PEER REVIEW OF RESEARCH ON BIOMETRIC DATA COLLECTION, PRIVACY, AND SURVEILLANCE AND HOW IT AFFECTS DIGITAL RIGHTS IN UGANDA

TERMS OF REFERENCE

1.0 Background

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) works to defend and expand the digital civic space to enable the protection and promotion of human rights and to enhance innovation and sustainable development. With support from Enabel and the European Union, CIPESA is implementing *"The Advancing Respect for Human Rights by Business in Uganda (ARBHR) project"* which, among others, seeks to reduce human rights abuses connected to business activities in Uganda, particularly those impacting women and children.

In efforts to advance its mandate and with funding from Enabel, CIPESA is implementing a project *titled Advancing Digital Rights by Businesses in Uganda.* Under the project, CIPESA will conduct research on ***Biometric data collection, privacy, and surveillance and how it affects digital rights in Uganda*** to inform advocacy on digital rights in the business sector.

2.0 Rationale

There has been increasing governments' appetite for collecting Biometric Digital Identification (BDI) partly driven by the need to transform service delivery and enhance public participation through developing central databases. Since data is central to planning and economic transformation, the adoption of biometric data and digital identities is one way of improving efficiency in service delivery. Critical government programmes that have necessitated the collection and processing of biometrics include civil registration, issuance of National Identity cards, passports and driver licences, updating and verification of voter's registers, refugees' registration, and mandatory SIM card registration. This has driven the demand and adoption of digital identity (ID) credentials.[1]

Over recent years, Uganda has witnessed adoption of BDI. For example, the country's electoral body, the Electoral Commission (EC), was able to extract relevant data, including biometric data and demographic information, such as polling stations, from the national identification register under the stewardship of the National Identity Registration Authority (NIRA), to compile the national voters' register during the 2016 elections.[2]

However, the EC's system has been criticised with allegations of mismanagement, corruption and a lack of adequate data protection safeguards.[3] This in addition to the existence of state-facilitated mass surveillance, data breaches, and identity theft, among others.[4] Likewise, the lack of comprehensive legislative and governance structures, such as independent oversight and redress mechanisms, also exacerbates surveillance, data protection, and cybersecurity concerns.[5]

---

[1] Integrating ICT in Elections: How Uganda Implemented Biometric Voter Registration, 2001–2016 https://www.kdevelopedia.org/asset/99202207120168788/1657590791650.pdf

[2] ibid

[3] https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/serious-concerns-around-ugandas-national-biometric-id-program

[4] https://www.kdevelopedia.org/asset/99202207120168788/1657590791650.pdf

[5] https://cipesa.org/wp-content/files/Biometrics_and_Digital_Identity_in_Africa_Brief.pdf

Similarly, as businesses continue to evolve adopting the BDI model, it has posed threats to data privacy especially with telecommunication companies and Internet Service Providers (ISPs) who have aided state surveillance activities. These entities are required to facilitate surveillance, including installing equipment and software that enable governments to lawfully intercept communications on their networks, including in real-time for such periods as may be required.[6] The assistance rendered by these intermediaries facilitates targeted internet disruptions, easy access to users' data, content removals, decryption of users' encrypted data, and state surveillance based on geolocations of the users.[7]

In light of the above, CIPESA will conduct research on Biometric data collection, privacy, surveillance and its affects on digital rights in Uganda to inform policy and practice change. The research will be conducted internally and with support from an external consultant for peer review. These TORs will thus guide the external consultant, who will for purposes of this assignment, provide consultancy services during the course of the research process.

3.0 Overall objective

To provide technical peer review of the research on Biometric data collection, privacy, and surveillance and how it affects digital rights in Uganda.

4.0 Scope of work

Under the guidance of the Programme Officer, the consultant is expected to handle the following;

a) To review and provide input into the draft data collection tools for the Key Informant Interviews (KIIs) and Focus Group Discussion (FGDs)- within 2 days of receipt of data instruments.

b) To support data analysis - 6 days.

c) To undertake peer review and provide technical input into the draft report - within 5 days from the date of receiving the draft report.

d) To provide editorial services, check validity of information as well as structure and presentation style of the final report - within 2 days of receipt of the revised draft report.

5.0 Methodology

The consultant will employ qualitative design through desk research, combining policy analysis, literature review and review of primary data collected in the different regions of the research study.

6.0 Deliverables

a) Reviewed data collection tools.
b) Reviewed data analysis.
c) Reviewed draft research report.
d) Edited final research report.

7.0 Schedule of Payments

The Consultant will be paid in instalments as follows;

Sn	Item	% payment of the contracted amount for the assignment

[6] State of Internet Freedom in Africa, 2021
https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2021-Report.pdf

[7] Compelled Service Provider Assistance for State Surveillance in Africa: Challenges and Policy Options
https://cipesa.org/2023/04/compelled-service-provider-assistance-for-state-surveillance-in-africa-challenges-and-policy-options/

1.	Review of data collection tools	20%
2.	Data analysis	20%
3.	Review and technical input in the draft report	20%
4.	Edit of the final report	40%

8.0 Required Skills and Experience

a) Advanced degree in Law, international human rights law, or a related field.
b) Comprehensive understanding of digital rights, data privacy and data protection laws.
c) Excellent research, writing and presentation skills;
d) Exceptional analytical abilities and strong attention to detail;
e) Demonstrated ability to produce clear reports and guidance with in-depth analysis and strategic recommendations in the relevant fields;
f) Ability to complete complex assignments in a timely manner and deliver quality results over a short period of time.

9.0 Application Procedure

The following documents should be submitted as part of the application: Cover letter, CV, two samples of research work and a financial proposal specifying a total lump sum amount for the tasks specified in this Terms of Reference.

The proposals should be submitted via email to programmes@cipesa.org and cc. nadhifah@cipesa.org.

The deadline for receipt of applications is January 27, 2025 **at 18.00 East African Time.**