

Africa's Ed-Tech Platforms: Protecting Children's Right to Privacy

Rachel Achieng' Odhiambo,* Emmah Wakoli,** & Michelle Rodrot***

I. EXECUTIVE SUMMARY

In the past decade, there has been a significant increase in the use of educational technology (Ed-tech) platforms in the African continent, with an estimated two hundred and twenty-four billion US dollars being spent on education in Africa today (Bouhaj, 2021). This figure is projected to increase to seven hundred and forty billion US dollars by the year 2030, at a compound annual growth rate of about fourteen per cent. The spending on Ed-tech will increase from one per cent as it was in the year 2021 to somewhere between six and ten per cent by the year 2030, estimated to reach fifty-seven billion US dollars (Bouhaj, 2021).

Ed-tech platforms are used to create a more engaging, inclusive, and individualized learning experience. A number of these platforms utilize Artificial Intelligence (AI). AI-enabled learning tools and approaches have revolutionized the global education sector (Pedro *et al.*, 2019). They have been recognized for their contributions to enhancing the quality of learning and teaching. AI aids teachers and students in their lessons (Pedro *et al.*,

* Rachel Achieng' Odhiambo holds an LL.B. from Kabarak University in Kenya and a Postgraduate Diploma from Rwanda Institute of Legal Practice and Development. She is also an advocate of the High Court of Kenya.

** Emmah Wakoli is a law graduate from Strathmore University. Legal research intern at the Centre for Intellectual Property and Information Technology Law (CIPIT).

*** Legal intern at Centre for Intellectual Property and Information Technology Law (CIPIT).

2019). Additionally, AI has been lauded for its potential to boost students' knowledge and learning habits, while also creating a more personalized approach to learning (Pedro *et al.*, 2019).

There are several AI-powered education technology companies that have been adopted in various regions of Africa. These include Knowledge AI in Mauritius (About KAIT - KAiT, 2022), Gradely in Nigeria (About - Gradely, n.d.), and Zedny in Egypt (About Zedny, n.d.), among others. A number of these Ed-tech platforms are highlighted on the Centre for Intellectual Property and Information Technology Law (CIPIT) AI application dashboard, which displays Ed-tech platforms in use in Africa that are developed by AI developers in Africa (Mapping of AI Applications in Africa, 2021). These platforms use AI to improve education and learning for children in their respective countries and beyond.

Article 1 of the United Nations Convention on the Rights of the Child (UNCRC) defines a child as 'every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier.' In essence, children's rights are human rights that protect the child as a person. In the digital realm, these rights are primarily concerned with the right to privacy. Article 16 of the UNCRC further states that no child shall be subjected to an arbitrary or unlawful invasion of privacy.

The primary audience for this brief is corporations. Although, children's rights to privacy are a collective responsibility of the parents, legal guardians, and other individuals legally responsible for the child. In the Ed-tech space, this responsibility extends to AI platform owners, who manage the platforms, and policymakers and regulators concerned with data protection and children's rights.

Data protection and privacy laws such as Nigeria's Data Protection Regulations (2019) and Kenya's Data Protection Act (2019), either explicitly or impliedly, stipulate that any data controller or processor, in this case, the Ed-tech platforms, needs

to display a privacy policy. The privacy policy should identify: (i) the platform owner, (ii) the data collected, (iii) the legal basis for the collection, (iv) the purposes of collection, (v) third parties' access to the data, (vi) details or measures relating to the security of the transmission of personal information, (viii) user rights, and (ix) amendment and data retention procedures. However, governments, civil society organizations, and human rights organizations around the world recognize that children deserve special consideration concerning data privacy and the internet (Policy Guidance on AI for Children, 2021).

Children are less likely to read or understand privacy policies, and they may have a limited understanding of their right to privacy and data protection. In addition, they are more susceptible to marketing techniques that adults can identify. The existence of their personal information online poses potential safety and security risks. Therefore, privacy policies on Ed-tech platforms must incorporate children's rights and an understanding of their right to privacy. This includes online protection and security measures established to protect children's data.

II. INTRODUCTION

Ed-tech is a young and 'high-risk' (in terms of data) industry, given that it primarily handles sensitive children's data and is composed primarily of small and medium-sized enterprises and a handful of large corporations. The vast majority of Africa's innovative Ed-tech businesses are in their infancy (Matthew, 2021). Ed-tech platforms use AI to comprehend the learners' learning capabilities. There is no doubt that AI will play an ever-increasing role in improving the quality and accessibility of education in the coming years and beyond; however, the success of this innovation may depend on the quality and foresight of regulatory frameworks. The establishment of such a framework will necessitate an analysis of the threats and opportunities posed by its implementation to learners, who are predominantly children, as

well as to their parents and guardians, teachers and tutors, businesses, and other key stakeholders.

Therefore, there is a need to critically consider the potential risks AI-powered platforms, lacking adequate regulatory or legal governance structure, pose to children and their right to privacy (Cordeiro, 2021). This consideration must also be extended to how regulations, when implemented, will affect stakeholders, and how support might be designed to stimulate innovation of ethical AI-enabled Ed-tech platforms. Furthermore, these Ed-tech platforms must be completely transparent on how they intend to collect, manage, and use any data collected from their users—this is where data protection laws are applicable.

When a website or a platform is intended for children, it must comply with the standards that have been set out in national data protection laws, which are intended to safeguard children's personal information in the digital space. It is imperative to note that not all data protection laws explicitly provide for these as most are still a work in progress. Currently, several data protection laws in Africa have specific mandates that address the protection of children's personal information. There are also several countries on the continent that are making efforts to develop online protection frameworks for children such as Kenya which recently invited comments for the Child Online Protection Guidelines (2022). If personal information is collected from a child, parental consent is required as a matter of general policy which is guided by article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC) (1990). The right to privacy is addressed in article 10 of the ACRWC and it states that no child shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, or to attacks on his honour or reputation, provided that parents or legal guardians have the right to exercise reasonable supervision over their children's behaviour. Data collection in this context refers to requesting information from users in order to create an account, profile, or make a purchase, as well as the use of tracking

cookies and data sharing with third parties. This is information that should be presented in a privacy policy.

A privacy policy is a statement that reveals the ways a data controller or processor, in this case, the Ed-tech platform collects, uses, discloses, and manages the data of its users (children's data). The authors identified the following requirements relating to privacy policies as guided by the standards set out in data protection laws:

1. The privacy policy should be prominently displayed on the website and easily accessible.
2. The privacy policy should have the following information:
 - i). the platform owner,
 - ii). the kind of data collected,
 - iii). the legal bases for collection,
 - iv). the purposes of collection,
 - v). third parties' access to the data,
 - vi). details or measures relating to the security of the transmission of personal data,
 - vii). users' rights,
 - viii). amendment and data retention procedures, and
 - ix). for platforms intended for use by children, statements on children's rights and parental consent.
3. Additionally, it is necessary to create a child-friendly privacy policy that a child can read and comprehend to ensure that they are aware of their rights while using the platform.

III. APPROACH

The authors analysed the privacy policies and protections afforded to children on various AI-enabled Ed-tech platforms, that

is, platforms whose software uses AI technologies such as machine learning, deep learning, natural language processing, computer vision, reinforcement learning, and other subfields of AI. The Ed-tech platforms analysed were developed and deployed on the African continent and were specifically designed for use by persons legally defined as children. The authors also compared the data protection measures, specifically the platforms' privacy policies, against national data protection laws on the processing of children's data to assess compliance.

IV. KEY FINDINGS

The primary findings from this study were as follows:

1. Eleven out of twenty-two platforms (primarily applications based in Western and Southern Africa) have privacy policies. However, only four of the analysed platforms mention children and their rights, as well as whether or how parents or guardians can actively participate by providing consent.
2. Eleven out of twenty-two platforms lacked publicly accessible privacy policies even after registering. These platforms do not display any privacy policies that users may read before registration nor are they available after registration. This raises concerns about parental consent; data collection processes; third-party data transfers, and security safeguards on children's data.
3. Except for the Nigerian Data Protection Regulation (2019), which contains a specific provision on privacy policy, the other African data protection frameworks pointed to components of a privacy policy, which the authors used as a guide to develop privacy policy principles.

V. GAPS

The following gaps were identified:

A. Lack of explicit inclusion of privacy policies

Although privacy policies are legally required by many national data protection laws, fifty per cent of the examined Ed-tech platforms lack privacy policies entirely, and in the cases where they exist, they do not address the protection of children's data or their right to privacy.

B. Lack of explicit statements on children's right to privacy in the privacy policies

Eight out of the eleven existing privacy policies completely fail to mention children's rights to privacy, let alone describe how they safeguard children's rights. There is a need to emphasize or include child-specific clauses in the privacy policy (i) for the benefit of parents, and (ii) for the benefit of the children, given that the platforms are used by children and designed for children. In addition, given that children's data could include voice, video, learning and performance capabilities, this section should include a clause stating that platform owners do not collect more data than is required for a specific purpose, and the extra safeguards, if any, that have been implemented to ensure extra protection for children's data.

The collected data cannot be subjected to automated processing of personal data or profiling as data protection frameworks, such as Kenya's Data Protection Act (2019), afford individuals the right not to be subject to solely automated decisions, including profiling, that has a legal or similarly significant impact on them. Additionally, care must be taken when using their data for marketing purposes, such as creating user or personality profiles.

C. Insufficient recognition of parental consent concerning the online protection of children

Four of the eleven privacy policies present in the platforms analysed in this study explicitly mention children. Three of the four privacy policies that mention children include policies that pertain to parental consent. With regards to children and consent, a parent or guardian must provide consent because consent cannot be obtained from the children themselves. Data protection frameworks in Africa set the general age of consent at either sixteen or eighteen years, depending on the country, meaning that a parent's or guardian's consent is required for users younger than this age. Under these data protection frameworks, it is unlawful to process any data without the consent of an adult with parental responsibility.

To ensure compliance, the platforms should use existing technology or technological measures to confirm that the parents consented and were not impersonated by their children. This could be remedied by enforcing age verification documents, like identity cards and birth certificates, and consent mechanisms within the Ed-tech platforms.

VI. POLICY RECOMMENDATIONS

Since a privacy policy is a legally binding document, all parties involved must comprehend its contents. This necessitates that it be written in a manner that is clear and simple to understand. Before signing up for these platforms, sections of the privacy policies that pertain to children should be explicitly provided and easily accessible on the platform's web page. The sections containing these policies should also include parental consent and safeguards implemented to protect children's privacy rights. The authors propose the following recommendations to satisfy the aforementioned requirements for child-specific data protection policies on AI-enabled Ed-tech platforms:

1. The platforms should ensure that a privacy policy is readily available to the public to ensure informed consent is given.
2. The inclusion of a data collection section that includes information on the type of personal information collected from children and how it is collected. It should also specify whether the data collection is through audio, video, or other formats.
3. The inclusion of a communications clause detailing whether the platform owner(s) intends to correspond, and how they intend to correspond, with the child or parent using their personal contact information. The platform owner should inform the child or parent of any personal communication they are likely to receive from the company even if the messages are not promotional.
4. A detailed list of who has access to the children's data provided, e.g., tutors, parents, platform owners, external organizations, etcetera, and if possible, how these parties use the data they access.
5. A clear and easily accessible statement detailing the rights of users who are legally defined as children. This includes providing information on the right to withdraw consent, the right to withdraw data from the platform, the right to request deletion of their data, and the right to request access to their information, among other rights, so that the children, as users, are aware of them.
6. A statement acknowledging that the platform owner(s) do not collect personally identifiable information from children. The acknowledgement should clearly state that the child user will not be asked to and should not provide their contact information or any other information that could be used to identify them.

7. A statement clearly stating the requirement of parental or guardian consent for users under a certain age (as defined and required by national laws). Information on how parents or guardians may contact the Ed-tech platform to have their children's data removed, especially if this data is obtained without their consent. A statement clearly stating that interactions between a tutor and a minor, including tutoring sessions, must take place in a supervised environment. Article 10 of the ACRWC states that parents or legal guardians have the right to exercise reasonable supervision over their children's behaviour. As such, a supervised environment is one in which the parent or legal guardian is aware of and actively monitors the child's activities on e-learning platforms.
8. The inclusion of a section informing users about the existence of third-party affiliates and detailing platform protocols in regard to sharing user information with them. The extent to which much information is shared with third parties should also be included.
9. The inclusion of a statement detailing the relevant data protection law relating to children's data protection and privacy. In addition to the applicable data protection law, reference should be made to relevant child protection frameworks that define a child and their right to privacy.

VII. CONCLUSION

There are numerous advantages to enhancing how AI-enabled Ed-tech platforms to process data in general and children's data in particular. Children are the primary stakeholders of these platforms, and given that they are essentially growing up in this era of datafication, it is likely that their data will be preserved for a long period. To realize the benefits of AI in the Ed-

tech industry, data must be collected and processed in a way that protects and preserves the rights of the children and end-users.

This study identifies risks and puts forward some recommendations to alleviate them. Firstly, Ed-tech platforms must prominently display, and adhere, to privacy policies on their websites. Second, these privacy policies must be simple for children to comprehend. This could mean the inclusion of two separate privacy policies; one intended for parents, guardians, and the general public, and another that has been simplified for children. Secondly, a statement specific to children's rights must be included in the privacy policies of all Ed-tech platforms, regardless of their approach. Lastly, these privacy policies must have certain components that give details on the collection, processing, and management of data.

While there are valuable opportunities to use AI in ways that benefit children, there are crucial questions that must be asked and answered in order to better safeguard children from the potential negative effects of AI. With mobile and desktop applications, video-based learning spaces, and social networking platforms that facilitate education, technology has had a substantial impact on education. Technology-based education is still evolving and is still in its infancy in Africa, allowing society to regulate it for the benefit and online safety of children.

REFERENCES

- About - Gradely.* (n.d.). Gradely; gradely.ng. Retrieved August 29, 2022.
- About KAIT - KAiT.* (2022, April 24). KAiT; www.kaitsolutions.com.
- About Zedny.* (n.d.). Zedny; zedny.com. Retrieved August 29, 2022.
- African Charter on the Rights and Welfare of the Child, (1990).
- Bouhaj, K. (2021, August 10). *EdTech in Africa: A Landscape. Published by GSV Ventures, Kenza Bouhaj, Medium.*
- Child Online Protection Guidelines (2022).
- Cordeiro, V. C. (2021, June 15). *Educational technology (EdTech) and children's right to privacy - Humanium.*
- Data Protection Act, (2019, Kenya).
- Mapping of AI Applications in Africa.* (2021, July 9). Centre for Intellectual Property and Information Technology Law; cipit.strathmore.edu.
- Matthew, J. (2021, September 15). *A look at the increasing relevance of the global edtech industry.* Techpoint Africa; techpoint.africa.
- Nigeria Data Protection Regulation, (2019, Nigeria).
- Pedro, F., Subosa, M., Rivas, A., & Valverde, P. (2019, 0 0). *Artificial intelligence in education: challenges and opportunities for sustainable development.* UNESDOC Digital Library.
- Policy guidance on AI for children.* (2021, November 19). UNICEF Office of Global Insight & Policy; www.unicef.org.