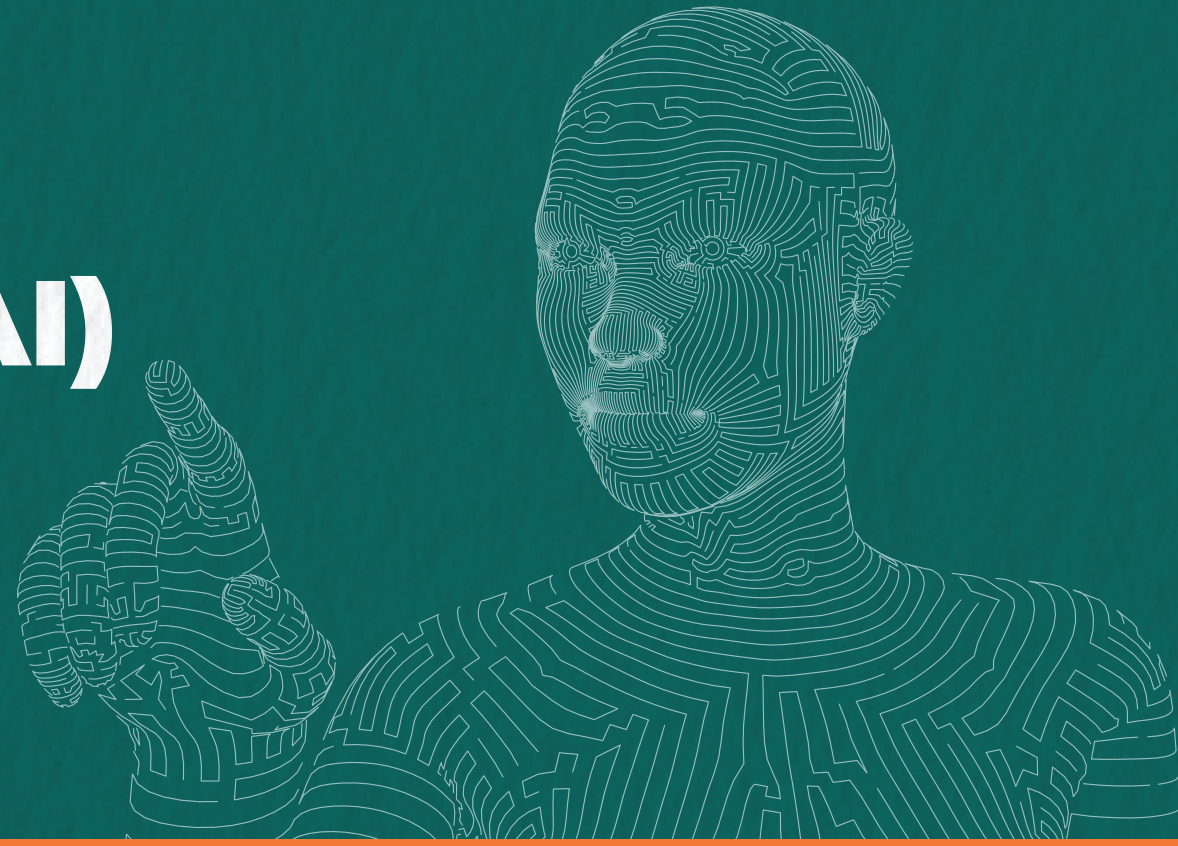


Gendered aspects of Artificial Intelligence (AI)

and its impact on Data protection for women and girls in Africa.



In the ever-evolving digital space, the intersection between Artificial Intelligence (AI) and privacy has become a complex concern, raising questions about the balance between innovation and safeguarding personal information. In 1956, John McCarthy¹, a young Assistant Professor of Mathematics at Dartmouth College invited a group of people to clarify and develop a machine that thinks and acts like human beings which drove the development of the first Artificial Intelligence programming language and ultimately the invention of artificial intelligence technology. Ever since, the narrative on artificial intelligence and scope of advancement has tremendously changed due to the emergency of computers with strong computing power in 1946. What is not known to us is whether gender issues were also considered during the process of invention.

As Artificial Intelligence continues to stand as a transformative force in society, it is crucial to recognize and address the gendered implications of their implementation, particularly in regards to data protection for women and girls in Africa. In this blog, we delve into the intersection of gender, AI, data protection and also examine the unique challenges and opportunities faced by women and girls in Africa in this ever-evolving digital landscape.

In Uganda, the intersection between Artificial Intelligence and data privacy has gained a lot of relevance, reflecting the impact of AI on various aspects of society,





including data protection. Uganda is currently witnessing the adoption of AI across sectors such as healthcare, finance, education and leadership. For example, many contemporary tools adopted include; AI-driven diagnostic tools like Flo used by women and girls for menstrual and pregnancy tracking, Chatbots like Siri, virtual assistants for customer service in the banking sector, personalised learning platforms like ChatGPT that adapt to students' individual needs and AI applications for crop monitoring and yield prediction like FarmBeats by Microsoft.

Although these bring about advancements, there are high chances of individuals' data privacy breach.

Globally, the relevance of AI and privacy intersects with the increasing integration of AI technologies into our daily lives. From smart cities to personalised digital services, the



global landscape reflects an increase in AI-driven applications. For example, Amazon employs algorithms to provide personalised product recommendations based on users' browsing and purchasing history, streaming platforms like Spotify and Netflix utilise AI to create personalised playlists and recommend movies based on user preferences, fitness apps like Apple Health use AI to analyse user data, provide personalised workout plans and offer health insights.

However, this increases the need for strong privacy frameworks that can adapt to the evolving challenges caused by technological advancements.

Gender and Data Protection and Privacy Concerns

Governments and regulatory bodies worldwide are trying to recognize the evolving intersection between AI and privacy. Regulations such as the General Data Protection Regulation (GDPR) in Europe, Data Protection and Privacy Act 2019 in Uganda and other similar

regulations globally aim to set standards for the responsible use of personal data. However, the rapid technological advancements often tend to outcompete the regulatory frameworks, leaving gaps that must be quickly addressed to protect individuals especially women and girls from potential privacy infringements. Navigating these regulatory gaps requires a deep understanding of both the capabilities of AI and the requirements of data privacy and protection for all groups of people who interact with these technologies.

The ability of AI to analyse heavy databases, extract patterns, and make predictions raises various privacy concerns. The adoption of AI in various sectors also presents potential threats to personal privacy. Its ability to collect and store large amounts of data raises questions about the ethical boundaries of data collection and storage such as consent about sexual life, reproductive health and data privacy concerning children. This was noted during a two-day workshop organised by WOUGNET on Assessment of Data Protection and Privacy Act, 2019 in compliance with the African Union Data Protection Framework, 2022.

The use of AI-powered surveillance systems such as facial recognition technology, CCTV cameras in public spaces or for law enforcement purposes raises concerns in Uganda. Unauthorised or indiscriminate surveillance

compromises an individuals' privacy, leading to unwarranted tracking and illegal profiling. These facial recognition systems tend to perpetuate gender biases, particularly against women and girls.

For instance, Ms. Christine Nampeera was indiscriminately surveilled with her partner by unknown people during their private time in one of the hangouts in Kampala but the public biases and ridicule was orchestrated to Nampera not the man whom she was together with at the time of capturing the video. This led to violent criticism and abuse of rights tilted towards Nampera because of her being a woman since the society is nurtured on violence towards women. Rapid adoption of WhatsApp in Uganda and use of X-space escalate the distribution of such videos without consent making it harder for law



AI applications in healthcare and sexual care like Flo, although beneficial for diagnostics and treatment, may involve processing of sensitive personal health and sexual life data beyond the minimality prescribed in the African Union Data Protection Framework 2022 or the Uganda National Data Protection and Privacy Act, 2019. Improper or unauthorised access to this data poses significant privacy threats. For example, if health or sexual records are not well protected, it could lead to the exposure of individuals' histories. During the workshop organised by Women of Uganda Network, a female participant expressed her dissatisfaction with the way personal health information is handled by hospitals and other health centres in Uganda.



The AI algorithms used in the financial sector for credit scoring and risk assessment may pose serious threats to personal financial data. Despite the fact that these algorithms promote financial inclusion in mobile banking and digital lending platforms, they also raise concerns about data privacy for women and girls. There is a risk of bias and discrimination when it comes to giving loans and various service provisions, as well as concerns about the transparency and effectiveness of the mode of data collection, practically impacting women's financial privacy.

For instance, Google, Instagram, Facebook and Pinterest utilise the user's search history to personalise advertisements. While this enhances targeted

advertisement relevance, it raises privacy concerns as users' search questions and preferences are used to tailor advertisements without clear opt-out mechanisms oftentimes. Therefore, if a user does not clear their search history, they may face targeted breach of personal data.

Best Practices to ensure gender inclusion and privacy protection

Transparency: Governments and regulatory bodies should enact and enforce laws that promote gender equality and data privacy especially for women and girls. These laws should be clear and understandable i.e. in all the regional and national languages for easy interpretation. This builds trust and enables users to make informed decisions on which technology to use for what purpose. Policy makers should also ensure that they implement clear laws that tackle AI.

Fairness: Actively address biases in AI systems to ensure fair outcomes for all users, irrespective of their age, gender, ethnicity and geographical location. This can involve regular auditing and testing of algorithms to identify and rectify biases through reviewing users' experience.

Consent: Seek and obtain consent before collecting and using their data for AI applications. Users should be aware of how their data will be used and as a data collector, you should only collect information that you need.

“When collecting data, ensure to use the principle of minimality which emphasises that a data collector must only collect data that they find relevant. You cannot start

asking a data subject about their sexual life if you are collecting data about agriculture” Anthony Masake, a legal officer at Chapter Four Uganda highlighted during a data protection and privacy workshop organised by Women of

Uganda Network with support from the Association for Progressive Communications. The workshop was attended by policy makers, law enforcers, journalists, civil society organisations, private sector, academia and internet users.

Seeking consent may also include provision of opt-in/opt-out options so as to ensure that users have control over the use of their personal information.



Accountability: Clearly explain to the users why you are developing that particular AI and how safe their data is with you. Also, be accountable for any personal violations.

Conclusion

As we witness and embrace the full potential of Artificial Intelligence in different sectors, we should not under look the fact that these innovations come hand in hand with some challenges which mostly affect the marginalised group of people i.e. women and girls, thus the need for powerful legislations and informed global dialogues. Therefore, we have to be vigilant and pay attention to the privacy and ethical concerns that may arise. The examples highlighted in this blog showcase the global impact of AI on our daily lives, especially women and girls.

By fostering global dialogue, we can collectively address the ethical considerations surrounding AI in terms of privacy, promote transparency in data collection and usage, and protection of individual privacy. It is through collaborative efforts that we can address AI and privacy challenges and create a digital space that respects and protects individual rights regardless of their gender, ethnicity, religion, age and geographical location.

Written by;

Irene Marunga Katushabe

Communications Associate, WOUGNET

