

THE REPORT ON PRIVACY IN THE DIGITAL AGE

To: UN Human Rights Office, The Office of the UN High Commissioner for Human Rights

From: *Knowledge House (KnowledgeHouseAfrica-KHA)*

Date: 4th June, 2022

Subject: **Report on right to Privacy in the Digital Age**

INTRODUCTION

Knowledge House (KnowledgeHouseAfrica-KHA) is delighted to submit this comment on **report on right to privacy in the digital age** ahead of the stakeholder meeting .

Knowledge House is an innovation hub spinning out social enterprises that apply ICT empowerment and support, Digital rights advocacy, Artificial Intelligence and education for improved livelihood of unconnected, underserved youth & women and unborn child . *Knowledge House as a body*, is happy to submit report **on right to privacy in the digital age**

- 1- The processing of sensitive matters should move beyond consent and place the privacy burden on companies by focusing on Fair Information Principles like data minimization, use limitation, and privacy by design, even if those requirements affect online business models.
- 2- Fundamental human rights is to be respected and no to mass surveillance systems or unlawful targeted surveillance programs. Emerging technologies should not be used to create mass surveillance systems or unlawful targeted surveillance programs”. This is because of the need to protect human rights when addressing emerging technologies. Human rights, such as rights to life, liberty, security, privacy, and expression, should be at the center of the debate for emerging technologies including artificial intelligence-powered systems and tools that employ discriminatory algorithms. Emerging technologies should not be used to create mass surveillance systems or unlawful targeted surveillance programme.
- 3- The developer and the deplorer of automated decision making system to subject to legislation on fundamental rights e.g. Data protection, privacy, non – discrimination, consumer protection, product safety and liability rules.
- 4- Data processing whether or not by automated means should ensure consideration of human rights concerns.
Online service providers should make clear which decisions are made with human review and which by automated means systems alone. This information should be accompanied by explanations of the decision-making logic used by algorithms. Further, the “existence, purpose, constitution and impact” of automated decision making and profiling systems

should be disclosed in an effort to improve the level of individual users' education around this topic.

They should make available and publicise data on the “frequency at which automated decision making and profiling systems are subject to complaints and requests for remedies, as well as the types and effectiveness of remedies available. Effective remedy processes are to end human right violation.

Bills should be responsible for creating a legislative framework hospitable to a pluralistic information landscape, preventing technology monopolies and supportive of network and device neutrality.

Lastly, useful tools to oversee automated decision making and profiling development:

1. human rights impact assessments performed prior, during and after the use of automated decision making and profiling systems;
 2. external audits and consultations with human rights organisations;
 3. enabled individual choice thanks to notice and consent;
 4. effective remedy processes to end human rights violations.
- 5- Human rights protection policies must be put in place to protect the vulnerable and marginalized. Why?

Data privacy breaches are among the most important ways in which automated decision making and profiling systems can be used to infringe human rights. Globally, there is also a growing adoption of automated decision making and profiling applications for human resource recruiting, credit assessment and even the administration of criminal justice.

These critical decision-making roles, which were once the preserve of humans, have enormous consequences for those affected by the decisions. The biggest concern with deploying these systems is the bias inherent in the algorithms that underlie automated decision making and profiling. These algorithms are usually formed with data that excludes members of a population. This leads to decisions and results that further exacerbate marginalization.

- 6- Ensure the creation of systems of transparency, liability, explainable, accountability, justification, and redress for decisions made on the basis of automated decision making; and profiling from data as greater data protection can protect individual privacy, and empower people to better participate in automated based decision-making and economic activities that use their data.
- 7- There is need to understand the potential misuses and abuses, unintended consequences, biases in sociotechnical systems, and even the costs of not deploying a tool when it may help someone in need. Human rights provide those working on automated decision making and profiling with a basis for understanding why governing systems – from technical standards to policy – should address values like nondiscrimination, Political Participation, Privacy, Freedom of Expression, The Disability Rights Approach and Accessible Design a law that aims to help ensure that algorithms used by city agencies are transparent, fair, and valid by setting up a task force to make recommendations on algorithmic regulation, transparency, and bias.
- 8- The commission should ensure anyone involved in data processing or the control of data shall develop security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing

organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

- 9- Provisions should be made for end-to-end encryption, which ensures the privacy of the contents of communications and the security of everyday transactions, is integral to the security infrastructure of the internet and crucial for maintaining trust in the digital economy. It is also essential for protecting the privacy of people at heightened risk, such as journalists, human rights, defenders and whistle-blowers, and members of other oppressed or marginalized groups.
- 10- The Office of the UN High Commissioner should protect human rights, right to explanation and hold platforms accountable in content governance. Given the rise and weaponization of algorithmically curated services and the prevalence of harmful content online, government and the private sector needs to take further action to protect users of online platforms. The bill should work toward implementing approaches that align with international human rights standards, while also striving to protect the right to free speech. Platforms should retain the ability to moderate their services, as otherwise online spaces are likely to become more harmful, especially for users-at-risk and underrepresented groups. Online platforms, however, should create meaningful transparency and accountability mechanisms in their content moderation and content curation practices.
- 11- 7 key requirements recommended for automated decision making and profiling system are: Human agency and oversight; Technical robustness and safety; Privacy and data governance; Transparency; Diversity, non- discrimination and fairness; societal and environmental wellbeing; and Accountability.
- 12- The Office of the UN High Commissioner should support ethically aware and human – centered data collection and analysis. It should make provisions to create governance and testing methodologies to address mistakes and inaccuracies. Companies need to put the needs of individual at the Centre of data innovation.

Conclusions and Recommendations

As indicated in this report, we believe that it is necessary to further ensure state and non state do carry out various impact assessments of AI on human rights. However, at this stage, we call on states to:

We also call on states and companies to:

Review the adequacy of existing frameworks and regulation: Different types of AI and different domains of application raise specific ethical and regulatory human rights issues. In order to ensure that they protect individuals from the risks posed by AI, existing laws must be reviewed, and if necessary amended, to address the effects of new and emerging threats to privacy and freedom of expression.

Ensure protection of international human rights standards: The development, use, research and development of AI must be subject to the minimum requirement of respecting, promoting, and

protecting international human rights standards. This should include developing an understanding of what constitutes 'AI human rights critical systems' and ensuring that laws and regulations, codes of conduct, ethical codes, and self-regulatory and technical standards meet the threshold set by international human rights.

Ensure accountability and transparency: Corporate, technical, and state actors must allow for meaningful multi-stakeholder participation, including civil society actors, in setting technical standards, regulation, and industry guidelines for AI systems, technology policy and industry standards to ensure transparent processes and legitimacy of outcomes. In particular, non-binding frameworks must be accompanied by strong accountability and oversight measures.

We also call on civil society to:

Continue to engage in order to mitigate any potential negative impact on fundamental rights such as freedom of expression and privacy. This will require a thorough understanding of the technology, the people involved in its development, and the context in which it is used.

Collect and disseminate 'human rights critical' case studies. AI: In order to fully comprehend the numerous ways in which AI will impact human rights, it is critical to collect and emphasize case studies that demonstrate how AI will impact human rights. These case studies must include examples from all over the world.

Create civil society alliances and expert networks: It is critical to stress the significance of developing knowledge-exchange programs and facilitating the development of cooperative strategies by civil society.

So far, academia and industry have taken the lead in advancing the debate on AI's societal impact. While civil society actors play an important role in these debates, it is critical to strengthen the voice of those working on public-interest technology.

Best regards,

'Kayode Akanni

<https://www.about.me/kayodeakanni>

<https://github.com/kayodeakanni>

<https://sites.google.com/udacity.com/intel-edge-ai-scholarship/community/project-showcase/showcase-winners>

Knowledge House (KnowledgeHouseAfrica-KHA)

Twitter: @KHAfrica