Lawpoint Uganda
Making the Law Easy and Accessible

DPO PRIVACY CENTRE EAST AFRICA

Limitations in Uganda's Data Protection and Privacy Act Cap 97

Narrow Scope Of Sensitive Data And Lack Of Explicit Protections For Biometrics, Genetics, And Location Data

Foreword

"Data privacy has over the years become one of the most compelling areas of law in our digital age, shaping how legal scholars and practitioners think about personal rights in the technology space. Uganda's Data Protection and Privacy Act, Cap. 97, provides an important legal framework to govern the collection, processing, and use of personal data, while safeguarding fundamental rights, such as access, correction, and security of personal information. The statute applies to all entities handling personal data within Uganda, as well as those outside the country processing data of Ugandan citizens, and stipulates conditions for lawful processing of certain sensitive information. It is noteworthy that whereas the law recognises certain special personal data, including biometric and genetic information, as deserving heightened care, it does not explicitly cover all emerging categories, such as location data, in the same structured way observed in other standards, for example, the European Union's General Data Protection Regulation (GDPR), which clearly defines sensitive data categories and imposes additional protections. This article offers a timely exploration of these nuances and their implications for fostering a firm, rights-based culture of data governance in Uganda."

Foreword by **Advocate PAUL SSEMAKULA**

Introduction

Uganda's Data Protection and Privacy Act Cap 97 which was enacted on March 1, 2019, serves as the primary framework for regulating the collection, processing, use, storage, and disclosure of personal data[1]. The Act applies to entities within Uganda and those outside handling Ugandan citizens' data, aiming to protect individual privacy amid growing digital adoption[2].

However, critics highlight its limited definition of sensitive personal data[3], which excludes explicit heightened protections for biometrics, genetic information, and location data categories increasingly prevalent in sectors like mobile money, national identification number (NIN) systems, and ride hailing apps. This gap potentially enables misuse without stringent oversight, as such data often defaults to general processing rules.

Scope of Sensitive Personal Data Under the DPPA

The DPPA does not formally define "sensitive personal data" but outlines "special categories" in **Section 9**, requiring additional safeguards[4]. These include data revealing religious, philosophical, or political opinions; ethnic or tribal origin; political allegiance; membership in political organizations; criminal records; or health records[5]. Processing of these categories is prohibited unless justified by law, public duty, national security, crime prevention, contractual obligations, medical purposes, or legal compliance, and always with the data subject's consent where applicable[6].

This narrow scope contrasts with broader international standards, such as the **EU's General Data Protection Regulation (GDPR)**, which explicitly includes genetic data, biometric data for unique identification, and health data as special categories warranting stricter controls. In Uganda, biometrics (e.g., fingerprints, facial recognition), genetics (e.g., GPS tracking) are treated as general personal data under Data Protection and Privacy Act Cap 97[7], defined as any identifiable information like nationality, age, occupation, or identification numbers. They lack the elevated protections afforded to the listed special categories, such as mandatory impact assessments or bans on automated processing without explicit consent.

1. Data Protection and Privacy Act Cap 97
2. Section 1 of the DPPA Cap 97
3. 2015 submission by Unwanted Witness
4. Section 9 of the DPPA Cap 97
5. Ibid
6. Gtuganda.co.ug
7. Section 2 of the Act

Absence of Explicit Rules for Biometrics, Genetics, and Location Data

Biometric and genetic data are immutable and highly sensitive, breaches cannot be remedied like changing a password. Location data enables profiting of habits, associations, and even sensitive attributes. Yet the DPPA applies only general principles: consent for collection[8], with exceptions for legal or public duties. No tailored rules exist for pseudonymization, minimization, or impact assessments in these areas.

This gap is evident in sectors like, Mobile Money (e.g., MTN MoMo), where biometrics and location aid fraud prevention but risk unauthorized profiling. Also in ride hailing gaps (e.g., Uber, Bolt), collecting continuous location without sector-specific limits. Finally, also in the NIN system, managed by the **National Identification and Registration Authority** (NIRA), which mandates biometrics for services like SIM registration, banking, and healthcare.

Reports of NIN data vulnerabilities including a 2017 breach and 2025 allegations linking the database to trafficking networks highlight risks, especially with biometrics shared for telecom verification enabling potential mass tracking[9].

Key Recent Cases Demonstrating Enforcement and Gaps

Enforcement seemed to be strengthened in 2025, though cases rarely address the sensitive data scope directly for example in **Ssekamwa Frank & 3 Others v Google LLC[10]**. Four Ugandans complained that Google collected and processed their personal data (names, emails, browsing history, location) without PDPO registration and transferred it abroad without safeguards, violating **Sections 29** on (registration) and cross-boarder rules. The PDPO ruled Google a data controller/collector under Ugandan law, ordered registration within 30 days, and required evidence of complaint transfers. No compensation was awarded for distress (court remedy needed). This landmark extraterritorial ruling shows growing reach but focused on registration, not biometric/location sensitivity.

Also in **PDPO v Ronald Mugulusi[11]** Following a borrower complaint, Mugulusi was convicted for operating without PDPO registration and unlawfully processing data without consent, creating/sharing a Whatsapp video exposing the borrower's name, photo, and contacts to pressure loan repayment. He pleaded guilty to non registration, received a UGX 300,000 fine and criminal record; the privacy count settled via reconciliation with compensation. This first criminal conviction under the DPPA signals enforcement against consent breaches in digital lending, but again, not tied to special categories like biometrics.

Authoritatively, in the case of **Initiative for Social and Economic Rights (ISER) & 2 Others v Attorney General & NIRA[12]** Civil society challenged mandatory NIN use for services (healthcare, social grants, education), arguing exclusion of vulnerable groups (up to 40% without IDs), surveillance risks from centralized biometrics, and privacy violations despite the DPPA. The High Court dismissed the case, deeming the system non-digital/offline and not it ignored biometric risks and exclusion impacts, underscoring weak judicial scrutiny of biometric heavy systems.

Additional 2025 matters include PDPO actions on data retention/breach notification (e.g., Chipper Technologies) and NIRA's response to breach allegations with security pledges, but no major resolutions on biometrics/genetics as special categories.

Recent Updates and Enforcement

The Data Protection and Privacy Regulations, 2021 (effective March 12, 2021) detail registration and transfers but do not expand sensitive categories. The PDPO (under NITA-U) had registered over 9,800 entities by early 2026[13]. The above cases mark progress in enforcement and extraterritorial application, yet the narrow sensitive data definition persists.

8. Section 7
9. Pdpo.go.ug
10. PDPO Decision, Complaint No. 08/11/24/6683, July 18, 2025
11. Director, Nano Loans Microfinance Ltd / Quick loan App) (Makindye Standards, Wildlife and Utilities Court, Conviction July 10, 2025
12. High Court Miscellaneous Cause No. HCT-00-CV-MC-0066-2022, Ruling June 10, 2025
13. Cipit.strathmore.edu

Conclusion and Recommendations

The DPPA's limited scope leaves biometrics, genetics, and location data exposed to misuse in critical sectors. Recent PDPO rulings and the first criminal conviction show enforcement momentum, but they highlight gaps rather than close them especially for high-risk data in NIN and digital services. Amendments are needed to classify these as special categories, require impact assessments, and align with global standards[14].

About the Author

Ssali John Ndigejjerawa
ssalijunior666@gmail.com
Director of Webinars — **Lawpoint Uganda**

14. Law.yale.edu