal with data privacy (Zalnieriute, 2015). Countries are not obligated to abide by any requirements for data protection imposed by other countries. However, privacy has been recognized as a right over the last several centuries through implementation in internationally binding agreements such as the United Nations' Universal Declaration of Human Rights (United Nations, 1948)

Customary norms guide supranational agreements like GDPR, which regulates how Europeans' personal data are managed, how they can be transferred beyond European borders, and how data can be retained and deleted (Georgiado et al., 2019; Makulilo, 2021), unifying a once fragmented field of norms and requirements. Further mechanisms restrict data transfer beyond the EU to another country, unless that country's legal framework complies with GDPR requirements (Makulilo, 2021).

Current customary norms guiding data privacy in Africa have not been created from traditional national political, social, and cultural structures (Tshiani & Tanner, 2018), but come from the private sector as non-binding and easily modified instruments (Abdulrauf, 2021). The African Union addressed this challenge by drafting the CCSPDP, which will provide a "legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data and to punish any violation of privacy without prejudice to the principle of free flow of data" (African Union CCSPDP, 2014, p. 13). However, CCSPDP will only become legally binding when 15 member countries ratify it (Abdulrauf, 2021), something that to date has not happened.

The African Union's Proposed Data Privacy Plan

The CCSPDP was adopted by the African Union in 2014 (CCDCOE, 2014). Civil society organizations and many private sector entities deemed the original 2011 draft too tolerant of restriction on privacy and freedom of speech imposed by more repressive countries (CCDCOE, 2014). Changes were recommended and implemented in the treaty's final version (CCDCOE, 2014). CCSPDP devises a legal framework to address electronic transactions and regulating e-commerce, data privacy and the protection of personal data, and the prevention of cybercrime (CCDCOE, 2015). CCSPDP features many privacy principles contained in the EU's GDPR, including data security, sensitive data protection, and lawful data processing protecting human rights, especially the right to privacy (Abdulrauf, 2021), while imposing financial constraints on violators (Gwagwa, 2014).

Several weaknesses undermine CCSPDP. First, CCSPDP does not rely on an independent judiciary system capable of conducting effective oversight of state and corporate activities (Gwagwa, 2014). Second, CCSPDP places national sovereignty as the supreme authority to protect data privacy. Articles 25.1 and 25.2, for example, contain provisions that are to be implemented as "each State Party … deems effective" or "deems necessary" (African Union CCSPDP, 2014). This deferral to member states runs the risk that countries could comply with the language of CCSPDP while abusing their citizens' privacy (Gwagwa, 2014). Third, some language is ill-defined, permitting draconian interpretations to suppress safeguards put in place by CCSPDP. For example, Article 29.3.1 makes it a criminal offense to use a computer network to insult a person for membership to a group (African Union CCSPDP, 2014), without defining the word insult. Finally, CCSPDP does not explicitly set a minimal legal threshold, allowing countries to decide how much or how little of CCSPDP to observe (Gwagwa, 2014). Unlike GDPR, the current CCSPDP offers little in the way of supranational enforcement or compliance requirements.

Technical expertise and enforcement of data privacy legal norms cost money, and many African nations are leery of spending resources on an issue which does not seem relevant or attended to by African citizens on a daily basis (Abdulrauf, 2021). Politicians and bureaucrats do not have a firm understanding of the concepts of data privacy, and do not perceive the lack of protection as a threat (Abdulrauf, 2021).

Conclusion

With data moving across borders instantaneously, supranational organizations like the African Union must take the lead in securing data privacy rights for their citizens, regardless of where the data is housed. Without legally binding protection from abuse, student privacy is at high risk of being undermined. The African Union's CCSPDP demands improvements to protect student data and facilitate the continued growth of educational technology usage, but remains non-binding until enough signatories have approved it. Binding treaty obligations will force African states to provide better digital data privacy protections for students throughout Africa.

The African Union must be proactive in implementing enforceable data privacy protections. It must convince member states to sign CCSPDP to provide continent-wide protections that promote data privacy implementation, compliance, and enforcement. It must legally and financially penalize violators while at the same time encourage new services that support education. It must also seek revisions to improve areas of CCSPDP that are lacking or that could be misinterpreted or abused by countries. Only through such a legally binding agreement will begin the meaningful development of protecting the privacy of students throughout the continent.

References

Abdulrauf, L. A. (2021). Giving "teeth" to the African Union towards advancing compliance with data privacy norms. *Information & Communications Technology Law, 30*(2), 87–107. https://doi.org/10.1080/13600834.2021.1849953

Abdulrauf, L. A., & Fombad, C. M. (2016). The African Union's data protection Convention 2014: A possible cause for celebration of human rights in Africa? *Journal of Media Law, 8*(1), 67–97. https://doi.org/10.1080/17577632.2016.1183283

African Union CCPSPDP. African Union. (2014, June 27). Treaties and Other International.

CCDCOE. (2014, July 14). *African Union adopts Convention on Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/incyder-articles/african-union-adopts-convention-on-cyber-security/

CCDCOE. (2015, February 20). *Mixed feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/incyder-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/

Gwagwa, A. (2014, July 21). The African Union Convention on Cybersecurity and Personal Data Protection (the "Convention"). *Zimbabwe Human Rights International Office Bulletin*.

Komljenovic, J. (2022). The future of value in digitalised higher education: Why data privacy should not be our biggest concern. *Higher Education, 83*(1), 119–135. https://doi.org/10.1007/s10734-020-00639-7

Legal Information Institute. (2022, July). *Customary international law*. Cornell Law School. https://www.law.cornell.edu/wex/customary_international_law

Makulilo, A. B. (2021). The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius. *The International Journal of Human Rights, 25*(1), 117–146. https://doi.org/10.1080/13642 987.2020.1783532

Office of the Attorney General. (2022). *California Consumer Privacy Act (CCPA).* State of California Department of Justice. https://www.oag.ca.gov/privacy/ccpa

Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology, 53*(4), 894–913. https://doi.org/10.1111/bjet.13226

Prinsloo, P., Slade, S., & Khalil, M. (2022). The answer is (not only) technological: Considering student data privacy in learning analytics. *British Journal of Educational Technology, 53*(4), 876–893. https://doi.org/10.1111/bjet.13216

Simmons, D. (2022, January 13). 17 *Countries with GDPR-like data privacy laws*. Comforte. https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws

Tshiani, V., & Tanner, M. (2018). South Africa's quest for smart cities: Privacy concerns of digital natives of Cape Town, South Africa. *Interdisciplinary Journal of E-Learning & Learning Objects, 14*, 55–76. https://doi.org/10.28945/3992

United Nations. (1948). *Universal declaration of human rights*. United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

Zalnieriute, M. (2015). An international constitutional moment for data privacy in the times of mass-surveillance. *International Journal of Law & Information Technology, 23*(2), 99–133. https://doi.org/10.1093/ijlit/eav005