Data Collection and Surveillance by Businesses and Their Effects on Digital Rights

April, **2025**

Funded by the European Union

THE REPUBLIC OF UGANDA
MINISTRY OF GENDER, LABOUR &SOCIAL DEVELOPMENT

CIPESA

Enabel

Acknowledgement

This research study was conducted by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) under the Advancing Respect for Human Rights by Businesses in Uganda (ARBHR) Project in partnership with Enabel in Uganda and funding from the European Union.

Special appreciation to James Nkuubi (PhD) who was the lead researcher and all contributors to this research including representatives of the Ministry of Gender, Labour and Social Development (MoGLSD), Uganda Human Rights Commission (UHRC) Personal Data Office (PDPO), Private Sector Foundation Uganda - Hoima, OXFAM, Chapter Four Uganda, Women of Uganda Network (WOUGNET), Initiative for Social and Economic Rights (ISER) Pollicy, Federation of Uganda Employers (FUE) Uganda Fish Processors and Exporters Association (UFPEA), Rwenzori Rare Metals (RRM), Petroleum Authority of Uganda (PAU) - Hoima, Total Energies - Buliisa & Hoima, Stanbic Bank - Buliisa, District Local Government Officials as well as Small and Medium-sized Enterprises in Albertine, Busoga and Kampala Metropolitan.

EXECUTIVE SUMMARY

The global digital revolution has rapidly transformed business operations, making data a vital commodity for economic growth and competitiveness. As Uganda's digital landscape expands, businesses are increasingly collecting personal and biometric data to offer innovative services across sectors like banking, health, agriculture, and fintech. However, this surge presents significant challenges related to data privacy, security, and related human rights violations. Efforts such as the African Union Convention on Cyber Security and Personal Data Protection aim to establish regional standards, while many countries, including Uganda, have enacted national laws to regulate data management. Despite these frameworks, enforcement gaps persist, raising concerns over responsible data handling. This study, carried out in 2025, investigated how Ugandan businesses collect, process, and utilise data, particularly biometric data, and how these practices impact digital rights, privacy, and security.

The study sought to examine how the current data collection, privacy, and surveillance policies and practices by businesses affect digital rights in Uganda. More specifically it a) Interrogated the policies, where available and practices of biometric data collection, privacy, and surveillance in the business sector in Uganda; b) examined how businesses collect, process, and utilise data (including that of a biometric nature); c) examined how these processes of collecting, processing and utilising data impact users' privacy, and the potential infringements on digital rights arising from surveillance practices; and d) through strategic recommendations, inform advocacy efforts to foster accountability and promote a digital environment that respects and protects individual rights.

A mixed-methods approach was employed, integrating literature review, field data collection across six districts of focus, 35 key informant interviews (KIIs), six focus group discussions (FGDs) - with stakeholders including business leaders, data protection experts, academia, civil society, policymakers and Government Ministries, and case studies. A comprehensive legal and policy critique was also undertaken on the existing policies, administration regulations and rules, and laws governing Uganda's biometric data and digital rights spectrum.

In relation to geographical scope, the study covered the Albertine and Busoga regions, and Kampala Metropolitan area. Specifically, it focused on six districts - Iganga and Jinja in Busoga; Hoima and Buliisa in Albertine; and Kampala and Wakiso in central Uganda.

Findings reveal that businesses commonly collect biometric data for security, identification, and operational efficiency. Examples include fingerprint data in banking, facial recognition in surveillance and national ID verification, and behavioral monitoring technologies. These practices are driven by legal compliance, government digitalisation policies, and security needs.

Despite significant strides made in the establishment of the data privacy and protection frameworks, there are a myriad of challenges that remain ranging from weak oversight, enforcement, resource limitations that continue to undermine effectiveness of these frameworks. At business level, there are growing concerns about the ethical use of such data, especially regarding informed consent, opacity of data practices, excessive data collection and misuse of data for surveillance and profiling. However, these are attributed to limited understanding of policies and regulations, technological deficiencies, absence of robust data security mechanisms and resource constraints.

The study concludes that collaborative efforts are required among all stakeholders particularly, government, civil society, and private sector organisations to establish robust frameworks that ensure biometric data is collected, processed, and stored securely and ethically. By implementing clear policies, investing in training and technology, and fostering transparency, there is a significant opportunity to reduce privacy risks and build public confidence in biometric and data collection practices.

Recommendations

a) Businesses/Companies

- Develop and implement comprehensive policy and legal compliance frameworks guaranteeing data protection at all stages of processing - collection, storage, usage and destruction.
- Promote a framework of data collection that guarantees and protects informed consent.
- Establish data storage, retention and destruction policies.
- Develop and implement data security/protection frameworks.
- Establish and consistently implement education and awareness programs.

b) Government of Uganda/Regulatory bodies

- Undertake a comprehensive review of the contemporary challenges in data protection for alignment with both national and international standards, balancing the diversity of human rights and freedoms that could be affected by intrusive policies.
- Enhance the active enforcement of the prevalent policies for instance through inspections, periodic audits, and penalties where there are established violations.
- Facilitate sustained public awareness campaigns on biometric data safety and management.
- Consider reduction or waiver of taxes on equipment that is used to capture data responsibly to ensure easy accessibility especially by small businesses.

C) Private Sector Associations

- Organise regular training sessions for member organisations on data privacy laws, security best practices, and emerging threats like phishing or hacking.
- Encourage member businesses to develop and implement customer education and awareness about the diverse issues concerning their data.
- Conduct continuous risk assessments related to biometric data collection.
- Undertake internal periodic data protection impact assessment and privacy audits to inform data protection mechanisms within the businesses.

d) Civil Society Organisations

- Establish and institutionalise multi-sector stakeholder collaboration and networking initiatives.
- Build public trust and awareness for a resilient accountability demanding citizenry.
- Undertake collective advocacy on emerging issues such as the recognition of the right to be forgotten.
- Develop advocacy and educational materials.
- Conduct strategic research and capacity building on data protection for businesses and the public.

1.0 INTRODUCTION

The digital revolution world over continues to swiftly transform the business world. This digital economy largely depends on the ability to harvest and harness data. This has contributed to the blossoming of the data economy, as data is now a tradeable commodity. It has also resulted in breaches of personal data , including subjects'[1] privacy and unauthorised access to data by collectors, processors, and malicious actors.

These data protection challenges dent trust in the digital space as a platform for commercial and financial activities. To counter these challenges, the African Union Convention On Cyber Security and Personal Data Protection seeks to establish a legal framework for cyber security and personal data protection in Africa as a standard for African countries to follow and adopt in their legal frameworks.[2]

In Uganda, as businesses strive to integrate technology into their operations, many have innovated and crafted more digital services.[3] Fintech has revolutionalised the banking industry while the health sector has also witnessed the emergence of digital health innovations.[4] In agriculture, traditional farm management tools are being replaced with 'precision agriculture' powered by digital innovations around crop production.[5] To thrive in the online space, these businesses have had to upscale their data intake,[6] and, the data sought is increasingly personal, and includes biometric data.

Businesses are accused of a diversity of breaches, including undertaking customer surveillance and unlawful sharing of data with third parties without authorisation by the data subject. Businesses therefore face the challenge of responsible data collection, processing, use, storage, while guaranteeing privacy and data protection.

This research examines contemporary practices of businesses in Uganda and their data management protocols to inform evidence-based advocacy and skills building to address the identified gaps.

1 According to Section 2 of the Data Protection and Privacy Act-2019, data subject means an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored;

2 Accessible at https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf

3 Michael Mukasa, 'Harnessing the power of the cloud to boost Uganda's digital transformation', October 18, 2024. Accessible at https://liquid.tech/uganda-digital-transformation/

4 Walter Mwesigye, 'Digital health: A new era for healthcare in Uganda', The Daily Monitor, February 22, 2025. Accessible at https://www.monitor.co.ug/uganda/magazines/healthy-living/digital-health-a-new-era-for-healthcare-in-uganda-4936614#story; See also https://www.rocketdigitalhealth.com/

5 Serita Eregwa, 'From field to farm: How digital innovation is transforming precision agriculture in Uganda', Plantwise, August 8, 2025. Accessible at https://blog.plantwise.org/2025/08/08/from-field-to-farm-how-digital-innovation-is-transforming-precision-agriculture-in-uganda/

6 Oloruntosin Tolulope Joel and Vincent Ugochukwu Oguanobi, 'Data-driven strategies for business expansion: Utilizing predictive analytics for enhanced profitability and opportunity identification,' International Journal of Frontiers in Engineering and Technology Research, 2024, 06(02), 071–081. Accessible at Article DOI: https://doi.org/10.53294/ijfetr.2024.6.2.0035

1.1 GENERAL OBJECTIVE OF THE STUDY

The study sought to examine how the current data collection, privacy, and surveillance policies and practices by businesses in Uganda affect digital rights.

1.2 SPECIFIC OBJECTIVES

a. Interrogate the policies and practices of biometric data collection, privacy, and surveillance in the business sector in Uganda.
b. Examine how businesses collect, process, and utilise data (including that of a biometric nature).
c. Examine how collection, processing[7] and utilisation of personal data impacts users' privacy and digital rights.
d. Inform advocacy efforts to foster accountability and promote a digital environment that respects and protects individual rights.

7 According to the Data Protection and Privacy Act-2019 and as shall be used in this report, "processing of data" means any operation which is performed upon collected data by automated means or otherwise including —
(a) organization, adaptation or alteration of the information or data;
(b) retrieval, consultation or use of the information or data;
(c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
(d) alignment, combination, blocking, erasure or destruction of the information or data

2.0 STUDY METHODOLOGY

The study adopted a mixed-methods approach, combining qualitative and quantitative methodologies.

2.1 Literature review

The study undertook literature review on the state of digital rights and business models in Uganda through analysis of existing studies, reports, and academic articles on biometric data collection, privacy, and surveillance. This literature informed the development of the field data collection tools and informed the analysis in this report.

2.2 Field data collection

The national scope of the study was representative, encompassing diverse regions and stakeholders across the country. Data was collected from six districts across three regions, specifically, Iganga and Jinja in Busoga; Hoima and Buliisa in Albertine; and Kampala and Wakiso in central Uganda. A total of thirty-five (35) Key Informant Interviews (KIIs) were conducted in the target regions with stakeholders including business leaders, data protection experts, academia, civil society, and policymakers and Government Ministries, Departments and Agencies (MDAs). The informants were purposively sampled due to their knowledge of the subject matter of business, human and digital rights. Additionally, six Focus Group Discussions (FGDs), targeting state actors, citizens, CSOs and business entities, were convened. Two tools guided data collection. See Annex A and B for the KII Guide and the Guide for the FGDs respectively. These tools were subjected to expert review, pre-tested in the field, and necessary adjustments made thereafter, before they were deployed.

2.3 Case studies, policy and legal analysis

The study also deployed case studies providing an opportunity to undertake in-depth examination of specific instances of biometric data collection and its consequences as observed in the country. A comprehensive legal and policy analysis was also undertaken on the existing laws, policies, and regulations governing Uganda's biometric data collection and digital rights.

2.4 Topical Scope

The study was guided by the seven principles of data protection enshrined within the Data Protection and Privacy Act, 2019 as the framework for examining the data collection, privacy and surveillance practices of the businesses. The principles are summarised below:

Image I: *Summary of the seven principles of data protection*

2.4.1 The Seven Principles Of Data Protection as provided for under Uganda Data Protection and Privacy Legal Framework[8]

A data collector, data processor or data controller or any person who collects, processes, holds or uses personal data shall consider the following principles —

a. **Accountability:** be accountable to the data subject for data collected, processed, held or used.
b. **Fairness & Legality;** collect and process data fairly and lawfully.
c. **Minimalism and Relevance;** collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data.
d. **Longevity of Keep;** retain personal data for the period authorized by law or for which the data is required.
e. **Information Quality;** ensure quality of information collected, processed and used or held.
f. **Transparency & Participation;** ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data (and
g. **Data Safety & Security;** observe security safeguards in respect of the data.

2.4.2 Legal Framework Governing Privacy and Data Protection

a) The Data Protection and Privacy Act, Data Protection Regulations & the Guidance Note on the Completion of the Annual Data Protection and Privacy Compliance Report.

The Data Protection and Privacy Act of 2019 regulates the collection, processing, storage, and sharing of personal data within the Country.[9] This legislation aims to protect individuals' privacy rights and ensure that personal information is handled responsibly and securely by both public and private sector entities.

Complementing the Act are the Data Protection and Privacy Regulations, 2021, which provide detailed guidelines and procedures to operationalise the law. These Regulations came into effect on March 12, 2021. In addition, the Uganda Personal Data Protection Office has issued occasional instructive Guidance Notices, including one issued in May 2023 and updated in January 2024 to align with the developments in data privacy.[10]

b) Digital Lending Guidelines 2024 for Tier 4 Microfinance Institutions and Money Lenders.[11]

In January 2024, the Uganda Microfinance Regulatory Authority, working with Bank of Uganda, issued the Digital Lending Guidelines, 2024 for Tier 4 Microfinance Institutions and Money Lenders. The Guidelines are targeted at any financial institution providing credit services using digital channels.[12] The guidelines protect customers' data collected by digital lending entities. Clause 9 (1) of the guidelines emphasises confidentiality, requiring digital credit providers to establish robust policies, procedures, and systems to safeguard customer information and transactions. Clause 9 (2) emphasises the importance of customer consent and places data sharing restrictions, expressly prohibiting digital credit providers from sharing customer information without their explicit consent. Additionally, under Clause 9 (3), the use of digital tools that access personal contact lists, messages, or call logs for delinquency management is discouraged, as it could compromise customer privacy and violate confidentiality principles.

Clause 9 (4) further provides that all individuals involved in the management and operation of a digital credit provider, including directors, officers, employees, and agents, are responsible for protecting customer confidentiality. Clause 9 (5) also mentions that they must refrain from divulging or misusing sensitive information during or after their engagement, except when authorised or necessary for their duties.

More progressively, Clause 14 (1) of the guidelines directs that a digital credit provider must obtain the customer's consent through a clear clause in the loan agreement when submitting or sharing credit information via a credit reference mechanism established by the Uganda Microfinance Regulatory Authority (UMRA). Clause 14 (2) also mentions that consent can be given orally, in writing, or electronically, provided the provider verifies the authenticity of the electronic consent.

8 Section 3(1) of the Data Protection and Privacy Act-2019.
9 The law came into force and commenced on 3 May 2019. The Act's short title is "An Act to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters.
10 GUIDANCE NOTE ON THE COMPLETION OF THE ANNUAL DATA PROTECTION AND PRIVACY COMPLIANCE REPORT. This is accessible at https://pdpo.go.ug/media//2024/01/Guidance-Note-on-Completion-of-the-Annual-DPP-Compliance-Report.pdf
11 Busein Samilu, 'Govt sets new rules for online money lending', The Daily Monitor, August 15, 2023. Accessible at https://www.monitor.co.ug/uganda/news/national/govt-sets-new-rules-for-online-money-lending-4336196
12 DIGITAL LENDING GUIDELINES FOR TIER 4 MICROFINANCE INSTITUTIONS AND MONEY LENDERS, JANUARY 2024 VOL. 1. Accessible at https://umra.go.ug/wp-content/uploads/2024/03/DIGITAL-LENDING-GUIDE-LINES-FOR-UMRA-2024.pdf

c) The Computer Misuse (Amendment) Act, 2022

The Uganda Computer Misuse Act was enacted in 2011, to "make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters."[13] The law was amended in 2022 to "enhance the provisions on unauthorised access to information or data; to prohibit unlawful sharing of any information relating to a child; to prohibit hate speech, the sending or sharing of malicious or unsolicited information; to regulate the use of social media."[14] This amendment provides for a number of offenses related to data infringement and general computer misuse, including unauthorised sharing of information about children under Section 23A.[15]

The law provides for the securing of access to data (Section 3); details what amounts to authorised access to data and the importance of consent in such cases (Section 5). Further, the Act provides for processes and procedures to be followed in cases of data related investigations. In particular, Section 9 (1) - (3) provides for mitigation measures such as a preservation order granted by the Court to preserve data where there exist "reasonable grounds to believe that such data is vulnerable to loss or modification." Additionally, Section 11 (1) provides for the procedures followed in criminal investigations or prosecutions that revolve around data. Thus, Section 11 (2) provides that an investigative officer can apply to court for a production order compelling a particular entity or individual to submit specific data stored in their possession or control, and service providers to submit subscriber information related to their services. The data must be provided in a form that is accessible, visible, and legible.

More prominently, Section 12 (1) - (3) also criminalises unauthorised access or interception of programmes or data without permission or authority, interference with data that causes damage or renders it ineffective, and the production, sale, distribution, or possession of devices or programmes designed to bypass data security measures. Section 12 (4) & (5) further criminalises the use of such devices to unlawfully gain access and the act of causing denial of service to legitimate users. Section 12 (6) & (7) mentions that offenses do not require intent to target specific data or programmes, and violators face penalties of fines, imprisonment, or both.

d) The Regulation of Interception of Communications Act, 2010 and the attendant regulations

This law was enacted to "provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda; to provide for the establishment of a monitoring centre; and to provide for any other related matters."[16] Section 3 authorises various Ugandan security agencies to conduct surveillance on electronic and postal communications, in the name of national security and countering terrorism. Key provisions in this law relevant to data protection include the establishment of a monitoring centre where authorised security agencies can intercept, in real-time, communications transmitted through telecommunication systems.

Section 8 (1) - (2) & (11) requires telecommunications service providers to ensure that their systems are technically capable of supporting lawful interceptions at all times. They are required to install hardware and software facilities and devices to enable interception of communications at all times or when required. Failure to comply can result in fines or cancellation of licenses. Section 9 also compels telecommunications companies to undertake mandatory data retention (including the massive bio-metric data demanded by companies) and SIM registration of their clientele and are required to retain call-related information (metadata) for six months or more.

This law remains a challenge in the guaranteeing of the right to privacy provided for under Article 27 of Uganda's constitution, as it permits surveillance of individuals' communication in a manner that weakens protections over personal data.

13 *The Computer Misuse Act, 2011, Long title.*

14 *The Computer Misuse (Amendment) Act,2022, Long title.*

15 *These include hate speech (Section 26A); unsolicited information unless in public interest (Section 26B); sending, sharing, or transmitting malicious content about others (Section 26C); Misuse of social media (Section 26D).*

16 *The Regulation of Interception of Communications Act, 2010, Long title.*

e) The Constitutional guarantees of the right to privacy

Article 27 of Uganda's 1995 Constitution recognises the right to privacy and calls for its protection. It provides that:

"(1) No person shall be subjected to—
(a) unlawful search of the person, home or other property of that person; or
(b) unlawful entry by others on the premises of that person.
(2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

The Constitution and the various laws also find inspiration from various international human rights instruments to which Uganda is a party. Having ratified those instruments, Uganda is obligated to bring its laws, policies and practices into conformity with those international instruments. They include the Universal Declaration of Human Rights,[17] the International Covenant on Civil and Political Rights,[18] the Convention of the Rights of the Child, the African Charter on the Rights and Welfare of the Child,[19] and the African Charter on Human and Peoples' Rights.

2.4.3 Institutional framework for the enforcement and implementation of the above legal framework

The National Information Technology Authority – Uganda (NITA) and the Uganda Personal Data Protection Office (PDPO) are the main entities responsible for data governance oversight.[20] The PDPO is mandated to coordinate, supervise and monitor data collectors, data controllers, data processors and data subjects on all matters relating to the personal data protection Act. In 2023, the PDPO issued a standardised template that organisations must use for their annual data protection and privacy compliance report. This template clearly delineates the specific information that all organisations subject to the law must include when submitting their reports at the end of each Government of Uganda financial year.[21]

In line with Regulation 4(b) of the Data Protection Regulations, the PDPO requires all organisations to report on their efforts to adhere to the Data Protection and Privacy Act and Regulations. Ultimately, these measures are aimed to ensure that organisations maintain high standards of data protection, and to facilitate the monitoring and enforcement of compliance across the private and public sectors.

17 Article 12 which provides that, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

18 Article 17 (1). No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2). Everyone has the right to the protection of the law against such interference or attacks

19 Article 16 (1). No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. (2). The child has the right to the protection of the law against such interference or attacks

20 Section 2 of the Data Protection and Privacy Act-2019.

21 See template accessible at https://pdpo.go.ug/media//2024/01/Data-Controller-Processor-Annual-Compliance-Report-Template.pdf

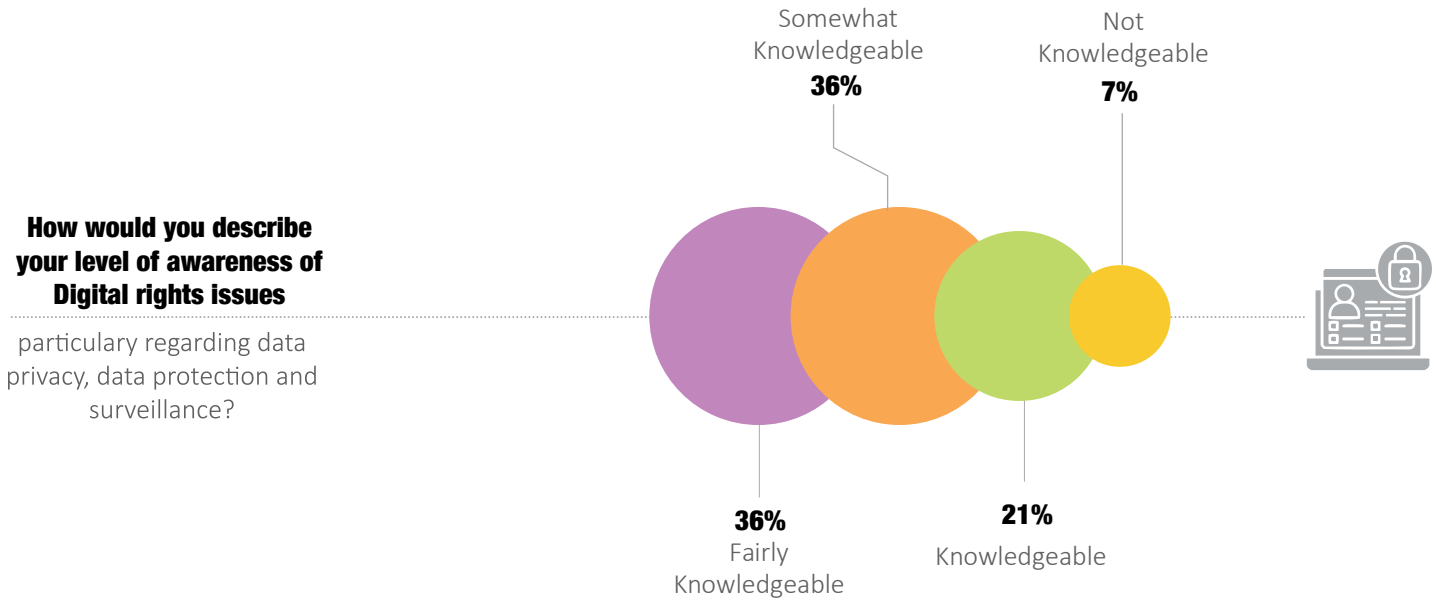
3.0 FINDINGS OF THE STUDY

Under this section, the study details findings on respondents' knowledge of various aspects related to digital rights and data privacy. Specifically, it aimed to assess their awareness of data privacy, data protection, and surveillance. Additionally, the survey explored respondents' understanding of biometric data, interpretation of the term as well as providing examples of biometric data collected by businesses in Uganda. It also inquired about the respondents' familiarity with existing laws or policies concerning data collection and privacy in Uganda and their perceptions of the importance of safeguarding data privacy and security for businesses. Lastly, it sought to understand the extent to which organisations have adopted digital technologies in their operations, including the types of systems or technologies in use. This approach helped to comprehensively gauge the level of awareness and engagement with digital rights and technology among respondents, as detailed in the extended analysis below.

3.1 CONCEPTUALISATION AND TYPES OF DATA COLLECTED BY BUSINESSES IN UGANDA

3.1.1 Appreciation of data privacy, data protection, and surveillance

The majority of respondents professed some level of knowledge (36% knowledgeable, 36% somewhat knowledgeable and 21% fairly knowledgeable) of data privacy, data protection and surveillance. None of the respondents indicated being very knowledgeable while7% indicated not being knowledgeable at all.



That notwithstanding, cases of poor appreciation of data protection and attendant privacy were also manifest amongst some key informants. More so, there was limited appreciation of repercussions of data breaches as one respondent, a community leader espoused it:

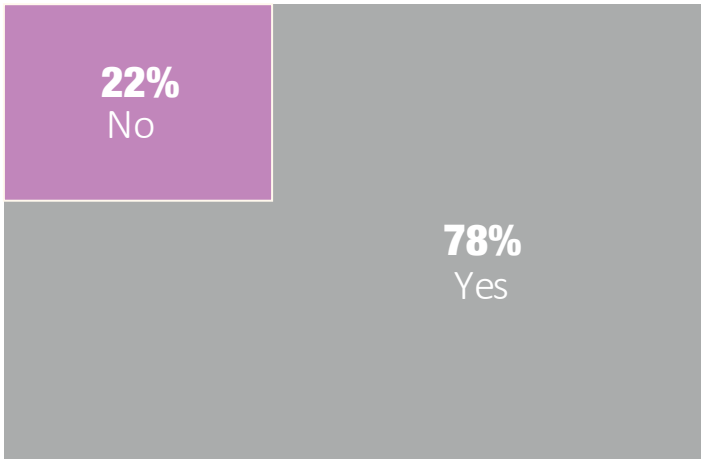
> **"We have a poor level of [knowledge] and we often just give the data without knowing associated advantages and disadvantages. Sometimes wrong or right data is given"**
> said a Local Government official in Hoima.

The limited awareness is primarily due to a lack of comprehensive understanding of data-related issues, leading to frequent sharing of personal information without a clear grasp of the associated risks and benefits.

3.1.2 Awareness of legal frameworks for data collection and privacy in Uganda

Asked about familiarity with laws or policies related to data protection and privacy in Uganda, 78% of respondents answered in the affirmative, directly referencing the Data Protection Act.

Are you familiar with any laws or policies related to data collection and privacy in uganda



The recognition of the Data Protection Act suggests that awareness campaigns and engagements around the act have been widespread and can be a stepping stone towards fostering a culture of compliance among service providers and informing citizens of their rights.

Interestingly, among those not knowledgeable about laws or policies, were some familiar with data rights. 'I know that no one is supposed to take my personal data but I do not know the actual law,'
said a Local Government leader in Hoima City.

Notably, familiarity with the laws and policies was found to be recognition of the specific data protection law as opposed to comprehensive understanding of the provisions within including enforcement mechanisms and obligations of data controllers, among other key aspects.

LAWS & POLICIES MENTIONED	PROVISIONS CITED
The Constitution	Articles 27 (Right to privacy) and 41 (Right to access to information)
The Data Protection and Privacy Act	No specific provisions cited but multiple mentions of this key legislation.
Computer Misuse Act	No specific provisions were put forward.
The Electronic Transactions Act	This law was mentioned as supportive of digital transactions. No specific provisions were mentioned.
Regulation of Interception of Communications Act and Electronic Signatures Act	Respondents mentioned these as other relevant laws they had knowledge of but without specific mention of provisions therein.
Internal Data Policies	A minority of responses highlighted internal company policies, indicating emerging awareness that data protection is also managed at organizational levels.

Overall, the findings indicate general familiarity with instruments central to Uganda's data protection and privacy legal framework. Recognition of constitutional protections alongside broader laws on electronic transactions, interception of communications, and sector-specific regulations was also exhibited by respondents. This knowledge base provides a foundation for informed engagement with digital rights issues, though ongoing education could further deepen understanding of specific provisions and enforcement mechanisms.

3.1.3 Understanding of biometric data and its use in business operations

a) Conceptualisation of "biometric data"[22]

The survey responses correctly identified biometric data as relating to physical or physiological characteristics such as fingerprints, iris scans, facial scans, and palm patterns. There was also a general recognition, as revealed from some respondents, that biometric data is a type of personal data, often collected digitally.

Image II: *Select Respondent appreciation of biometric data*

However, some conflated biometric data with other forms of personal data such as name, ID numbers or addresses. "[Biometric data] means information about an individual, hard and soft. Examples include Names, ID number, Date of Birth, signature, finger prints," said one respondent. There were some definitions from the respondents that were less precise, ambiguous or confusing-depicting inadequate knowledge about biometric and non-biometric data-or other forms of personal identifying information. Additionally, there was a tendency to interchange biometric data with "biodata," (a reference to biographical details and not physical traits). Examples of such responses include: "This is data related to an individual for example, name, age, sex, phone contacts among others."

Whereas most respondents demonstrated a reasonable understanding of biometric data, and acknowledged that biometric data is often collected when accessing services, a significant subset lacked detailed knowledge of its implications, how it is used, stored and the potential risks involved in its breach if it happens.[23] Indeed, many averred that the primary purpose of collecting biometric data was identification and security, without linking it to surveillance.

b) Examples of biometric data collected by businesses in Uganda

According to the survey participants, various examples of biometric data are collected by businesses and institutions in Uganda, as summarized below in the image and described thereafter qualitatively.

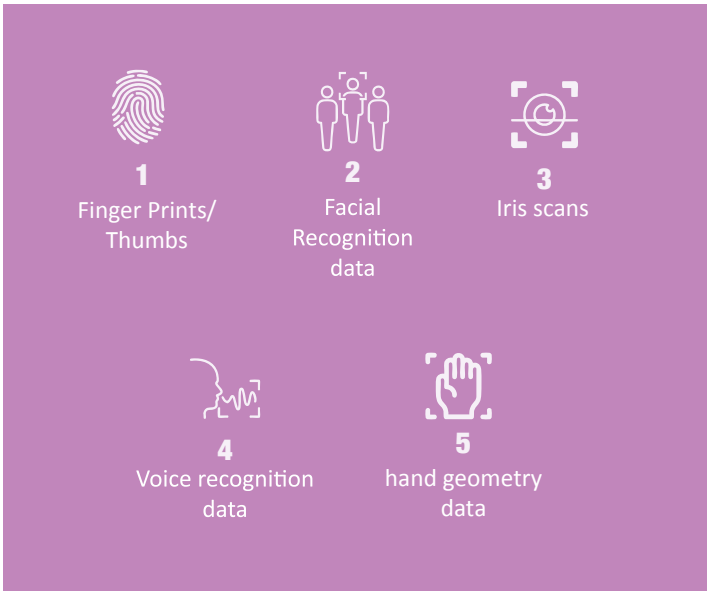


Image III: *Summary of the five examples of bio-metric data commonly collected by businesses in Uganda*

Fingerprint data is widely used in access control systems, banking applications,[24] and employee attendance tracking systems in various corporate businesses. Respondents also highlighted its widespread collection as part of SIM card registration by telecom companies. A notable example in attendance tracking was in the education sector. Mengo Senior Secondary was cited for using students' finger-print data to monitor their class attendance and transmission to parents/ guardians via text message.

22 For purposes of this survey, the classification of the responses from the participants was tested against the legal definition of 'data' provided for under the Data Protection and Privacy Act-2019- under section 2 which conceptualizes data as information which —
(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
(b) is recorded with the intention that it should be processed by means of such equipment;
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
23 This emerged across the FGDs and KIIs held in the regions of focus for the project and the study.
24 Martin Luther Oketch, 'Stanbic to begin taking biometric data of all clients,' The Daily Monitor, March 26, 2024. Accessible at https://www.monitor.co.ug/uganda/news/national/stanbic-to-begin-taking-biometric-data-of-all-clients--4568896

Secondly, facial recognition data, utilised in surveillance systems, national ID verification, SIM card registration and digital payment systems was also noted. Respondents also highlighted iris scans, collected in high-security environments, including border control points and some banking institutions, to enhance security and identity verification. However, it is worth noting that little is known about particular companies employing this, due to the opaque nature of some of these businesses.

However, it is in the public domain that the Ministry of Internal Affairs, through the National Identification and Registration Authority (NIRA), is preparing to launch a new biometric system for mass enrollment and ID card renewal. A key feature of this system is the integration of iris scanners, which will be used to capture iris details from approximately 17.2 million Ugandans, including those seeking to register for the first time or renew their national IDs.[25] The new system aims to augment the accuracy and security of identity authentication, leveraging the high precision of iris recognition technology.[26] This biometric improvement is envisioned to advance identification dependability, as iris scans are known to have a very low chance of false matches compared to other methods like fingerprint or facial recognition.[27]

The other biometric data examples stated by respondents including voice recognition and hand geometry had limited day-to-day use cases with the former only cited for call centres and the latter in access controls within secure facilities.

While not strictly biometric data in itself (Since the National ID Card is a document), the underlying system for Uganda National IDs does rely on biometric data-mainly fingerprints and facial images. Arguably, businesses collecting National IDs are indirectly accessing a system built on biometrics. The responses mentioning NIN, age, sex and residence were referring to the information on the card, but linked to the biometric system within the Ministry of Internal Affairs and more specifically-under NIRA.

It should be noted that Uganda's Bank of Uganda (BoU) announced in June 2023, a total of 74 financial institutions—including commercial banks (27), microfinance companies (5), foreign exchange bureau (1), fintech firms (34), insurance providers (2), and telecommunications organizations (2)—had gained access to the NIRA database to facilitate digital Know Your Customer (KYC) verification initiative.[28] This move is part of the enforcement of the Registration of Persons Act 2015 and aims to streamline KYC procedures by enabling institutions to authenticate customer identities through national ID data, thereby supporting secure and efficient onboarding processes.[29]

While some institutions have fully integrated and are operational with the system, others are still in the testing phase, reflecting a gradual, phased rollout since the policy's initiation in 2020. The increased collaboration between the national ID system, under the management of NIRA and Uganda's financial services industry is a manifestation of a broader trend in Uganda toward harnessing digital identification to foster safer, more inclusive financial services.

25 The Independent, 'Muhoozi confirms new IDs to include iris details but not DNA', August 16, 2024. Accessible at https://www.independent.co.ug/muhoozi-confirms-that-new-ids-to-include-iris-details-but-not-dna/

26 Ayang Macdonald, 'NIRA explains adding iris biometrics to Uganda ID', Bio-Metric Update, Jul 4, 2024. Accessible at https://www.biometricupdate.com/202407/nira-explains-adding-iris-biometrics-to-uganda-id

27 Ifeoma Joy Okorie, 'Uganda to add iris biometrics into national IDs for enhanced security and verification', Techpoint-Africa, February 15, 2024. Accessible at https://techpoint.africa/news/uganda-iris-biometrics-national-ids/

28 Bank of Uganda, 'Annual Report 2023/2024,' at 51-52. Accessible at https://www.bou.or.ug/bouwebsite/bouwebsitecontent/publications/Annual_Reports/All/Auditor-Generals-Report-2024-30-Sept-1646-hrs-Compressed.pdf

29 Ayang Macdonald, 'Uganda financial institutions sign on for digital KYC through national ID', Biometric Update, Oct 14, 2024. Accessible at https://www.biometricupdate.com/202410/uganda-financial-institutions-sign-on-for-digital-kyc-through-national-id

3.1.4 Why securing and safeguarding individuals' data is crucial for business responsibility

In Uganda, the significance of protecting individuals' data cannot be overstated, especially given the legal framework established by the Data Protection and Privacy Act, 2019. The law underscores the responsibility of the businesses to handle personal data ethically and securely, ensuring that individuals' rights are respected and maintained. The principles of the Act reflected respondents' views as to why it is important for businesses to safeguard data privacy and security.

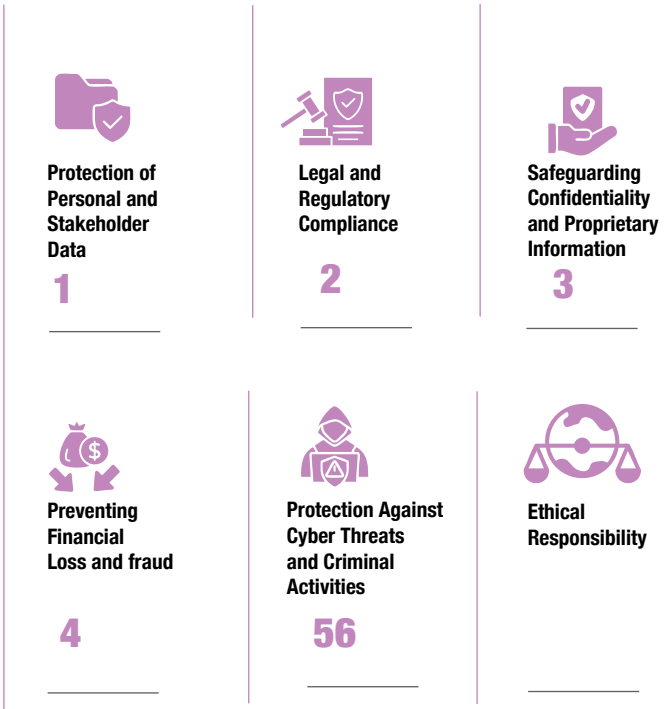


Image IV: *Summary of the respondent views on the importance of businesses to safeguard data privacy*

Many stated that safeguarding personal data was critical to curbing cybercrime and fraud, protecting proprietary business information and reputations. Notable responses from FGDs include:

"Hackers can use the data to defraud and deprive you what is rightly yours."

"You (data owner) may end up in prison or killed due to misuse of your data"

"Easy access of phone data in Uganda has resulted in phone cheats through mobile money. Other forms of crime can easily be carried out if personal data is not protected."

"Data gives access and control and therefore if it falls in the wrong hands, it can be manipulated to put an individual's safety in jeopardy."

"To prevent cyber-attacks which might lead to loss and leakage of crucial information for the business hence affecting its reputation."

"Safeguarding data privacy and security builds trust, prevents breaches, ensures compliance, protects reputation, and avoids costly legal and financial penalties."

"Because if it lands in the wrong hands, it may cause financial loss and breach of privacy."

FGD participants in Buliisa noted that businesses that fail to adhere to the data protection law risk severe consequences as non-compliance can lead to the state invocation of fines, legal penalties and in the extreme, the revocation of a company operating license. A common example highlighted was credit companies that misuse next of kin details included in loan applications, to contact family members of loan defaulters without their consent. Such breaches not only threaten peoples' privacy but also expose these businesses to legal liabilities.

Building customer trust was also mentioned amongst the reasons why securing personal data was critical for businesses. Specifically, on biometric data, FGD participants in Wakiso noted that its misuse can have serious consequences including identity theft, financial fraud and reputational damage. According to respondents, it is in the interest of the businesses to protect this data to build trust and confidence. "Customers, employees and partners in business are more inclined to trust and engage with a business that prioritises data privacy and security", said a respondent in Wakiso district.

According to key informants interviewed in Kampala, there was convergence of thought that data breaches can result in costly lawsuits, regulatory fines and compensation claims from the affected individuals. Additionally, businesses face operational disruptions and high costs related to data recovery, security upgrades and implementing preventive measures. These impacts can be long lasting and detrimental to the business's sustainability.

The other projected justification is the need for businesses to protect their business interests amidst competing rivals. Respondents noted that by maintaining robust data privacy and security measures, a business operating in a competitive environment can emerge from the pack as a distinct trusted key player. "Customers are increasingly aware of data privacy concerns and may prefer to engage with businesses that demonstrate a commitment to safeguarding their information", said an FGD participant in Wakiso district. A business that is aligned to the contextual demands of privacy may thus achieve an edge over competitors due to its robust data protection mechanisms. Respondents noted examples in the hospitality industry (especially hotels) averring that the more discreet entities are about clients, the more they are patronised by many.

3.1.5 Adoption of digital technologies in business operations

Findings reveal that overall adoption of digital technologies by businesses is more pronounced in urban areas around Kampala and Wakiso districts. The most prominent reasons for the lagging behind of entities in rural areas was meagre resources, with many using personal phones and outdated desktop computers. As noted by one key informant; "We lack equipment for data collection but there are efforts to budget for these machines so that we can guarantee the privacy of individuals as opposed to using personal phones."

Another respondent noted women and youth owned businesses were more severely affected by resource limitations, ultimately affecting their ability to uphold data protection and privacy. "Most businesses, especially those owned by women and youth do not even collect data and if they do, their processing is poor since they have limited knowledge of what is expected of them and they do not have the necessary equipment."

3.2 COLLECTION, PROCESSING & USAGE OF DATA BY BUSINESSES IN UGANDA: PERCEPTIONS ON JUSTIFICATIONS, AND BENEFITS

This section presents the findings related to the perceived motivations and effects of biometric data collection by businesses in Uganda. Additionally, it presents participants' perspectives on the potential consequences of mishandling biometric data, including impacts on reputation and overall business performance, such as loss of customers, diminished trust, or even business closure.

3.2.1 Purposes for the collection and processing of users' data by businesses in Uganda

According to the respondents, biometric data is collected by businesses in Uganda for multiple purposes. The nature of business - whether telecom or financial services for instance - determined the purpose and modalities of the data collection and processing.

a) Compliance with national policy and legal regulatory frameworks

Firstly, biometric data collection is undertaken, in majority cases, as a legal requirement and part of compliance with the regulatory frameworks from the diverse sectors of banking and financial services, communications and transportation among others. More prominently highlighted amongst the respondents were telecommunications companies' collection of fingerprint and facial data during SIM card registration as required by the law.

The process of implementing SIM card registration in Uganda officially began on March 5, 2012, under the auspices of the Uganda Communications Commission (UCC), the Uganda Police Force and the Minister of Security.[30] The initiative was driven by the need to enhance security and curb crime associated with the rapid increase in mobile phone usage across Africa. The registration requires all mobile users to register their SIM cards through biometric and personal data collection integrated with national IDs.[31]

b) Digitalisation strategy of the state

Respondents noted that government efforts to improve efficiency and security of public service delivery were also characterised by biometric data collection. Examples cited included citizen identification and immigration, as part of which, the government collects biometric data for issuance of National ID cards as well as screening and clearance of travellers at border points. As part of these digitalisation efforts, service providers are also required to collect biometric data which provides a more precise and dependable means of authenticating individuals' identities.

c) The quest for safe and secure customer transactions

The financial services sector including commercial banks were cited by respondents for collection and utilisation of biometric data such as fingerprint and facial recognition to authenticate customers, "facilitate secure transactions and prevent fraud." The collection of biometric data in the financial services sector has been heightened by the urgency to strengthen security as banks and financial institutions adopt technology for convenient financial services.

According to UCC, as at September 2024, mobile money transactions stood at 1.96 billion Uganda shillings. To counter the threat of fraudulent transactions on digital platforms, the industry has had to upgrade their mechanisms for customer verification and authentication hence the demand for biometric data collection. This quest, underpinned by e-banking, has continued to grow in leaps and bounds within Uganda's banking system from a meagre 39% in 2019.[32] A vivid example to speak to this is in the sphere of agent banking. As at February 2020, banking agents related transactions had skyrocketed to Shs 1.6 trillion from Shs 457 billion by end of 2018.[33] As at June, 2025, these digital transactions were at Shs 29.4 trillion, from Shs 16.7 trillion the previous year signifying a 76.1% growth in value.[34] More recent statistics from Bank of Uganda show that by June 30, 2025, a total of 24 banking institutions-that is, 23 commercial banks and 1 Microfinance Deposit-taking Institution were fully engaged in the agent banking digital payments ecosystem in the country.[35] Equally notable is also the increase in the number of agents on the shared platform between 2024-2025, by 49.1% from 15,288 agents in June 2024 to 22,793 agents in June 2025, further underpinning the magnitude of biometric data under collection by these banking institutions.[36]

30 *Fred Kiva, 'Operators Rush to Beat SIM Registration Deadline', Uganda Radio Network, 17 Jan 2013. Accessible at https://ugandaradionetwork.net/story/operators-rush-to-beat-sim-registration-deadline?districtId=0*

31 *The Daily Monitor, 'Simcard Registration: Is it Big Brother at work?', January 31, 2012 — updated on January 03, 2021. Accessible at https://www.monitor.co.ug/uganda/business/technology/simcard-registration-is-it-big-brother-at-work--1508420*

32 *Frank Kisakye, 'Evolution of e-banking in Uganda', The Observer, November 9, 2021. Accessible at https://observer.ug/viewpoint/evolution-of-e-banking-in-uganda/*

33 *Ibid.*

34 *Pedson Mumbere, 'Agent Banking Transactions Soar to Shs 29.4 Trillion, Marking 76.1% Growth-BoU Report', NilePost, October 8, 2025. Accessible at https://nilepost.co.ug/business/293146/agent-banking-transactions-soar-to-shs-294-trillion-marking-761-growth-bou-report*

35 *Ibid.*

36 *Ibid.*

Equally manifesting at a first rate is the retreat by banks into online/banking Apps which, by inherent standards, rely on customer biometric collection to allow usage for mainly security purposes as exemplified by some of the banks herein:

a. Stanbic Bank-Uganda operates the Stanbic App for 24/7 personal banking, bills payments and money domestic and international transfers;[37]
b. Stanbic Bank also operates the FlexiPay: a digital wallet;
c. Centenary Rural Development Bank (Centenary Bank) operates the CenteMobile for account management and general payments for utilities among other uses;
d. Equity Bank Uganda runs the Equity Mobile App (which replaced Eazzy-Banking), which offers mobile wallet payments, and loan management;
e. Diamond Trust Bank (DTB) Uganda operates DTB 24/7 App: for account management;
f. Standard Chartered Bank Uganda operates SC Mobile Uganda for account management;
g. Bank of Africa Uganda runs the BOA Mobile Wallet which allows for utility payments, and account management;
h. Opportunity Bank Uganda has the Opportunity Mobile Banking which facilitates interbank transfers, and utility payments;
i. Postbank Uganda which owns Wendi-a digital wallet.

Further compounding encroachments on personal data in the name of countering potential fraud has been the advent of behavioral monitoring technology.[38] These technologies that thrive on behavioral biometrics are described as 'advanced technology that leverages machine learning techniques to continuously assess the identity of online users, based on their behaviors, such as how they type, swipe, or move their devices.' Thus, by continuously monitoring the way users interact with their devices, the technology can build detailed behavioral profiles used as a reference to detect possible fraudulent activities. As soon as the system detects abnormal behaviors, alert responses are triggered in the background to perform additional investigations to protect the integrity of the legitimate user's account.'[39]

In the context of mobile money and digital banking in Uganda, behavioral monitoring technology is used to track users' transaction patterns, device usage, and other digital behaviors to detect potential fraud. For example, if a customer's mobile money account suddenly shows transactions from a different location or device, or if their typical transaction amounts or frequency are significantly altered, the system may flag this activity as suspicious behavior. This monitoring can lead to automatic account restrictions or requests for additional verification, which encroaches on personal data privacy in the name of fraud prevention.[40]

There is consensus that this kind of biometric harvests surrounding behavioral profiling cannot be wished away for security purposes. What however is critical, is the convergence around three key aspects. Firstly, 'ensuring that the chosen Behavioral Biometrics technologies comply with all privacy regulations'. And secondly, 'adapting contracts and legal documents' involved in such transactions to ensure that the customers have knowledge of the data being collected and consent for the same. Lastly, making sure users are aware that these data are being collected and know and have a choice to make adjustments in the app to opt out of these biometrics data collection whenever they want to.[41]

d) Workforce management

Respondents also noted that the other rapidly emerging justification for collection of data lies in workforce management. Implementation of biometric systems at entrances of premises to record arrivals and departures was said to accurately record staff attendance. One example pointed out by respondents was the standoff at Makerere University as lecturers sought to resist a biometric monitoring system as summarised in the case study below.[42]

37 See also Martin Luther Oketch, 'Stanbic to begin taking biometric data of all clients', The Daily Monitor, March 26, 2024. Accessible at https://www.monitor.co.ug/uganda/news/national/stanbic-to-begin-taking-biometric-data-of-all-clients--4568896

38 Maryanne Gicobi, 'Now lenders grapple with biometrics', The East African, September 22, 2017 — updated on July 05, 2020. Accessible at https://www.theeastafrican.co.ke/tea/business-tech/now-lenders-grapple-with-biometrics-1373946

39 Paolo Raffin and Nicolò Pastore, 'How Behavioral Biometrics can help you fight online banking fraud', 15/3/2022. Accessible at https://www.cleafy.com/insights/how-behavioral-biometrics-can-help-you-fight-online-banking-fraud

40 The Daily Monitor, 'Technology changing banking sector faster', March 03, 2025. Accessible at https://www.monitor.co.ug/uganda/oped/commentary/technology-changing-banking-sector-faster-4949422

41 Paolo Raffin and Nicolò Pastore, 'How Behavioral Biometrics can help you fight online banking fraud', 15/3/2022. Accessible at https://www.cleafy.com/insights/how-behavioral-biometrics-can-help-you-fight-online-banking-fraud

42 The Independent, 'Makerere: New biometric systems to monitor staff and student attendance', May 5, 2024. Accessible at https://www.independent.co.ug/makerere-new-biometric-systems-to-monitor-staff-and-student-attendance/

Makerere University Staff and Student Biometric Attendance Management System[43]

In May 2024, Makerere University launched the Digital Staff Access System hosted by the College of Computing and Information Science.[44] A similar system was also in place to monitor student attendance (the Student Attendance System). The system captured thumbprints of lecturers and their facial features for clocking in/out. At the time of its launch, voice-recognition capability was being explored to support staff that may be unable to use the biometric devices.[45]

For purposes of accountability, the system was built to allow students to equally monitor and report absenteeism of lecturers. According to the University, the system was built to counter absconding from duty and perennial breach of the 8am-5pm University demands for their employees' presence at the University. Other benefits of the system include continual generation of analytics for teaching loads and recruitment needs.[46]

The system however received resistance from the staff through their umbrella body- Makerere University Academic Staff Association (MUASA) opining that their teaching, research and out-reach mandate was unique in nature and "different from the routine public service mandate, whose working hours are 8:00am-5:00pm, Monday to Friday.'[47] The stand-off between the university administration and the staff signified the perceived invasion of privacy and productivity of employees.

e) Financial management

Further to workforce management, respondents stated that biometric attendance systems facilitate streamlined payroll processes by providing validated data on actual hours worked, reducing administrative errors, and expediting payroll calculations. It was also noted that the data collected via biometric workforce systems enables business owners to optimise staffing levels and ascertain recruitment needs as part of forecasting and strategic planning, ultimately supporting organisational goals and ensuring compliance with labor regulations.

f) Security and access control

Respondents noted as well, that biometric workforce systems integrated with access controls support security of personnel, premises and property by limiting unauthorised entry and/or access to restricted zones. This rush to secure operations and premises was said to have given a boost to security companies whose service provision has expanded from physical security and patrols to the installation and maintenance of biometric security systems.

43 Makerere University, 'General Launch of Mak Attendance Management System a Moment of Truth', May 3, 2024. Accessible at https://news.mak.ac.ug/2024/05/launch-of-mak-attendance-management-system-a-moment-of-truth/

44 Jane Nafula, 'Makerere staff want teaching equipment not biometrics – MUASA', The Monitor, May 08, 2024

45 Makerere University, 'General Launch of Mak Attendance Management System a Moment of Truth', May 3, 2024. Accessible at https://news.mak.ac.ug/2024/05/launch-of-mak-attendance-management-system-a-moment-of-truth/

46 Makerere University, 'General Launch of Mak Attendance Management System a Moment of Truth', May 3, 2024. Accessible at https://news.mak.ac.ug/2024/05/launch-of-mak-attendance-management-system-a-moment-of-truth/

47 Kevin Githuku, 'Makerere lecturers reject work attendance biometric system', The Daily Monitor, October 24, 2023. Accessible at https://www.monitor.co.ug/uganda/news/national/makerere-lecturers-reject-work-attendance-biometric-system-4411986

3.2.2 Assessment of proactive disclosure of data collection processes by businesses to users

The survey also sought to inquire into the adequacy of disclosure measures by Ugandan businesses of how they collect, store and use the data harvested from their customers and employees. Emerging from respondents was that many businesses, including financial institutions such as banks, fall short in providing comprehensive and transparent information to their customers, employees, and users regarding how their personal data is collected, processed, stored, and utilised. Further, while some of the bigger national businesses such as telecoms and financial institutions, often possess advanced data management capabilities, they typically offer only limited disclosures about their data practices, leaving customers with insufficient understanding of how their information is handled. Secondly, was the general view that customers are frequently required to provide personal information such as during account registration or transactions without clear, accessible explanations regarding how their data will be used or shared. For example, banks often present lengthy, complex privacy policies that few customers read or comprehend fully, which undermines informed consent.

For entities with publicly available data privacy policies (banks were singled out as perfecting these practices), the policies were only on their websites and often in one language (English) rendering them inaccessible to offline and non-English speaking users.

Examples of privacy policies of banking institutions available online:

a) The Centenary Rural Development Bank's Privacy Policy accessible at https://www.centenarybank.co.ug/assets/uploads/docs/Updated-Privacy-Policy-for-Centenary-Bank-Website%20-v1.3.pdf states: "This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You. We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy"

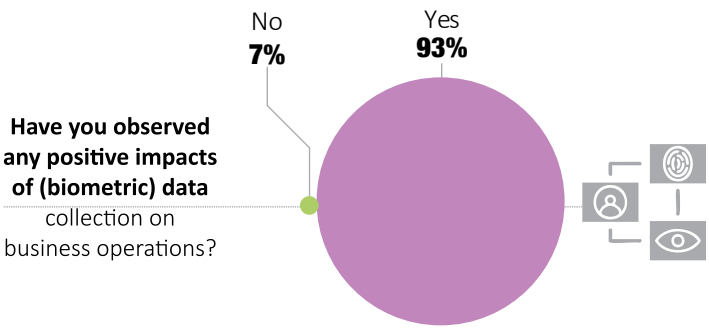
b) Stanbic bank has what it terms 'Privacy and security statement', accessible at https://www.stanbicbank.co.ug/uganda/personal/about-us/legal/privacy-and-security-statement. The stated purpose of the statement is "to inform you about how we collect, use, store, make available, disclose, update, safeguard, destroy or otherwise deal with (process) your personal information (also referred to as personal data in some countries) and to explain your rights relating to the privacy of your personal information and how the law protects you… Protecting the privacy, confidentiality and security of your personal information is very important to us as it is critical for us to maintain your trust and act in the right way to meet your needs. We have therefore implemented Group-wide policies and procedures to ensure that your personal information is protected." Stanbic Banks goes on to inform customers that should any grievances "not be addressed to your satisfaction; you have the right to lodge a formal complaint with the Personal Data Protection Office" and provides the relevant contact details.

c) Equity Bank Limited has on its website what it describes as an "Information Security Policy", accessible at https://equitygroupholdings.com/ug/images/docs/Equity-Bank-Uganda-Information-Security-Policy.pdf . It also possesses a Data Privacy Policy which states that "We must receive or collect some information to operate, provide, improve, understand, customize, support, and market our Services. This also includes when you install, access, or use our Services. The types of information we receive and collect depend on how you use our Services."

To many of the respondents therefore, the issue is not as simple as posting these data policies online but taking concrete steps to ensure that the clientele relates to them in the most basic and accessible way possible depending on their literacy levels and communication channels. For now, respondents concluded, this pro-activeness of reach is missing and where existent, it is inadequate.

3.2.3 Positive impacts of biometric data collection on business operations

Survey respondents were asked if they had observed any positive impacts of [biometric] data collection on business operations. Over 90% responded positively. This reflects a strong consensus that the data collected enhances or positively influences various aspects of business operations.



Specific examples of the positive impacts mentioned include:

Customer satisfaction and reputation boast: One of the key positive impacts fronted by the respondents is that biometric data facilitates effective customer follow-up. By accurately identifying individuals through biometric identifiers such as fingerprints, facial recognition, or iris scans, businesses in Uganda can streamline communication and service delivery to the great specificity of a particular customer by just referencing his/her data. This precise identification ensures that "interactions are personalized and that follow-up actions are targeted, reducing errors and enhancing customer satisfaction, thereby boasting businesses," said a key informant in Kampala.

Relatedly, according to respondents, biometric data "improves the capability to collect and act on customer reaction." When customers are correctly identified, their feedback can be proficiently linked to their profiles, enabling businesses to analyse trends and preferences more meritoriously. This leads to more informed decision-making, allowing businesses to adapt their services or products to better meet customer needs.

Operation efficiency: In the same vein as customer satisfaction, biometric data collection was noted as key to evaluation of the business progress and set-backs. As highlighted in a Kampala FGD, "by collecting the right data from the right category of data subjects such as employees, businesses measure performance and track profitability, daily employee operational efficiency, among other critical aspects". Performance and metrics from workforce and financial management systems in section 3.2.1 above "helps business managers monitor performance data accurately and make data-driven decisions," said a respondent from Hoima.

Improved service delivery and customer retention: Additionally, and based on their lived realities, respondents noted that biometric data is essential in the improvement of service delivery in particular sectors including among many, banks with online banking systems. These systems, thriving on clientele data for biometric identification, ensure that only authorised users access utilities or services, reducing fraud and unauthorised usage. These systems, operational remotely, "speed up service provisioning by eliminating lengthy in person processes and providing quick, secure access," thereby enhancing overall customer experience thanks to biometric data collected.

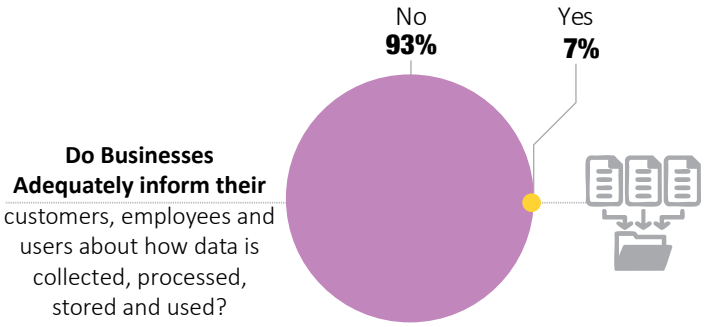
3.2.3 Implications of improper handling of [biometric] data on a business entity

The positive impact of biometric data collection and processing on business operations notwithstanding, the implications of mishandling cannot be understated. According to respondents, breaches can "cripple the business due to reputational loss", "lead to job losses", "loss of high value customers" and "adversely affect business performance if the data can no longer guide strategies or inform decision making".

3.3 EMERGING RISKS AND CHALLENGES IN BIOMETRIC DATA COLLECTION & USE

3.3.1 Concerns in collection data by business

In the survey, respondents were asked to share their concerns regarding how businesses handle the collection, processing, storage, and utilisation of personal data. Keeping data subjects informed emerged as a key concern - with 93% of respondents indicating that businesses did not adequately inform their customers, employees and users about how their data is collected, processed, stored or used. Only 7% responded in the affirmative.



This stark disparity indicates the prevalence of a widespread perception that transparency around data handling practices is lacking among Ugandan businesses, which raises concerns about trust, and compliance with data protection standards.

This lack of transparency, coupled with complex legal jargon in privacy policies, creates a significant power imbalance, where individuals are often unable to exercise informed choices or opt out effectively, thereby risking their privacy and security. Specific concerns raised are highlighted below.

a) Opaqueness in the processes and procedures surrounding data collection and utilisation by businesses

One of the most outstanding concerns from the respondents lay in the opaque processes and procedures surrounding data collection and use by businesses. According to respondents, a majority of businesses gather amounts of personal and even biometric data without providing clear, easily digestible information about what data is being collected, the methodologies of its collection (how), the mode of storage and where it shall be stored, and who it shall be shared with. One respondent in Kampala noted:

> **"The standard cliché is data will be "used in accordance with our internal policies" without detailed descriptions of how, where, or for what specific reasons the data will be used and more so, without access to the said policies to the data subject."**

This, seemingly deliberate ambiguity was said to leave individuals from whom this data has been harvested largely unaware of the enormous digital footprints they are leaving behind and its potential far reaching implications. Further, these data practices are often clothed with what respondents called "long and complex legal jargon writings," making it virtually impossible for the average person to fully comprehend their rights or how to effectively exercise the right of choice to opt out of the data collection. This disproportionateness of information produces an inherent power unevenness, where businesses hold the keys to one's digital identities while they remain in the dark.

b) Lack of informed consent or/and its dubious concealment[48]

According to the respondents, what is seemingly presented as consent, is often deeply buried within highly convoluted and lengthy terms of service which users are involuntarily made to accept in their totality, as a precursor to accessing a service. It is this that respondents termed 'take it or leave it' phenomenon or approach to privacy which effectively coerces individuals to surrender their personal and biometric data without an informed understanding of the consequences arising therefrom.

c) Weak and insufficient data security/protection systems to counter breaches

With the exception of established businesses and financial institutions, respondents expressed concern with small and medium size entities, stating that they often "lack robust protective mechanisms and tools such as encryption and secure storage despite the sensitivity of the information collected." Consequently, individuals remain exposed to the ever present threat of data breaches, cyber-attacks, and leaks. According to respondents, concerns regarding the security of data extend to the knowledge and skills of the human resources that have access to and process data. Still on human resources, security measures around exiting staff (resignation or termination) and their access to internal systems and data in the custody of a business which are rarely revoked promptly was also highlighted.

d) Data collection beyond what is necessary

Respondents also expressed concerns over the non-implementation of the notion of data minimisation. Businesses were cited as "in the habit" of collecting more data than is strictly necessary for the provision of services. For example, requiring facial or fingerprint recognition for entry into a building for staff members, when a simple ID check would suffice exemplifies this over reach. This excessive biometric data collection increases the risk of abuse and an unnecessary pool of data for cyber criminals. "The businesses seem to focus on maximising data acquisition rather than adhering to the principle of only collecting that which is relevant and necessary for the stated purpose," said a respondent.

e) Third party data sharing without express authorisation/ consent[49]

Also deeply troubling, an emerging practice highlighted is that of sharing data with third parties among which include advertisers and data brokers, without the necessary explicit consent of the data subject. Because the practice is monetised, it can lead to targeted surveillance, where individuals can be surveilled and profiled based on their online and offline activities. "Individuals are often unaware that their personal information is being traded and exploited by entities with which they have never had any direct interaction," said a respondent from Jinja district. The most prominent example pointed out by the respondents, was the case of Safe Boda, herein summarised as a case study.

Safe Boda Data Breaches in Uganda[50]

In 2020, SafeBoda,[51] a ride-hailing app operating in Uganda, Kenya, and Nigeria, was accused of sharing users' personal data with third-party applications without their consent. This, it was alleged, was in breach of provisions of the Data Protection and Privacy Act (DPPA) of 2019, specifically Section 7, which prohibits sharing personal data without user consent or prior notification. In a complaint filed by Obedgiu Sammy before Uganda's National Information Technology Authority (NITA-U), it was alleged that SafeBoda deployed a Software Development Kit (SDK) with capabilities to transmit user information to Facebook, even when users did not have Facebook accounts or the app installed on their phones.

SafeBoda also reportedly used another app called CleverTap that collects a range of user information, including phone numbers, device models, location, time zones, usernames, and internet service providers. At the time of these allegations, the app was being used by over one million users for commuting, goods delivery, and grocery shopping, among others. It was alleged that the unauthorised sharing of personal information compromises user safety and privacy, putting millions at risk.

An investigation by NITA-U- under section 32 of the DPPA; was undertaken and found that SafeBoda unlawfully shared clients' data with third parties. It further found that:[52]

48 Under Section 2 of the Data Protection and Privacy Act, consent cannot be assumed. Therein, "consent" means any freely given, specific, informed and unambiguous indication of the data subject's wish which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her.' Anything that falls outside this ambit is not consent.

49 Section 2 of the Data Protection and Privacy Act-2019 defines "third party" in relation to personal data, a person other than the data subject, the data collector, data controller, or any data processor or other person authorized to process data for the data controller or processor.

50 Pearl Elisabeth K, 'SafeBoda Accused of Sharing Client's Personal Data with Third Party App', July 16, 2020. Accessible at https://chimpreports.com/safeboda-accused-of-sharing-clients-personal-data-with-third-party-app/

51 Meera Senthilingam, 'Uber for motorbikes' - the smart way to get around in a bustling capital', CNN, March 25, 2015. Accessible at https://edition.cnn.com/2015/03/25/africa/the-smart-way-to-get-back-on-a-bike----safebodas-in-kampala

52 Report of NITA investigations and decision at https://www.unwantedwitness.org/download/uploads/NITA-U-FINAL-REPORT.pdf

I. SafeBoda did not comply with the legal requirement to disclose to the data subjects the recipients of the data collected from them. The SafeBoda's Privacy Policing & Data Protection Policy version of 2017 and 2019 respectively did not provide information on recipients with whom its users personal data will be shared;
II. SafeBoda shared users' personal data with an analytics company called CleverTap. Since the users did not provide specific and informed consent to share their data with data processors, it was a breach of the DDPA.
III. The contract between SafeBoda and CleverTap included a commitment to maintain confidentiality and security of the data collected as required by the DPPA. However, there were no measures put in place to ensure confidentiality and integrity of the data collected as required.
IV. SafeBoda had designated a Data Protection Officer as required by the DPPA.
V. SafeBoda did not have well documented procedures for breaches in security which affected its ability to detect and immediately notify the Data Protection Officer and NITA-U of any breaches in its securities.
VI. SafeBoda did not sell users' data."[53]

The case of Safeboda highlights critical lessons for businesses and regulatory oversight. Notably, despite NITA-U's findings, the authority did not impose any penalties. Instead, it issued several recommendations urging the company to take corrective actions over a four-month remediation period and to submit a detailed action plan within two weeks of the decision date. This gave the company an opportunity to address and remedy the identified breaches.

In its decision, NITA-U explicitly considered several key factors, which appeared to influence its decision to grant SafeBoda the opportunity to undertake self-remediation before any formal enforcement action. These factors include:

a. SafeBoda's demonstrated cooperation throughout the investigation process, indicating a willingness to engage transparently and constructively with regulators;
b. The development of an improved data protection and privacy policy by SafeBoda during the course of the investigation, reflecting proactive efforts to align with best practices;
c. SafeBoda's efforts to adhere to recognized standards and best practices in data protection, suggesting a commitment to strengthening its data privacy framework; and;
d. The initiatives undertaken by SafeBoda to raise awareness among its staff regarding the provisions of the Ugandan Data Protection Act, which demonstrates an understanding of the importance of internal compliance and staff training.

These considerations indicate a regulatory approach that encourages cooperation and proactive compliance rather than immediate punitive measures. This approach highlights a balanced regulatory philosophy that values collaboration and improvement, especially in the context of emerging data privacy infrastructure in Uganda and across Africa.

53 *'Safeboda Found In Breach Of Data Privacy Laws', Accessible at https://afmpanga.com/safeboda-found-in-breach-of-data-privacy-laws/*

f) Absence of data deletion protocols leading to indefinite storage

According to respondents, businesses practice the pervasive indefinite storage of data, even when it is no longer needed, which inherently increases the risk of unauthorised access and potential misuse. Limited business entities have implemented the right to be forgotten or engage in secure data deletion processes to facilitate data removal.[54] "As it stands now, there are concerns that even in the event of individual insistence of data deletion, it may still linger on in various data bases, vulnerable to breaches," said a FGD participant in Kampala. Thus, the perpetual retention of data without a clear justification or time frame for deleting is an ever present fear for abuse of biometric data.

This concern was prominent in the Albertine region where there is ongoing oil and gas extraction. Respondents were concerned about the uncertainty that surrounds the data handling post-operational cessation of companies such as TOTAL which has together with government collected a substantial amount of data from the local communities that were to be affected by its exploration activities.

Even where data disposal practices may exist, respondents raised concerns about residual data that may not be handled according to best practices.

g) Weak compliance and enforcement regulatory framework

While legislative frameworks such as the Data Protection and Privacy Act, 2019, exist to address some of the above concerns, respondents noted that the reality on ground is often different. Enforcement was purportedly weak and "many businesses remain non-compliant", said a number of respondents. The gaps in enforcement were attributed to limited resources and capacity to effectively audit businesses and penalise violators, leaving individuals with limited avenues for redress. "This gap between legislative and implementation creates a situation where businesses can operate with relative impunity, knowing that the likelihood of facing consequences for biometric data privacy violations is low."

Additionally, due to weak oversight, many businesses are operational but without the appointment of the legally required dedicated data protection officers or establishing the necessary internal compliance mechanisms of the law.[55] More worryingly, is that the enforcement of penalties or fines for non-compliance remains extremely weak and where executed, it is sporadic, thereby allowing the persistence of unlawful data protection practices. This regulatory gap diminishes incentives for businesses to prioritize responsible biometric data handling, perpetuating a cycle of lax practices.

h) Unlawful exploitation of personal data

Lastly, respondents noted the unlawful exploitation of personal data. Such exploitation of data was said to lead to blackmail, biased decision making and discrimination.

The Case Study of Nano Loans Microfinance Ltd and its Director, Ronald Mugulusi[56]

On Friday, April 25, 2025, Ronald Mugulusi was arraigned and charged under the Data Protection and Privacy Act, before the Makindye Standards, Wildlife and Utilities Court. Together with others still at large, Mugulusi was charged with collecting personal data without registering with the Personal Data Protection Office (PDPO). The accused allegedly operated the Quickloan app - a digital money lending service. The company collected Micheal Wombwa's data including name, telephone number and photograph for a Shs 60,000 loan.[57] Upon Wombwa's failure to repay the loan, the company processed the same data into a video without the victim's consent and threatened to disseminate it online if the loan was not repaid.

Wonambwa reported the incident to the PDPO, which, together with the Criminal Investigations Directorate (CID), initiated investigations and established that Quickloan is operated by Nano Loans Microfinance Ltd, which was not registered with the PDPO, despite being a data collector and processor as defined by the law. The case is still ongoing.

54 Patience Ngabirano et al, 'The Data Protection and Privacy Act, 2019; An analysis of the compliance requirements for data collectors, processors or controllers under the Act', Dec 14, 2020. Accessible at https://www.kaa.co.ug/the-data-protection-and-privacy-act-2019-an-analysis-of-the-compliance-requirements/#:~:text=Introduction,the%20provisions%20of%20the%20Act .

55 Respondent perspective in FGD, held in Kampala district.

56 Sarah Tumwebaze, 'Fast cash, long pain: The dark side of Uganda's mobile lending apps boom,' The Daily Monitor, April 30, 2025. Accessible at https://www.monitor.co.ug/uganda/business/finance/fast-cash-long-pain-the-dark-side-of-uganda-s-mobile-lending-apps-boom-5022688#story

57 Dorothy Nakaweesi, 'Digital money lender remanded over Shs60,000 loan', The Daily Monitor, April 25, 2025. Accessible at https://www.monitor.co.ug/uganda/news/national/digital-money-lender-remanded-over-shs60-000-loan-5017638

Sarah Tumwebaze, 'Fast cash, long pain: The dark side of Uganda's mobile lending apps boom,' The Daily Monitor, April 30, 2025. Accessible at https://www.monitor.co.ug/uganda/business/finance/fast-cash-long-pain-the-dark-side-of-uganda-s-mobile-lending-apps-boom-5022688#story

This case also brings attention to the troubling practice of "borrower-shaming" employed by certain digital lending platforms.[58] These resort to publicly exposing defaulters using their personal information and images earlier collected, as a means to pressure them into repaying loans.[59] This tactic not only damages the borrower's reputation but also raises serious ethical and legal concerns.

What makes this case even more significant is the privacy rights involved and abuse of collected data. While borrowers may voluntarily provide their personal details when applying for a loan as was in this case, businesses are not permitted to repurpose that information for unrelated activities for example as in this case, creating and sharing humiliating videos, without the borrower's explicit consent. This is a violation of Uganda's Data Protection and Privacy Act, to the effect that data collected for one purpose (like processing a loan) should not be used for another, especially for humiliating or harmful purposes.

3.3.2. Risks associated with processes of data collection

The survey findings reveal that respondents predominantly associate several key risks with the collection and use of biometric data by business including; Misuse of data (surveillance & profiling); Privacy breaches; and Cyber security threats.

Below is a summary of the risks that were propounded by the respondents during the survey as synonymous with processes of biometric data collection and usage amongst businesses.

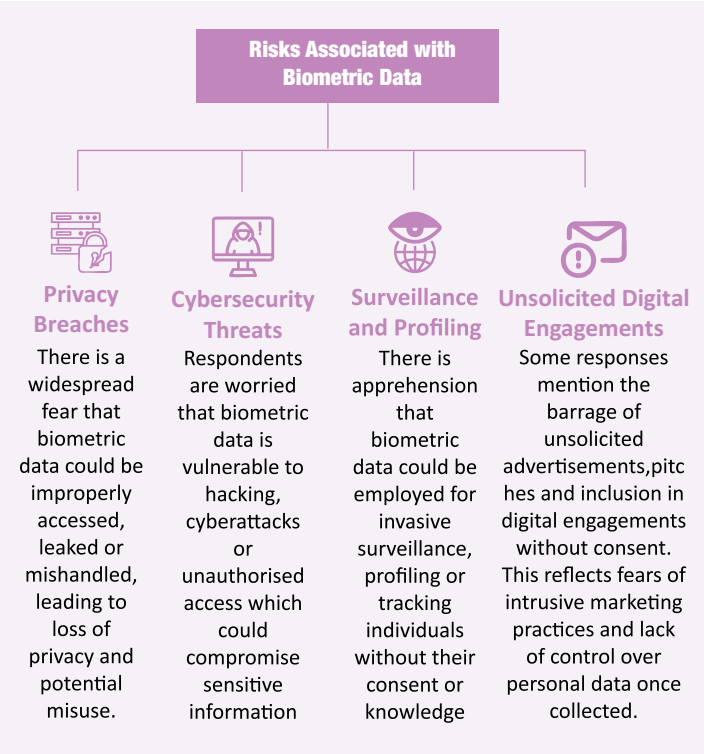


Image V: *Summary of the respondent views on the risks associated with processes of data collection by businesses*

58 *Sarah Tumwebaze, 'Fast cash, long pain: The dark side of Uganda's mobile lending apps boom,' The Daily Monitor, April 30, 2025. Accessible at https://www.monitor.co.ug/uganda/business/finance/fast-cash-long-pain-the-dark-side-of-uganda-s-mobile-lending-apps-boom-5022688#story*

59 *BBC, 'Kenya outrage over debt collectors' shaming tactics', 5 August 2021. Accessible at https://www.bbc.com/news/world-africa-57985667*

Surveillance practices in Ugandan businesses and their justification

The survey also sought to ascertain the perspectives of the respondents in relation to the necessity, by businesses in Uganda, to undertake surveillance practices. For purposes of conceptualisation, the survey gave the example of data collection and analysis of employees within the workplace including through CCTV, biometric access systems, GPS tracking and activity monitoring software. 87% of respondents agreed that employee surveillance practices are necessary.

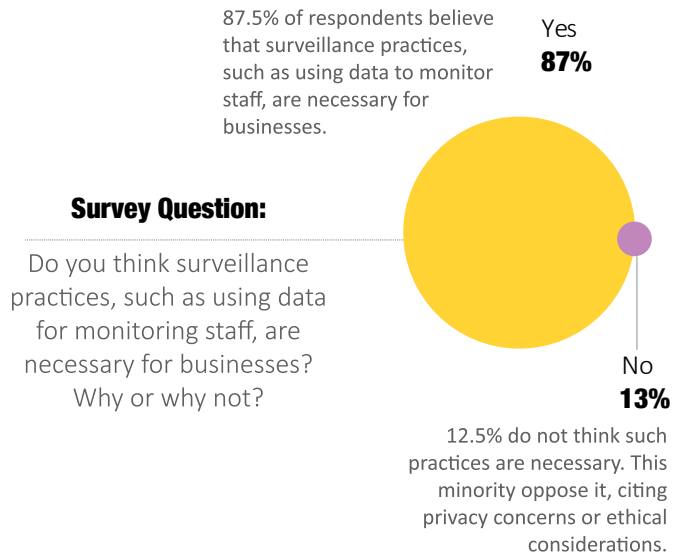


Image VI: *Summary of the respondent views on surveillance practices by businesses*

However, respondents indicated that the extent to which such surveillance practices are necessary depends on the context, purpose, and manner in which they are implemented. The use of surveillance practices in high security and sensitive operations such as banks, scientific research laboratories, or government facilities, using biometric access controls was generally considered reasonable and necessary to prevent unauthorised access, theft and sabotage. "Surveillance enhances security, accountability, productivity, and compliance within business environments," said one respondent. "Where you have a large number of staff or where you need to measure productivity, or in case you need a mechanism to support the link between staff working hours and results, you need to undertake surveillance," reflected another respondent.

Other arguments included:

- Fleet management - to assess fuel consumption, to prevent theft or misuse by drivers, thereby protecting the company's financial interests.
- Workplace culture - to encourage and foster discipline, where employees are aware that their actions are being observed, leading to increased responsibility and adherence to work ethics
- Value chain management - to assess bottlenecks such as turnaround time for delivering of services and areas of improvement.

Whereas the necessity of surveillance was acknowledged, respondents emphasised the need to safeguard against abuse.

"Businesses ought to know where their staff are and what they are up to particularly when they are expected to be at work. Surveillance is important for the security of persons and property. There is a growing shift to digital and online businesses, physical supervision is becoming more difficult and outdated. Surveillance can be important. This is as long as the surveillance does not cross the limit to become an invasion of privacy."

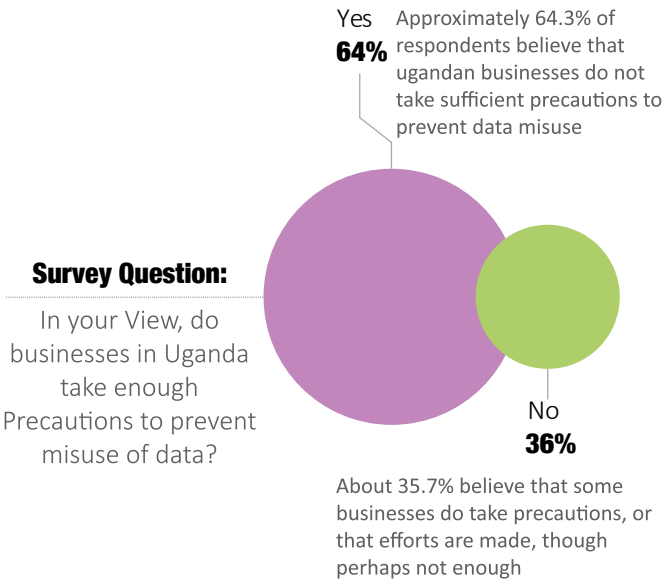
The undermining of privacy rights has the potential to cause discomfort, stress, and a breakdown of trust between employees and management. Respondents also noted the risk of businesses using surveillance data for unfair disciplinary actions or unauthorised employee profiling including, in worse scenarios, black mail of employees.

Ultimately, while surveillance can be beneficial for security and efficiency, it must be balanced with respect for employees' privacy rights. Therefore, transparency about monitoring practices, clear policies, and respecting legal boundaries are essential to maintain ethical standards.

3.3.3 Challenges faced by businesses in ensuring the ethical and lawful collection and processing of data

Despite efforts by some businesses to ensure that they align their operations to ethical and lawful collection of data and its processing, they have been faced with a diversity of challenges.

Only 64% of respondents felt that businesses in Uganda take enough precautions to prevent misuse of biometric data.



According to respondents, a significant number of businesses, at least those they interact with, are unfamiliar with responsible biometric data handling best practices, which has contributed to widespread non-compliance. This knowledge gap has created vulnerabilities, increasing the risk of sensitive biometric data being misused or inadequately protected as discussed herein below:

a) Lack of knowledge, capacity, awareness and infrastructure to buttress responsible biometric data harvesting in Ugandan businesses

Although Uganda boasts of a law that governs data protection, respondents noted that businesses have limited access to specialised training, inadequate technological resources, and a general lack of awareness about biometric data management best practices which has "bred negligent conduct". Added to this is the inadequacy of information surrounding the diverse statutory obligations of these businesses in relation to data protection frameworks.

SMEs in particular, lack resources or knowledge to interpret legal requirements, leading to unintentional non-compliance more so in rural areas. There is also 'insufficient dissemination of information and training on what constitutes responsible data collection, processing, and storage.'[60] Consequently, many businesses do not implement necessary policies or procedures to align with legal standards, increasing the risk of data breaches and misuse.

Thirdly, according to respondents, most businesses, especially the SMEs, do not prioritise or invest sufficiently in cyber security infrastructure. They often lack basic security measures such as encryption, firewalls, intrusion detection systems, or multi-factor authentication, which are essential for the protection of biometric data. Larger organisations like banks and telecom companies, despite their resources, have experienced data breaches-such as the recent hack of the Bank of Uganda,[61] Equity Bank,[62] and Stanbic Bank,[63] thereby highlighting vulnerabilities in their cyber security defenses. These incidents underscore the widespread weaknesses in cyber security preparedness across the sector. One respondent noted:

> **'If Bank of Uganda can be hacked and money stolen, yet we expect it to have the highest levels of cyber security, what do you expect from an upcoming small company?'[64]**

Relatedly, Uganda currently faces a significant shortage of trained professionals specialising in data and cyber security. A number of businesses rely on general IT staff who may lack the necessary expertise to implement robust data security measures or conduct privacy impact assessments.[65] Consequently, few organizations undertake proactive steps such as privacy impact assessments before deploying biometric systems, increasing the likelihood of vulnerabilities and non-compliance with the best practices. Associated with the above challenge is the danger of employing the inadequately skilled personnel to handle highly sensitive biometric information. This breeds a higher risk of mishandling such as improper storage, accidental leaks, or deliberate misuse.

60 *Respondent perspective in FGD, held in Kampala district.*
61 *Elias Biryabarema, 'Uganda confirms hack of central bank accounts, official downplays extent of loss', Reuters, November 29, 2024. Accessible at https://www.reuters.com/world/africa/hackers-steal-17-mln-uganda-central-bank-state-paper-2024-11-28/*
62 *The Observer, 'Equity bank staff, customers in Shs 65 billion fraud', March 11, 2024. Accessible at https://observer.ug/news/equity-bank-staff-customers-in-shs-65-billion-fraud/*
63 *The Observer, 'Shs 2bn loss: Stanbic fined Shs 340m over unsecured online banking system', April 17, 2025. Accessible at https://observer.ug/news/shs-2bn-loss-stanbic-fined-shs-340m-over-unsecured-online-banking-system/*
64 *Respondent perspective in FGD, held in Wakiso district.*
65 *Respondent perspective in FGD, held in Kampala district.*

b) Inadequate data policies and security practices

Respondents decried the practice of "Ugandans opening up so many businesses that collect biometric data without establishing clear policies concerning secure storage, access control, and data retention." Many purportedly store biometric data on unsecured servers, personal computers, or cloud services lacking encryption or other security measures. This exposes sensitive data to potential breaches, hacking, or unauthorised access. One respondent in Wakiso noted that:

> **There is a tendency towards ad hoc data management without structured governance frameworks, making it difficult to ensure accountability and compliance with data protection standards. These ad hoc processes are only set up when there are threats of inspections or enlightened citizens who demand them. They are often simple computers and laptops. In hotels it's worse. Those people write data on paper and one wonders where they put it after writing? Are they scanned? Put in a store room? They are hardly digital.**

One of the case studies that provides for the appreciation of risks involved in data collection, processing, storage, use and poor security frameworks, happened in June, 2022, involving the Uganda Securities Exchange.[66]

The Case Study of Uganda Securities Exchange Data Breach & Soft Edge Uganda[67]

The Personal Data Protection Office (PDPO) of Uganda undertook an investigation of the Uganda Securities Exchange (USE) and its technology Partner-Soft Edge Uganda following a reported security breach which lasted for 12 days, allowing unauthorised access to personal data in the custody of USE. The breach was specifically attributed to a change in the firewall configuration that left a port open, which did not follow the established change management procedures. The data accessed included "full names of investors, emails, phone numbers, passwords, usernames, plaintext credentials and access tokens, addresses, details of foreign persons and companies, bank details such as account and ID numbers of users."[68] This breach was not addressed in a timely manner by either USE or Soft Edge Uganda in direct contravention of the Data Protection and Privacy Act of 2019 and attendant regulations, highlighting serious compliance shortcomings.

Upon investigation, the PDPO identified several areas of non-compliance. For instance, the Maintenance Agreement between USE and Soft Edge Uganda Limited lacked necessary data protection and privacy clauses. It failed to specify the types of personal data to be shared and the obligations of both parties to ensure data security and privacy. This inadequacy left the parties without clear data protection and privacy-related responsibilities.

Another significant finding was that both USE and Soft Edge Uganda Limited failed to regularly verify whether the implemented security safeguards were effective. This oversight led to the data security breach going unnoticed for 12 days. Furthermore, Soft Edge Uganda Limited, a data processor for USE, was not registered with the PDPO as required by the Act. This registration was not completed even after an investigation into the data security breach started, constituting a legal violation."[69]

66 Paul Murungi, 'Data breach puts hundreds of USE investor details at risk', The Daily Monitor, June 16, 2022. Accessible at https://www.monitor.co.ug/uganda/business/finance/data-breach-puts-hundreds-of-use-investor-details-at-risk-3850096

67 The USE issued a press statement on this matter accessible at https://www.use.or.ug/uploads/announcements/Public%20Statement-Alleged%20Data%20Leak%20at%20USE.pdf

68 Paul Murungi, 'Data breach puts hundreds of USE investor details at risk', The Daily Monitor, June 16, 2022. Accessible at https://www.monitor.co.ug/uganda/business/finance/data-breach-puts-hundreds-of-use-investor-details-at-risk-3850096

69 See The Personal Data Protection Office (PDPO), 'Personal Data Protection Office Concludes Investigation into Data Security Breach at Uganda Securities Exchange" -Kampala, Uganda. 13th July, 2023.

In response to these violations, the PDPO ordered both organisations to implement corrective measures within a three-month period to rectify all the non-compliant related spheres with the data protection and privacy legal framework and regulations. In particular, it recommended that USE "initiates disciplinary proceedings against relevant personnel as per its employee policies due to their role in the breach."[70] Furthermore, the PDPO recommended that "USE ensures that the Information Systems Policies Manual is implemented throughout its operations and that reviews and updates are made to the policy and data-sharing agreements to ensure compliance with the Data Protection and Privacy Act and supporting Regulations."[71]

Additionally, the PDPO commenced what it termed as enforcement action against USE and Soft Edge Uganda Limited for non-compliance with the Data Protection and Privacy Act, and supporting Regulations in areas where violation of the law was established."[72] These actions underscore the PDPO's commitment to enforcing data protection standards and ensuring that organisations uphold their legal obligations to safeguard personal data effectively.[73]

c) Inconsistencies in data collection, processing, and control

Findings reveal that many organisations with large operations including cross border, struggle with maintaining uniform standards across different departments or regions, leading to inconsistent data practices. This has been partly as a result of variations in data collection methods and processing protocols deployed during data capture. Resultantly, this breeds unreliable datasets, making it difficult to ensure compliance with legal requirements and ethical standards. This inconsistency can also hinder data integrity, making informed decision-making challenging for the businesses.

d) Lack of cooperation from user in process of data collection

According to some respondents, some businesses suffer from data subjects' lack of cooperation during data collection such as intentional failure to disclose information. "When clientele deliberately withholds, provides false or misleading details or obscures relevant details during data collection, processing and usage can lead to incomplete or inaccurate data records further corrupting the entire business data ecosystem", noted a respondent.

e) Technological glitches in data transfer and management

Respondents opined that rapid technological advancements have bred a diversity of complexities in transferring data securely and accurately. Challenges have persisted manifesting in data loss during transfer, there is also duplication of records, or errors in data entry which are occurring due to among many factors the outdated or incompatible systems.

f) Inadequate data storage facilities

Many businesses face significant risks to data safety. "Insufficient security measures or lack of proper storage environments can lead to data breaches, unauthorised access, or data corruption," said a respondent in Jinja. Another in Wakiso noted: "Without robust storage solutions, organisations face difficulties in safeguarding sensitive information and ensuring long-term data integrity".

70 Ibid.

71 Ibid.

72 The Personal Data Protection Office (PDPO), 'Personal Data Protection Office Concludes Investigation into Data Security Breach at Uganda Securities Exchange" -Kampala, Uganda. 13th July, 2023.

73 The abridged version of the report is available at https://www.unwantedwitness.org/download/Abridged-Investigation-Report-of-the-Data-Security-Breach-Uganda-Securities-Exchange.pdf

3.4 BUSINESSES' POSITIVE CONTRIBUTION TO THE PROTECTION OF DIGITAL RIGHTS IN UGANDA

Part of the survey was to inquire into the readiness of the businesses operational in Uganda to make a contribution towards achieving the delicate balance between protection of digital rights and requisite data collection business demands. The emerging perspectives included the following;

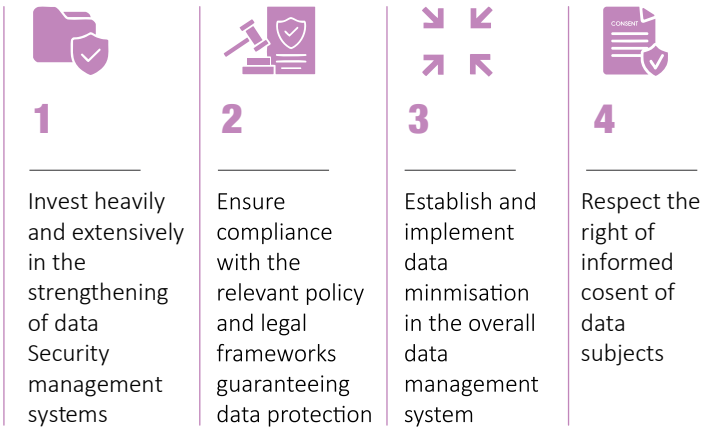


Image VII: *Summary of the respondent views on undertakings by businesses in the protection of digital rights in the era of heightened data collection for business.*

Respondents highlighted the need for businesses to invest heavily and extensively in the strengthening of their data security management systems. This includes proper storage and implementation of robust cybersecurity protocols to safeguard personal and sensitive data against unauthorised access, theft, or breaches.[74] This entails tapping in the diverse digital security tools and measures including the most prominent of encrypting data both at rest and in transit, using secure servers, regularly updating software to patch vulnerabilities, and employing firewalls and intrusion detection systems.[75] By doing so, businesses shall help prevent data leaks that could compromise individuals' privacy and violate their digital rights.

The findings also indicate that a greater focus must be placed on ensuring compliance with the relevant policy and legal frameworks guaranteeing data protection in all the relevant processes of its collection, storage, usage and destruction.[76] This creates a deterrent effect and promotes a culture of accountability, ensuring that businesses treat digital rights with the seriousness they deserve as they prioritise compliance with data protection laws to avert fines, sanctions, or operational restrictions.

Businesses must also establish and implement data minimisation as a central component of their overall data management system.[77] Ugandan businesses need to identify and categorize the types of data they collect such as personal identifiers, health information, financial data among other categories and establish tailor made policies defining the time of retention for each category. Clearly defining these categories shall help prevent unnecessary or indefinite data retention, reducing the risk of misuse or breaches and respecting individuals' rights to privacy and data control including respecting the now emerging personal choices of the right to be forgotten.

Respondents also emphasised the need for businesses to effectively respect the right of informed consent of data subjects.[78] They must ensure that consent is obtained lawfully, with a clear explanation of purpose, and documented in writing for accountability.[79] This business practice places the respect for individuals' autonomy over their data and therefore placing an obligation on these businesses to obtain informed, explicit consent before collecting or processing personal information. Informed consent protocols should be transparent and understandable -providing clear explanations of why the data is being collected, how it will be used, and who it will be shared with.[80]

Where possible and indeed as a preferred mode of operation, consent should be obtained through written or electronic means, and organisations must keep records of this consent to demonstrate compliance and accountability.

Focusing on these critical areas would help ensure that businesses in Uganda not only comply with legal requirements but also uphold the fundamental digital rights of individuals. By strengthening data security, enforcing compliance penalties, clearly defining data retention policies, and obtaining lawful and informed consent, organisations can foster a digital environment that respects privacy, promotes transparency, and builds public confidence in the responsible handling of personal information.

74 *Respondent perspective in FGD, held in Kampala and Wakiso, Jinja and Iganga districts.*
75 *Respondent Key Informant Interview, Kampala District.*
76 *Respondent perspective in FGD, held in Kampala and Wakiso, Jinja and Iganga districts.*
77 *Respondent perspective in FGD, held in Kampala and Wakiso, Jinja and Iganga districts.*
78 *Respondent Key Informant Interview, Hoima District.*
79 *Respondent Key Informant Interview, Hoima District.*
80 *Respondent Key Informant Interview, Hoima District.*

CONCLUSION & RECOMMENDATIONS

4.1 CONCLUSION

The study reveals that Uganda's expanding biometric data ecosystem is accompanied by substantial risks to individuals' digital rights, privacy, and security. Although legal frameworks and institutional oversight exist, enforcement challenges, limited awareness, and technological deficiencies undermine their effectiveness. Many businesses, especially SMEs and those in rural areas, operate with inadequate understanding and resources, increasing the likelihood of data breaches, misuse, and ethical violations.

Additionally, while biometric data collection and surveillance are recognised as essential for security, operational efficiency, and digital transformation, their implementation must be responsibly managed. This includes ensuring transparency, obtaining genuine informed consent, strengthening legal enforcement, and building capacity for responsible data handling. Balancing security needs with privacy rights is crucial to fostering trust and safeguarding individuals' digital freedoms in Uganda's evolving digital landscape. Addressing these challenges requires coordinated efforts among policymakers, regulators, businesses, and civil society to establish a resilient, rights-respecting biometric data environment.

In conclusion, a collaborative effort involving the government, civil society, and private sector organisations is essential to establish a robust framework that ensures biometric data is collected, processed, and stored securely and ethically. By implementing clear policies, investing in training and technology, and fostering transparency, these stakeholders can significantly reduce privacy risks and build public confidence in biometric and data collection practices.

4.2 RECOMMENDATIONS

4.2.1 Businesses

a) Businesses/companies should craft and implement a comprehensive policy and legal compliance framework for their entities guaranteeing data protection in all the relevant processes of its collection, storage, usage and destruction.

This includes strict adherence to the Data Protection and Privacy Act, 2019, by establishing protocols that guarantee lawful collection, processing, and storage of personal data, including biometric information. This creates a deterrent effect and promotes a culture of accountability, ensuring that businesses treat digital rights with the seriousness they deserve as they prioritise compliance with data protection laws to avert fines, sanctions, or operational restrictions.

b) Promote a framework of data collection that guarantees and protects informed consent.

Data collection protocols should provide for the obtaining of explicit and informed consent from individuals before collecting their biometric data. This involves clearly communicating the purpose, scope, and duration of data collection, as well as individuals' rights regarding their data. Where possible and indeed as a preferred mode of operation, consent should be obtained through written or electronic means, and organizations must keep records of this consent to demonstrate compliance and accountability

c) Establish data storage, retention and destruction policies

Develop and enforce clear policies on how long biometric data is stored. Data should only be retained for as long as necessary to fulfill the purpose for which it was collected, after which it should be securely deleted. All these measures must be known by the clientele in the quest to establish transparency and elicit mutual trust. Clearly defining these categories shall help prevent unnecessary or indefinite data retention, reducing the risk of misuse or breaches and respecting individuals' rights to privacy and data control including respecting the now emerging personal choices of the right to be forgotten.

d) Develop and implement a data security/protection framework

This could involve a diversity of measures and tools aimed at ensuring that data is protected at all costs. Such diverse digital tools include the use of encryption techniques to protect biometric data both at rest (storage) and in transit (during transmission) against unauthorised access, theft, or breaches. This could also involve the enhancement of access controls through the employment of multi-factor authentication (MFA) for accessing biometric data to ensure that only authorised personnel can retrieve or modify sensitive information. The security framework could also consider the conduction of regular security audits and periodic vulnerability assessments to identify weaknesses in data handling systems and address them proactively. Other tools include the implementation of the role-based access control (RBAC) systems to limit data access strictly to personnel with designated roles, reducing the risk of internal misuse or accidental exposure.

e) Appoint, train and designate data protection officers (DPOs) of acumen as personnel responsible for overseeing business/company compliance with data protection laws, handling data protection strategies, and serving as points of contact for data privacy issues. This increases accountability and oversight within the organisation due to the centralised nature of data related aspects.

f) Establish and consistently implement an education and awareness program.

This should target regular business/company staff training on data privacy, cybersecurity best practices, and how to recognise phishing threats among others. This must be consistently updated to keep the staff updated about the constantly evolving threats. In equal measure and simultaneously, educate customers on how their biometric data is collected, stored, and protected to build trust and transparency.

4.2.2 Government of Uganda

a) Undertake a comprehensive review of the contemporary challenges in data protection, the current legal and policy framework governing biometric data with a view of identifying loopholes to inform reform to strengthen data protection. The policy and legal protective framework must be aligned with both national and international standards, balancing the diversity of human rights and freedoms that could be affected by intrusive policies.

b) Enhance the active enforcement of the prevalent policies through among other aspects inspections, periodic audits, and penalties where there are established violations. The framework of enforcement should be publicised for transparency purposes and sanctions, if any, should be undertaken in a fair manner, to avoid their abuse. Additionally, the regulatory agencies and agents must be capacitated and skilled to effectively monitor compliance and impose appropriate sanctions on violators.

c) Provide structured guidance and support through offering of clear guidelines, standards, and tools to assist businesses in implementing secure data collection and processing practices.

d) Facilitate sustained public awareness campaigns in various forms including dissemination of information in local languages to inform citizens about their rights regarding biometric data and how to recognise safe data practices, and avenues for remedies in cases of breach.

e) Government to consider reduction or waiver of taxes on equipment that is used to capture data responsibly in the best possible way so that they can be accessed easily even by small businesses.

4.2.3 Private Sector Associations

a) Organise regular training sessions for member organisations on data privacy laws, security best practices, and emerging threats like phishing or hacking. This should be undertaken periodically, to allow capacity building that is evolving alongside the challenges and threats to data protection as they emerge. Equally important is the need to conduct training and awareness programs for staff members and third-party contractors, equipping them with the knowledge and understanding of their roles in protecting the privacy of personal data. This comprehensive approach helps foster a culture of data protection throughout the organisation and among its partners.

b) Encourage member businesses to craft and implement customer education and awareness about the diverse issues concerning their data. This is necessary to facilitate transparent communication with customers about data collection and protection measures, fostering trust and informed consent.

c) The associations should promote and support their member businesses and companies in the use of secure servers with restricted access controls for biometric data. They should, through the development of knowledge products such as manuals, guide their members to the implementation of secure deletion methods to permanently erase data when no longer needed. All of these should be part of a comprehensive and transparent data management system.

d) Conduct ongoing risk assessments related to biometric data collection and processing activities within their member businesses to ably develop mitigation strategies to address potential privacy and security risks proactively. This could also help in the establishing and sharing of best practices, successful strategies and standards among members to ensure consistent, high-quality data protection across industries.

e) Undertake internal periodic data protection impact assessment and data protection and privacy audits to inform data protection mechanisms within the businesses. This process allows the companies to identify and undertake measures to mitigate risks associated with data processing activities that may pose a high risk to users' privacy rights and freedoms and data protection.

4.2.4 Civil Society Organisations

a) Establish and institutionalise multi-sector stakeholder collaboration and networking initiatives

CSOs should invest in establishing multi-stakeholder platforms where civil society, government, academic institutions, tech experts, international organisations and private sector actors can share knowledge, coordinate efforts, and develop joint strategies for data protection. These alliances also help stakeholders to stay updated on emerging trends and innovative data protection mechanisms.

b) Build public trust and awareness for a resilient accountability demanding citizenry

Facilitate community dialogues and workshops to educate citizens about their biometric data rights and how to recognise and report breaches and the promotion of the use of transparent communication strategies by businesses, including clear privacy notices and accessible channels for grievances.

c) Develop advocacy and educational materials

CSOs are in a vantage position to develop educational materials such as brochures, posters, and digital content that explain biometric data rights, risks, and safe practices for both communities and businesses, in simple digestible language. In the same vein, they can develop and provide accountability and compliance toolkits for businesses including among others checklists, templates, and guidelines to help them implement compliant data collection and storage procedures.

d) Undertake strategic research and knowledge sharing

CSOs should undertake research to identify gaps, challenges, and best practices in biometric data protection, especially in local contexts. This can include surveys, case studies, and policy analysis. From these research undertakings can be developed, published and disseminated knowledge products on data protection such as manuals, guidelines, and toolkits that outline best practices for some of the prominent aspects such as data collection, storage, consent, and security. These resources could be accessible in local languages and tailored to different sectors/businesses to close the awareness and knowledge gap on data protection, rights and breaches. This could extend to establishing mechanisms for ongoing assessment of data protection practices across sectors, sharing lessons learned and successful strategies on data protection documented from diverse businesses to inspire and guide other struggling businesses and communities.

e) Capacity building on data protection and related aspects for businesses, civil society and community platforms

Civil society organizations (CSOs) should organise regular training sessions for their staff, businesses and communities on data privacy laws, security best practices, and emerging threats like phishing and hacking. This serves a three tier agenda. Firstly, supporting the appointment and continuous training of Data Protection Officers (DPOs) and general building capacities of the businesses would enhance their compliance rates with the legal obligations on data protection. Secondly and in relation to civil society, enhanced capacities strengthen their ability to monitor businesses for compliance and advocate effectively for reforms including enabling CSOs to provide expert advice and support to vulnerable groups and communities on data protection frameworks. Thirdly, building the capacities of communities enhances citizenry oversight and demand for accountability from businesses in cases of data breaches and below-the required standards.

f) Advocacy and policy engagement on data protection

From the aforementioned research undertakings, CSOs can use the research findings and data to advocate for stronger legal frameworks, enforcement mechanisms, and clear guidelines that protect individual rights and promote responsible biometric data use. The research could also facilitate public awareness campaigns on biometric data rights, emphasising the importance of informed consent, data security, and individuals' right to access and delete their data. CSOs should also collaborate with policymakers to support reforms, review existing laws, and push for the adoption of international standards for data protection.

In conclusion, a collaborative effort involving the government, civil society, and private sector organisations is essential to establish a robust framework that ensures biometric data is collected, processed, and stored securely and ethically. By implementing clear policies, investing in training and technology, and fostering transparency, these stakeholders can significantly reduce privacy risks and build public confidence in biometric and data collection practices.

ANNEXTURE A:

FOCUS GROUP DISCUSSION GUIDE

Note to Moderator: Please use the following script to facilitate a discussion among participants. Make sure to probe answers to clarify details and explore reasons for stated opinions and actions.

Introduction

Good morning/ afternoon. I am (your name), and this is (name of note taker). I am here to help moderate the discussion, and (name of note taker) will help me take notes and make sure we correctly capture each relevant detail.

We would like to have a discussion about how businesses in Uganda collect and use data, the impact on user privacy, and the potential violations of digital rights that may occur. This study is being conducted by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as part of The Advancing Respect for Human Rights by Business in Uganda (ARBHR).

Note that there are no right or wrong answers: so, please answer as honestly as you can. Everyone is entitled to their views. All your responses are completely anonymous.

We would like to audio record the discussion to ensure accuracy of information. The records will be used only for the purpose of transcription and will not be shared. Note that no one's name or personal information will be shared or reported publicly in any part of this research. In order for us to be able to hear each other and respect each other's opinions, once the discussion has started, please make sure that we observe the following:

- Only one person must speak at a time;
- We will not show any form of disrespect to each other; and
- Everyone should feel free to speak and express their views and opinions.

Does anyone have any questions at this stage? (Answer accordingly if so.)

If you understand, if there are no further questions, and if you are in agreement with this please confirm for the recording by stating a clear "Yes".

Section 1: Participant Background and Knowledge

1. How would you describe your level of awareness of digital rights issues, particularly regarding data privacy, data protection, and surveillance?
2. Are you familiar with any laws or policies related to data collection and privacy in Uganda? If yes, which ones?
3. What do you understand by the term "biometric data"? Can you give examples of biometric data you think businesses in Uganda collect?
4. Why is it important for businesses to safeguard the privacy and security of individuals' data that they collect?

Section 2: Perceptions of Data Collection and Use

1. What concerns, if any, do you have about how businesses are collecting, processing, storing and utilizing the data of their visitors, customers, and employees?
2. Do businesses in Uganda have adequate knowledge and capacity to responsibly collect and use [biometric] data? Please explain your answer.

Section 3: Perceived Impact on Businesses

1. 1What would you consider to be the main reasons why businesses in Uganda collect and process users' data? [For the moderator: Consider areas such as:
   a) Improve their operational efficiency
   b) Gain customer trust and satisfaction
   c) Compliance with legal and regulatory frameworks
   d) Financial implications]
2. Have you observed any positive impacts of [biometric] data collection on business operations? If yes, please share examples.
3. How does the improper handling of [biometric] data potentially affect the reputation or performance of a business entity?
4. (Look out for e.g. Loss of customers and customer trust, collapse of business, blacklisting of the business, etc.)

Section 4: Perceived Impact on Digital Rights

1. What risks do you think may arise from businesses collecting, processing and using [biometric] data?
   (a) Breaches of privacy
   (b) Cybersecurity threats
   (c) Misuse of data (e.g., surveillance or profiling)
   (d) Other (please specify)
2. What challenges do you think businesses face in ensuring lawful and secure collection and processing of personal data?
3. Do you think surveillance practices, such as using data for monitoring staff, are necessary for businesses? Why or why not?

Section 5: Recommendations and Solutions

1. What actions do you think the government, civil society organisations, and private sector associations should undertake to help businesses improve their data collection practices and address concerns about privacy and surveillance?

We shall contact you in case we have additional questions?

On behalf of CIPESA, thank you very much for your participation.

ANNEXTURE: "B": KEY INFORMANT INTERVIEW GUIDE

Introduction
Dear Sir/ Madam,

My name is (your name). I am conducting this interview on behalf of the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as part of The Advancing Respect for Human Rights by Business in Uganda (ARBHR) project, which seeks to reduce human rights abuses connected to business activities in Uganda, particularly those impacting women and children.

The study CIPESA is conducting seeks to explore how the current data collection, privacy, and surveillance policies and practices by businesses affect digital rights in Uganda. Specifically, the study will examine how businesses collect, process, and utilise data (including that of a biometric nature), how these processes impact users' privacy, and the potential infringements on digital rights. The findings will inform advocacy efforts to foster accountability and promote a digital environment that respects and protects individual rights.

You have been identified as one a key informant interview given your experience and work around human rights/ natural resource governance/ business responsibility in Uganda. The information gathered will be treated with confidentiality, including your identity (should you choose to remain anonymous).
We would like to audio record the discussion to ensure accuracy of information. The records will be used only for the purpose of transcription and will not be shared. The interview will last about one hour.

If you understand, if there are no further questions, and if you are in agreement with this please confirm for the recording by stating a clear "Yes".

Section 1: Participant Background and Knowledge
1. Name/title of respondent (Optional if you prefer anonymity):
2. Organization:
3. How would you describe your level of awareness of digital rights issues, particularly regarding data privacy, data protection, and surveillance?
4. What do you understand by the term "biometric data"? Can you give examples of biometric data you think businesses in Uganda collect?
5. Are you familiar with any laws or policies related to data collection and privacy in Uganda? If yes, which ones?
6. Why is it important for businesses to safeguard data privacy and security?
7. Has your organization adopted digital technologies in its operations? If yes, please describe the types of technologies or systems used.

Section 2: Perceptions of Data Collection and Use
1. What concerns, if any, do you have about how businesses are collecting, processing, and utilizing users' data?
2. Do you think businesses in Uganda have adequate knowledge and capacity to responsibly collect and use [biometric] data? Please explain your answer.
3. Do businesses adequately inform their customers, employees, and users about how their data is collected, processed, stored, and used? Please explain your responses.

Section 3: Perceived Impact on Businesses

1. What would you consider to be the main reasons why businesses in Uganda collect and process users' data? [For the moderator: Consider areas such as:
   a) Improve their operational efficiency
   b) Gain customer trust and satisfaction
   c) Compliance with legal and regulatory frameworks
   d) Financial implications]
2. Have you observed any positive impacts of [biometric] data collection on business operations? If yes, please share examples.
3. Do you think that the improper handling of [biometric] data can harm a business's reputation or performance? Why or why not?
4. How does the (mis)use of data affect employee or customer trust in businesses?

Section 4: Perceived Impact on Digital Rights

1. What risks do you associate with businesses collecting and using [biometric] data?
   (a) Breaches of privacy
   (b) Cybersecurity threats
   (c) Misuse of data (e.g., surveillance or profiling)
   (d) Other (please specify)
2. What challenges do you think businesses face in ensuring the ethical and lawful collection and processing of data?
3. Do you think surveillance practices, such as using data for monitoring staff, are necessary for businesses? Why or why not?
4. In your view, do businesses in Uganda take enough precautions to prevent misuse of data?

Section 5: Recommendations and Advocacy

15. What do you think businesses in Uganda can do to better uphold digital rights, especially concerning biometric data and surveillance?
16. How can frameworks like the United Nations Guiding Principles on Business and Human Rights (UNGPs) be applied more effectively in the Ugandan business context?
17. What role should government and civil society play in ensuring responsible biometric data use and protecting digital rights?

Any final thoughts?

Can we contact any of you in case we have additional questions?

This concludes our discussion. We want to thank you very much on behalf of CIPESA for your participation. If you have any questions, I would be happy to answer them. Thank you.

ANNEXTURE

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 10B Katalima Crescent, Naguru.| P.O.Box 122311,Kampala (U)
+256 414 289 502| programmes@cipesa.org| @cipesaug
www.cipesa.org