STRIKING THE BALANCE BETWEEN DATA PRIVACY, BANKING, AND INNOVATION IN UGANDA

INTRODUCTION

In Uganda's rapidly evolving financial landscape, banks and fintech companies now rely heavily on the collection and analysis of personal data to design new products, enhance efficiency, and expand financial inclusion. Yet, as data-driven innovation accelerates, concerns about how personal information is collected, safeguarded, and shared have also intensified.

This creates a central policy and regulatory challenge: how can Uganda promote technological advancement in the financial sector while ensuring that individuals' privacy rights are respected and protected?

Striking this balance is essential for building public trust, encouraging responsible digital transformation, and creating a stable environment for both consumers and innovators. Weak data protection measures can expose individuals to significant risks, but overly restrictive rules may also stifle creativity, investment, and growth.

This discussion, therefore, examines how Uganda can navigate these competing priorities, protecting data privacy without undermining the innovation that drives modern banking.

BACKGROUND

Historically, banks treated customer data merely as transactional records used for reconciliation and archiving. Today, data has become a strategic asset and a core input for credit assessment, risk modelling, product personalization, regulatory compliance, and fraud prevention. In the digital economy, data is effectively the currency that powers fintech business models.

Over the last decade, Uganda's financial sector has expanded rapidly, with fintech companies growing at an impressive pace and providing services that traditional banks have struggled to deliver. Although formal financial inclusion stands at about 58%, many Ugandans, especially those in rural or low-income communities, still find it difficult to access conventional banking services. This gap has created space for fintechs and mobile money operators to play a transformative role by offering affordable, convenient, and user-friendly financial solutions.

This digital shift has also reshaped how financial data is collected, managed, and used in Uganda. Banks, telecoms, and fintech startups now handle large volumes of sensitive information, including identity records, transaction histories, device data, and behavioral patterns used for credit scoring and product development.

While these innovations create opportunities for collaboration, such as between financial service providers and industry bodies like FITSPA, they also bring regulatory challenges. Rapid technological change has introduced new uncertainties for policymakers, raising questions about data protection, cybersecurity, and the responsible sharing of data. Many of Uganda's data and technology laws predate artificial intelligence, algorithmic systems, and cloud-based finance, creating a growing gap between rapid technological change and a legal framework that remains limited.

An Overview of Uganda's Data Privacy and Digital Finance Regulatory Landscape

1. **The Constitution of the Republic of Uganda, 1995**

The Constitution protects individuals against unlawful searches, intrusions, and interference with private correspondence. Traditionally, these safeguards applied to physical spaces such as the home or personal property. Today, however, as personal information is stored in phones, computers, cloud platforms, and financial databases, the notion of a "search" extends beyond physical entry. Accessing a person's data, whether by state agencies, digital lenders, telecoms, or financial institutions, constitutes an intrusion of privacy.

Likewise, constitutional protection of "correspondence and communication" now encompasses emails, mobile messages, digital transaction records, metadata, geolocation data, biometric identifiers, and other forms of digital communication. Unauthorized collection, surveillance, or sharing of such information amounts to interference with privacy. Digital footprints are, therefore, an extension of the individual and warrant the same constitutional protection as physical property.

For Uganda's financial sector, this interpretation renders data harvesting without informed consent, excessive data collection by digital lenders, and unlawful disclosure of customer information constitutionally questionable. It places a clear obligation on banks, fintechs, telecoms, and regulators to treat personal data as protected property that cannot be accessed or processed arbitrarily.

2. **The Data Protection and Privacy Act, Cap. 97**

The Act provides Uganda's primary legal framework governing the collection, use, storage, and disclosure of personal data, and is central to balancing privacy with innovation in banking and fintech. It requires valid consent, data minimisation, security safeguards, fair and transparent processing, and restricts unlawful disclosure and cross-border transfers, while granting individuals rights over their data. In practice, however, weak enforcement and rapid technological change mean that excessive data collection, unclear consent mechanisms, and poorly controlled third-party processing persist across the digital finance ecosystem.

3. **The National Payment Systems Act, Cap 59**

The National Payment Systems Act, Cap 59, provides the legal foundation for licensing, supervising, and regulating payment service providers and fintechs in Uganda, with a core focus on safety, reliability, and consumer protection. While not a data protection statute, it imposes clear obligations to secure systems, safeguard customer information, ensure confidentiality, and prevent unauthorized access to payment data, including through local data-hosting requirements. Although these measures strengthen trust and oversight, stringent licensing and compliance thresholds create regulatory friction that can constrain innovation, particularly for smaller fintechs.

4. **Tier 4 Microfinance Institutions and Money Lenders Act, Cap 61, and its Regulations**

The Tier 4 Microfinance Institutions and Money Lenders Act, Cap 61, regulates SACCOs and money lenders through licensing, supervision, and consumer protection, indirectly affecting data practices in microfinance. While oversight by UMRA promotes basic standards of record-keeping and confidentiality, the Act does not directly address data privacy and leaves significant gaps in the regulation of digital and app-based lenders. As a result, risks relating to consent, data minimisation, and abusive data practices persist, highlighting the need for complementary privacy enforcement and regulatory harmonisation.

5. **The Digital Lending Guidelines for Tier 4 Microfinance Institutions and Money Lenders, 2024**

The 2024 Digital Lending Guidelines issued by UMRA seek to promote responsible, transparent digital lending by setting standards on disclosures, governance, cyber-risk, and data handling for Tier 4 institutions. While they introduce basic data protection obligations and require compliance with the DPPA, their scope excludes app-based, cross-border, and online digital lenders that pose the greatest consumer risk. The absence of clear technical standards or minimum benchmarks further weakens enforcement, resulting in uneven data practices and limited regulatory impact.

The Data Compliance Challenges in Uganda Today

1. **Data hosting, cross-border transfers, and infrastructure constraints**

Compliance challenges arise because financial laws require institutions to host data locally, while modern digital finance depends heavily on global cloud infrastructure. This mismatch limits innovation, increases operational costs, and prevents institutions from adopting advanced AI tools or international fintech services. Even though the DPPA permits cross-border data transfers, significant risks remain when data is sent to countries with weak privacy protections, as seen in past incidents involving foreign marketing companies accessing Ugandan phone numbers.

2. **Faulty consent architecture**

Many digital lenders obtain data before users even download applications. Privacy notices are often bundled with vague terms and conditions, resulting in invalid consent. This undermines transparency and exposes users to unfair data practices.

3. **Weak third-party management**

Organizations may have strong internal governance but weak oversight over third-party processors. Contracts lack clear obligations, monitoring is inconsistent, and external vendors frequently operate without adequate controls. This creates major vulnerabilities in the data value chain.

4. **Overlapping mandates.**

NITA (U), BoU, UMRA, and UCC all regulate different aspects of the ecosystem, yet their mandates frequently overlap. Banks and payment providers answer to BoU, Tier 4 lenders to UMRA, telecommunications platforms to UCC, and ICT and data governance standards to NITA (U). This fragmentation creates conflicting requirements, duplicated compliance processes, and uncertainty about which regulator has final authority. As a result, fintechs and digital lenders struggle to navigate multiple obligations, face higher compliance costs, and operate within gaps where oversight is unclear or inconsistently enforced.

Practical steps towards a balanced and innovative ecosystem

To build a regulatory environment that encourages innovation while safeguarding consumers, organizations, and regulators should consider the following actions:

1. Strengthen multi-agency coordination between BoU, UMRA, UCC, and NITA-U to reduce fragmentation and duplication.
2. Introduce a unified licensing regime for all digital lenders, including non-deposit-taking fintechs.
3. Adopt risk-based capital adequacy requirements tailored to fintech business models, ensuring liquidity buffers and operational resilience.
4. Improve consent architecture by requiring clear, standalone consent notices and restricting pre-permission data access.
5. Mandate robust third-party risk management, including contractual safeguards, audits, and monitoring.
6. Expand regulatory sandboxes to allow innovators to test products under supervision.
7. Review data localization rules to allow secure use of global cloud services while maintaining necessary sovereignty safeguards.
8. Increase enforcement capacity to ensure uniform compliance across both large and small operators.

Conclusion

Uganda's digital finance ecosystem is rich with innovation but challenged by regulatory fragmentation, outdated legal frameworks, and uneven enforcement. Data has become central to financial operations, yet the laws governing its use and protection have not kept pace with technological change. Achieving a balance between data privacy, banking stability, and digital innovation requires coordinated regulation, modernized legal frameworks, and strengthened compliance practices across the financial sector. With targeted reforms and collaborative regulatory oversight, Uganda can build a safer, more inclusive, and innovation-friendly digital financial environment.

About the author:

PRISCILLA NAYIGA

Priscilla is a Ugandan lawyer with a focus on fintech law, banking, and corporate finance.

She is a Legal Associate at Diamond Advocates, where she advises fintech companies, financial institutions, and technology-enabled businesses on digital financial services regulation.

She holds a Master of Laws (LLM) and Bachelor of Laws (LLB) from Makerere University School of Law, as well as a Diploma in Legal Practice from the Law Development Centre.

About the author:

GALANDI TONY KIIRE

Galandi is the Managing and Founding Partner of Diamond Advocates. He is also the WONE Global Technology Leader for Uganda.

He is also the founder of Lawtech Associates and Consult, the company behind the Legal AI Research Assistant.

He also won the 2025 Uganda Law Society Digital Excellence Award for leading a pioneering legal practice at the forefront of innovation and legal technology.

He holds a Master's in Institutional Leadership and Management, a Postgraduate Diploma in Legal Practice, and an LLB from Makerere University.