BEYOND THE LOAN: ANALYSING THE PRIVACY IMPLICATIONS OF THE PRACTICES OF DIGITAL LOAN APPS IN UGANDA

By

Kityo Martin[1]

[1] About the author: Kityo Martin is a legal scholar with a keen interest in the intersection of technology and human rights. Having completed his LLB at Islamic University in Uganda, Kityo is currently pursuing the bar course at the Law Development Centre, Lira in Uganda. Kityo has dedicated much of his research to exploring the impact of digital technologies on individual freedoms in Uganda. His work focuses on privacy law, artificial intelligence regulation, and other emerging technologies. He has also worked on several compliance projects for tech companies and actively engages in discussions about digital privacy frameworks in Africa. He is passionate about safeguarding the rights of individuals in the digital age while promoting responsible innovation. Many thanks to Aida Gift Kisambira for her thoughtful peer review and constructive feedback, which greatly contributed to the final version of this paper.

TABLE OF CONTENTS

1. INTRODUCTION

Technology is steadily driving development in Uganda across sectors like public service,[2] agriculture,[3] and health.[4] The financial technology (fin-tech) sector is no exception. Among these developments are the digital ways of obtaining credit or loans with easier access as compared to traditional banking methods.

The days of waiting in long bank queues for loan assessments are behind us. Presenting property ownership documents as collateral or undergoing on-site verifications is no longer necessary.

Digital loan apps have replaced the 'old' way of doing things providing a convenient alternative to traditional credit access, requiring no collateral or extensive formalities. These apps promote financial inclusion, allowing individuals in financial need to obtain funds quickly. However, this convenience comes at a cost.

Unlike banks that collect financial data such as income or salary records, credit history, and property information presented as security to determine if a person qualifies for a loan, digital loan apps instead collect personal data like location, contacts, device details, and access users' SMS messages. This includes not only personal but also special (sensitive) data[5] which has far-reaching impacts on an individual's privacy than personal data. Many of these apps employ practices including invasive data collection, unauthorised access to contacts and SMS messages, and unclear data sharing arrangements. Some demand excessive permissions, allowing them to track users' locations, browsing history, and device information hidden in complex and unclear privacy policies.

---

[2] T. Nalubega and D. E. Uwizeyimana,'Artificial Intelligence Technologies Usage for Improved Service Delivery in Uganda' (2024) 12 Africa's Public Service Delivery & Performance Review 11 at page.5; *See also* UNESCO Uganda, Report on Training Workshops on Artificial Intelligence for Disaster Risk Reduction in Uganda 2021-2022 (August 2022) https://unesco-uganda.ug/wp-content/uploads/2022/08/Report-for-Artificial-Intelligence-for-Disaster-Risk-Reduction-in-Uganda_compressed.pdf (accessed 2 October 2024).

[3] ShareAmerica, 'AI is Improving Africa's Harvests' (US Embassy, 26 March 2024) https://ug.usembassy.gov/ai-is-improving-africas-harvests/ accessed 6 August 2024.

[4] Alex Mirugwe, Adoption of Artificial Intelligence in the Ugandan Health Sector: A Review of Literature (School of Public Health, Makerere University, Kampala 2024) <http://dx.doi.org/10.2139/ssrn.4735326> accessed 2 October 2024; Mona Minakshi et al, 'High-Accuracy Detection of Malaria Mosquito Habitats Using Drone-Based Multispectral Imagery and Artificial Intelligence (AI) Algorithms in an Agro-Village Peri-Urban Pastureland Intervention Site (Akonyibedo) in Unyama Subcounty, Gulu District, Northern Uganda' (2020) 12(3) Journal of Public Health and Epidemiology 202.

[5] Data Protection and Privacy Act, Cap 97, Section 9.

These concerns thus necessitate the emergence of this paper to critically examine the practices of digital loan apps, assessing their impact on users' right to privacy and their compliance with privacy laws, including the 1995 Constitution of Uganda[6] and the Data Protection and Privacy Act.[7]

Part one introduces the paper while part two outlines the legal framework governing the regulation of digital loan apps and the protection of personal data in Uganda. Part three adopts a doctrinal approach to critically analyse the practices of digital loan apps, particularly in customer acquisition, risk assessment, and management. This analysis, based on privacy policies, compares these practices with the requirements of the Data Protection and Privacy Act (DPPA). With this, the paper aims to highlight the broader implications of digital lenders' practices on individuals' right to privacy in Uganda, identifying gaps in compliance. It calls for digital lenders to enhance their adherence to regulatory frameworks and urges institutional regulators to implement stronger mechanisms that protect user privacy within the digital financial sector.

1.1 Conceptual Background

Before proceeding further, it is important to define the major terms on which this study is based.

Personal data refers to information that can be used to identify an individual directly or indirectly.[8] Personal data goes beyond the name of an individual. It includes other information such as a national identity number, location data and opinions of an individual as long as such data can be used to distinguish one individual from another in terms of identity.

On the other hand, special (sensitive) personal data is a type of personal data regarded as highly intrusive and vulnerable due to the potential for significant harm if such data is accessed by unauthorised persons.[9] Special data includes information which reveals details about sexual orientation, medical records, financial information, political beliefs, and religious or philosophical

[6] Constitution of the Republic of Uganda 1995 (as amended), ('Constitution')
[7] Cap 97 ('DPPA').
[8] DPPA, Section 2; General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2 ('GDPR'), Article 4; *See also* Muhangi, Kenneth. "Overview of the data protection regime in Uganda." Journal of Data Protection & Privacy 3, no. 1 (2019): 82-92.
[9] DPPA, Section 9.

beliefs of an individual.[10] Unauthorised access or leakage of such sensitive information can lead to severe consequences for individuals, including reputational damage, identity theft, discrimination, and exclusion thus the unique naming–special/sensitive.[11] Because of its potential for leading to significant harm, sensitive personal data requires stringent protection measures and can only be collected in exceptional circumstances such as when a data subject has given explicit consent.[12]

Digital loan apps are mobile applications that offer users a convenient and often automated way to access loans. They allow users to apply for and receive loans entirely through their smartphones, eliminating the need for physical paperwork or in-person interactions. These apps use technology such as artificial intelligence to automate the verification process and data analytics to assess creditworthiness and risk to facilitate quick loan approvals. Digital loan apps in Uganda include ManguCash, iSente, FlyPesa, Kasente, Banana Credit, Fair Credit, Mara Loans among others.

Given the digital loan sector's profitability, the space has seen traditional players, like banks and mobile money providers, and emerging ones, such as small and mid-sized credit service providers, enter the space—registering considerable success in customer acquisition and profits.[13]

2. LEGAL FRAMEWORK

Various laws provide for the regulation, licensing and operation of digital loan apps in Uganda. This section provides for a brief overview of the core legislation governing the regulation of digital loan apps.

[10] DPPA, Section 9.
[11] L Noonan, '5 Damaging Consequences of Data Breach: Protect Your Assets' https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach (accessed 2 October 2024).
[12] DPPA, Section 9(3); Makulilo, Alex Boniface, 'Protection of Personal Data in Sub-Saharan Africa' PhD dissertation, Universität Bremen, 2012 at page 174, http://repository.out.ac.tz/2503/1/00102854-1.pdf. (accessed 10 September 2024).
[13] Uganda Bankers' Association. "Series II: Digital Lending: The Supply Side, the Supporting Functions, and the Regulatory Environment." https://ugandabankers.org/wp-content/uploads/2024/07/Series-II-Digital-Lending-Article-The-Supply-side-the-Supporting-Functions-and-the-Regulatory-Environment.pdf. (accessed September 10, 2024).

2.1 Domestic Legal Framework

2.1.1 1995 Constitution of the Republic of Uganda

The Constitution is the supreme law in Uganda and all other laws must conform to its provisions to retain validity.[14] The Constitution envisages the right to privacy as a fundamental human right provided for under Article 27 broadly encompassing freedom from intrusion into one's private life, home and communications. Scholars, Warren and Brandeis have also interpreted the scope of this right to include the 'right to be left alone.'[15]

2.1.2 Data Protection and Privacy Act Cap 97

The DPPA was enacted in 2019 laying out a legal foundation for the protection of personal data of individuals. The DPPA provides for different safeguards including principles of data protection,[16] such as transparency, accountability, transparency, lawful and fair collection of data to be adhered to by data collectors, controllers and processors to safeguard individuals' right to privacy. It further provides for the rights of data subjects[17] and the mechanisms for seeking redress in case of any breach by entities and organisations.[18] Additionally, the DPPA provides for key institutional actors such as the Personal Data Protection Office (under the oversight of the National Information Technology Authority) to oversee the regulation and application of the DPPA.[19] The DPPA is also complemented by the Data Protection Regulations[20] which were passed to operationalise and elaborate on provisions in the DPPA.

2.1.3 Tier 4 Microfinance Institutions and Money Lenders Act, Cap 61

The Tier 4 Microfinance Institutions and Money Lenders Act[21] lays down provisions regulating microfinance institutions and money lenders in Uganda. It aims to promote transparency, protect borrowers' rights, and establish standards for financial operations within the sector.[22] The Act

[14] Constitution, Article 2(2).
[15] Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4 (1890): 193-203.
[16] DPPA, Section 3.
[17] DPPA, Part V.
[18] DPPA, Part VII, VIII.
[19] DPPA, Section 4.
[20] 2021 ('DPPRs)
[21] Tier 4 Microfinance Institutions and Money Lenders Act, Cap 97 ('Tier 4 Microfinance Institutions and Money Lenders Act').
[22] Tier 4 Microfinance Institutions and Money Lenders Act, Section 2.

mandates that non-deposit-taking microfinance institutions must provide borrowers with clear information on loan procedures, financial costs, and borrower rights while ensuring the confidentiality of personal data.[23]

2.1.4 Digital Lending Guidelines, 2024

In January 2024, the Uganda Microfinance Authority passed the Digital Lending Guidelines[24] in response to the growing trends of digital credit loan providers and emerging consumer protection concerns.[25] The Digital Lending Guidelines set forth various licensing requirements These guidelines are crucial in setting regulations and oversight in this rapidly growing sector to help strike a balance between increased access to finance and also protection of consumer rights.

3. PRIVACY IMPLICATIONS OF DIGITAL LOAN APP PRACTICES

3.1 Deficiencies in Registration Practices

Registration involves the formal submission of identity details to national regulatory authorities to ensure that a data collector or controller complies with established legal standards for the collection and processing of personal data. This step verifies the legitimacy of entities handling personal data and their commitment to complying with regulatory requirements.

Section 29 of the DPPA requires data controllers and processors to register with the personal data protection office to have their companies entered in the data protection register.[26] Similarly, Guideline 11 of the Digital Lending Guidelines requires digital credit service providers to operate at least one physical office with additional requirements to indicate their business address via digital channels such as websites and mobile apps.

On searching the data protection register for registered loan apps, most loan apps such as Flypesa are not registered.[27] While some such as Numida business loans, Mangu Cash, iSente are

[23] Tier 4 Microfinance Institutions and Money Lenders Act, Section 67.
[24] 2024.
[25] Busein Samilu, 'Online Money Lenders Preying on Ugandans,' Daily Monitor (31 August 2024), https://www.monitor.co.ug/uganda/news/national/online-money-lenders-preying-on-ugandans-4185722. (accessed 31 August 2024).
[26] Tier 4 Microfinance Institutions and Money Lenders Act, Section 61 which requires money lenders to operate under licenses issued by the Uganda Microfinance Regulatory Authority; *See also* DPPRs, Regulation 15.
[27] This position is as a result of a search conducted in September 2024.

registered, there is largely no continuing compliance with the obligations of the DPPA on their end (as discussed further in this paper). Others do not indicate their physical address on their digital channels.

It is important to note that even after registration, entities have a continuous obligation to adhere to the data protection and privacy laws of Uganda to ensure compliance.

3.2 Ambiguities in User Consent

Consent is the process of obtaining permission from a user before collecting or processing their personal data. It forms the foundation of data privacy, acting as the gateway to any operation on an individual's information. The extent of access to an individual's personal data hinges on the consent they provide—whether they open the door wide or keep it firmly shut.

In the case of digital loan service providers, the collection of personal information begins once users agree to the privacy policies of the apps or websites they interact with. However, many users, especially those seeking financial assistance through digital loan apps, often do not thoroughly review, read, or fully understand the terms and conditions to which they consent. Several factors contribute to this, including a general culture of laziness to read, illiteracy, and a lack of awareness regarding the privacy risks involved. Yet, regardless of education or literacy level, the most common factor influencing this behaviour is the vulnerability of users in need of financial assistance. In their urgency to obtain loans, individuals frequently consent without properly scrutinizing the terms they agree to.

At their most vulnerable, individuals seeking loans from digital loan apps are driven by financial necessity—whether immediate or long-term. At this point, their primary goal is to access the funds they need, and they are willing to do whatever it takes, including accepting terms and conditions without hesitation. This highlights the responsibility of digital loan service providers to ensure that their users are fully aware of the implications of their choices given, especially given their vulnerable state

The DPPA emphasises the importance of consent in various ways. Section 7 mandates that data collectors obtain prior consent from data subjects before collecting or processing their personal

data.[28] Exceptions to this requirement are made for legal, public duty, national security, law enforcement, or medical purposes.[29]

Section 9 of the DPPA further strengthens protections surrounding special (sensitive) categories of personal data—such as religious beliefs, political opinions, financial information, and health records. This provision prohibits the collection of such sensitive data unless explicit consent is given by the data subject or the data collection is necessary for legal, employment, or legitimate non-profit activities.[30]

Guideline 10.2 of the Digital Lending Guidelines permits digital credit providers to obtain consent through electronic means, provided that such consent is authentic.[31] To meet this standard, users must have a clear understanding of the actions being carried out on their data.

Thus, consent must be specific, clear, freely given, and informed. Simply obtaining consent as a formality is not enough. Digital loan providers must ensure that the consent they obtain from users is meaningful, especially when dealing with sensitive data. Proactive measures of translating privacy policies into local languages, using infographics, and simplifying complex terms can help users make much more informed choices when dealing with privacy policies.

3.3 Excessive Data Collection Practices

Section 3 of the DPPA provides for the principle of data minimisation which requires that entities collect and use only the necessary data. Additionally, Section 12 provides for the principle of purpose limitation which requires that entities use data only for a specified purpose and not beyond that for which the data was originally collected for.[32]

Guideline 24 of the Digital Lending Guidelines requires digital loan providers to obtain sufficient information to accurately identify their users. Cross-referencing this with the provisions of the DPPA cited earlier, the law creates an obligation for digital loan apps to collect only the data necessary for identification purposes.

[28] DPPA, Section 7.
[29] DPPA, Section 7(2).
[30] DPPA, Section 9(3).
[31] Digital Lending Guidelines, Guideline 10.2.
[32] DPPA, Section 12.

Typically, information such as a user's National ID, phone contact, and address is adequate to verify their identity. Yet, these digital loan apps collect an excessive array of personal data including device specifications i.e model number, clipboard data, apps on a user's device, calendar information, text messages and call log records.[33] These categories of data enable digital loan apps to study a user's financial status and spending habits, location, and third-party contact information.

This broad scope of data collection far exceeds what is necessary for identification, directly violating both the data minimization and purpose limitation principles. This ultimately infringes upon the rights of borrowers and third parties through the gathering of information unrelated to the loan purpose.[34]

3.4 Financial Profiling of Users

Digital loan providers use personal data including location, salary records, clipboard data, messages and business cash flows, to analyse an individual's financial habits and status. These forms of data are used as reference points to assess the loanworthiness of an individual, establish a user's financial identity[35] and manage the risk associated with loan provision. Based on these data points, digital loan apps come up with financial profiles of users on which decisions to grant or deny loans are based.

The use of credit or financial profiles as the primary basis for loan decisions by digital loan apps is problematic. The process of verifying user identity online (eKYC- Electronic Know Your Customer) relies on a system of using national identity cards (National IDs) which have for long been a point of contestation. Scholars and civil society organisations such as Unwanted Witness and Centre for Human Rights and Global Justice argue that the bureaucratic and expensive process of acquiring or replacing a National ID may lock out an average Ugandan who cannot afford the

[33] *See* Mangu Cash 'Privacy Policy,' https://mangucash.cc/privacy-policy (accessed 31 August 2024). Mangu Cash for instance, requests users to grant their app permission to read SMS messages. They claim that their app is only able to read messages related to finance. However, this is not right as the app reads all messages and only sieves out those that are necessary to it–financial-related ones.

[34] Paul Murungi, "Money Lending Apps Asking for Too Much Data, Govt Says," Daily Monitor, August 2, 2023, https://www.monitor.co.ug/uganda/business/technology/money-lending-apps-asking-for-too-much-data-govt-says--4314756. (accessed 17 September 2024).

[35] Privacy International, ' Fintech: Privacy and identity in the new data-intensive financial sector.' 2017 https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf. (accessed 17 September 2024).

costs associated.[36] This is particularly concerning since a National ID in Uganda has been inevitably turned into an 'access key' to social services like health care, financial services from banks, and civic participation in elections among others without which an individual risks being locked out of the system 'and left to die.'[37] This indeed leaves out the Ugandans who would want to access digital loans but lack a National ID.

Furthermore, digital loan providers track and analyse users' borrowing patterns, repayment histories, and even spending behaviour through user credit profiles.[38] While this information is used to determine loan eligibility and limits, it also exposes users to potential misuse of their personal data, especially when such profiling is shared with third parties or used beyond the original purpose.

Users who fail to meet loan obligations suffer consequences on their credit profiles such as reduced access to future loans. In a bid to maintain a good credit profile, borrowers continuously take out loans and repay them in time to maintain favourable credit profiles, often to increase their loan limits and just to stay in the 'good books' of digital loan apps. However, this practice can create a cycle of dependency and financial vulnerability, as users are driven to borrow continuously. Meanwhile, app owners benefit from this cycle, accumulating wealth as users are repeatedly forced into borrowing widening the wealth gap between digital loan providers and their users.[39] This

[36] Center for Human Rights and Global Justice (CHRGJ), Initiative for Social and Economic Rights (ISER), and Unwanted Witness. 'Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,' (2021) at p.28, https://chrgj.org/2021-06-08-report-chased-away-left-to-die/. (accessed 10 September 2024); Unwanted Witness. 'Championing an Inclusive, Trustworthy, and Accountable Approach to Uganda's ID Infrastructure and the Transition to a New Generation ID (Position Paper).' (2024), at pp. 17, 18, https://www.unwantedwitness.org/wp-content/uploads/2024/06/UW-position-paper-07.06.2024-Full.pdf, (accessed 10 September 2024).

[37] Center for Human Rights and Global Justice (CHRGJ), Initiative for Social and Economic Rights (ISER), and Unwanted Witness. 'Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,' (2021), https://chrgj.org/2021-06-08-report-chased-away-left-to-die/. (accessed 10 September 2024).

[38] See Privacy International. 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector' (2017), at page 31, https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf, (accessed 10 September 2024); Centre for Intellectual Property and Information Technology Law (CIPIT), "Privacy and Data Protection Practices of Digital Lending Apps in Kenya," Journal of Intellectual Property and Information Technology Law 1, no. 1 (2021), at page 141, https://doi.org/10.52907/jipit.v1i1.68.

[39] Centre for Intellectual Property and Information Technology Law (CIPIT), "Privacy and Data Protection Practices of Digital Lending Apps in Kenya," Journal of Intellectual Property and Information Technology Law 1, no. 1 (2021), at page 135, https://doi.org/10.52907/jipit.v1i1.68.

cycle of dependency not only increases financial vulnerability for users but also deepens privacy concerns.

3.5 Lack of Transparency in Decision-Making Processes

Section 3 of the DPPA obligates entities to operate with transparency, ensuring openness and actively involving data subjects in the collection, processing, use, and retention of their personal data. Similarly, Section 67 of the Tier 4 Microfinance Institutions and Money Lenders Act mandates transparency by obligating lenders to provide borrowers with clear, accurate information about loan procedures, financial obligations, and associated costs.

The practice of digital lenders is that they utilise various forms of information such as location, phone type, cash flows, salaries etc in assessing whether a user is worthy of being granted a loan. Despite the many complex decision-making processes employed on user information, these processes are hardly disclosed to users.

While some digital loan providers seek users' permission by requiring agreement to privacy policies before accessing personal data, they often fail to inform borrowers that this data will be used to assess whether they should be granted loans. As a result, many users remain unaware that the information they provide is being analysed to determine their eligibility for loans–whether high or low amounts.

This keeps users in the dark on the technical know-how of the dos and don'ts to ensure that they remain in the good books of the lenders and keep receiving loans. Users who unknowingly fail to keep their credit profiles in the clear with the decision-making indicators end up arbitrarily getting reduced loan amounts, and sometimes totally denied loans. This lack of transparency contradicts Section 71(1) of the Tier 4 Microfinance Institutions and Money Lenders Act, which mandates non-deposit-taking microfinance institutions to provide borrowers with full and accurate information on micro-lending procedures, conditions, and associated financial costs.

Many digital loan apps lack a solid online presence, missing key components such as websites where users can access essential information. Some are not even available on official app platforms like the Play Store or App Store. Even some with an online presence often fail to publish clear

privacy policies,[40] leaving users in the dark about how their personal data is collected, used, and protected.

3.6 Third-Party Privacy Risks Associated with Debt Recovery Practices

Conceding, it is right for credit-providing companies to recover their monies lent to people. However, this should be done in the rightful ways envisaged by the law.

Guideline 15 of the Digital Lending Guidelines bars credit recovery practices which involve threats, use of obscene language, or contacting persons who were not originally a party to the loan. It further requires that when a loan becomes delinquent, a user must be duly informed via E-mail/SMS but not use unsolicited frequent calls.[41]

The practice however is; that in case a user defaults on making payments in time, digital loan service providers take radical measures such as repetitive calls, sending abusive text and WhatsApp messages, calling contacts in a borrower's phonebook informing them how the borrower failed to pay their loan. In other instances, when initial attempts to contact the user who took out the loan fail, they resort to spam contacting their next of kin and other persons they believe are closely related to the loan defaulter. They proceed to use derogatory language and issue threats causing fear amongst users and also damaging their reputation.

These practices undermine not only the privacy of the individual concerned but also the privacy rights of other persons (third parties) who are contacted by the loan providers in a bid to recover their monies.

[40] *See* Banana Credit, https://www.bananacreditug.com/; LoanGo, https://www.loango.vip/pc.html; (as of 5th October 2024.)
[41] Digital Lending Guidelines, Guideline 15.

3.7 Automated Data Processing

Digital loan apps use artificial intelligence (AI) to study the financial details of users and assess their eligibility for loans.[42] These processes are often fully automated with no humans in the loop to intervene in the decision-making process.[43]

Section 27 of the DPPA only allows automated processing which significantly affects the rights of a data subject under exceptional circumstances. The provision further puts in place extra conditions of notifying a data subject in case a decision that significantly harms the rights of a data subject is taken based on a fully automated process.

The AI algorithms that perform loan assessments are not perfect. They are prone to bias, mistakes and inconsistencies.[44] Leaving AI systems to fully perform actions of credit assessment, risk management and customer acquisition can lead to undesirable consequences such as inaccuracies and discrimination potentially excluding users from accessing loans and worsening existing systemic inequalities.

3.8 Conditional Access to Data Rectification Rights

Section 16 grants individuals the right to request corrections or rectifications of their data held by a data collector or controller. This aligns with the principle of data quality and accuracy, which seeks to ensure that the information collected from individuals is both accurate and complete, thereby avoiding the potential consequences that arise from inaccuracies.

Despite this provision, some digital lending companies make the right of an individual to update or correct information conditional on payment of a potential fee.[45] While some don't request a fee,

[42] David Mwesigwa, "Cameras, Mobiles, Radios – Action!": Old Surveillance Tools in New Robes in Uganda Collaboration on International ICT Policy for East and Southern Africa (CIPESA) at page 234, https://cipesa.org accessed 8 August 2024; *See also* JUMO https://jumo.world/ accessed 8 August 2024.
[43] David Mwesigwa, "Cameras, Mobiles, Radios – Action!": Old Surveillance Tools in New Robes in Uganda Collaboration on International ICT Policy for East and Southern Africa (CIPESA) at page 234, https://cipesa.org accessed 8 August 2024; *See also* JUMO https://jumo.world/ accessed 8 August 2024.
[44] M, Kityo et al, "A Critical Analysis of the Data Protection and Privacy Act, 2019 in Regulating Artificial Intelligence to Protect the Right to Privacy in Uganda" (LLB dissertation, Islamic University in Uganda, 2024).
[45] *See* Mangu Cash 'Privacy Policy,' https://mangucash.cc/privacy-policy. (accessed 31 August 2024).

they put in place bureaucratic administrative processes such as contacting them to have the data of an individual corrected.[46] Human rights including the right to privacy should not come at a cost.[47]

Individuals must be able to request that information about them be corrected and updated to reflect the most accurate records about them without facing any hurdles. This can be best achieved by implementing self-help systems that enable users to correct their own information without needing to contact anyone and with less technicalities.

3.9 Concerns Over Collection of Personal Data from Third Parties

Digital money lenders such as Airtel and MTN Uganda promise comprehensive security measures to protect users' personal data.[48] These measures may include PIN requirements, secret codes, One Time passwords (OTPs), security questions, and other encryption protocols. However, while these safeguards can enhance security, they are not completely fool proof.

However, there are vulnerabilities in the data transmission process of mobile money providers[49] as messages related to mobile money transactions are sent and stored on users' phones without stringent encryption protocol, making them susceptible to interception or unauthorised access.[50] Digital loan apps exploit these vulnerabilities by reading all text messages on a user's phones and filter out financial-related ones.[51] This access provides insights into a user's amounts of money sent and received, spending patterns and the overall mobile money account balance of a user.

Section 11(1) of the DPPA mandates that personal data must be collected directly from the data subject and not from other third-party sources. Exceptions may be made for publicly available

[46] Pesafly, 'Privacy Policy', https://web.pesafly.com/ (accessed 31 August 2024).
[47] C, Kalema and A, Kigozi, 'The Essential Role of Cost-Free Access to Personal Data in the Digital Age', Unwanted Witness (.org), https://www.unwantedwitness.org/the-essential-role-of-cost-free-access-to-personal-data-in-the-digital-age/, (accessed August 31, 2024).
[48] *See* MTN Group, 'Data Privacy and Protection,' March 2023, https://www.mtn.com/wp-content/uploads/2023/03/Data-Privacy-and-Protection-.pdf.
[49] Ali, Guma, Mussa Ally Dida, and Anael Elikana Sam. "Evaluation of key security issues associated with mobile money systems in Uganda." Information 11, no. 6 (2020): 309.
[50] *See* Privacy International. 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector' (2017), at page 29, https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf, (accessed 10 September 2024).
[51] *See* Mangu Cash 'Privacy Policy,' https://mangucash.cc/privacy-policy. (accessed 31 August 2024).

data, collection made with prior consent, or collection of data necessary for law enforcement and national security.[52] However, even in these cases, strict limitations and safeguards apply.

For instance, where consent is purportedly given; such consent must be informed, freely given and specific, and where data is collected for purposes of law enforcement; such collection must adhere to principles of proportionality, necessity, and legality to respect an individual's right to privacy.[53]

As noted earlier, the dubious process of obtaining consent from digital loan app users is fraught with a lack of sufficient information for users to make informed choices regarding the data collection practices of digital loan app users.

4. CONCLUSION

In conclusion, while digital loan apps provide convenient access to credit and promote financial inclusion,[54] they present significant privacy concerns. These apps often collect excessive personal and sensitive data, sometimes without clear user consent or transparency, leading to risks in financial profiling, automated decision-making, and data sharing with third parties. Despite the DPPA and other legislation offering guidelines to mitigate these risks, many digital lenders fail to comply with these regulations fully. To address these challenges, digital loan providers must enhance their privacy practices, and regulators must strengthen oversight to ensure user privacy protection as the sector continues to grow. In a commendable move, the Uganda Micro-Finance Regulatory Authority has recently issued notice to the public about loan apps operating illegally without the requisite licences.[55] However, more efforts are needed from institutions such as the PDPO to ensure protection of users' privacy.

[52] DPPA, Section 11(2).
[53] Dr. Lagu Charles and 3 others vs Attorney General (Miscellaneous Cause No. 370 of 2020) [2023] UGHCCD 10 (31 January 2023) at page 12.
[54] Evans, Olaniyi. "Connecting the poor: the internet, mobile phones and financial inclusion in Africa." Digital Policy, Regulation and Governance 20, no. 6 (2018): 568-581.
[55] Agaba Nicholas, 'Government Lists 59 Illegal Online Loan Apps' https://kampalapost.com/content/government-lists-59-illegal-online-loan-apps (accessed 2 October 2024).

5. BIBLIOGRAPHY

Constitution

1995 Constitution of the Republic of Uganda (as amended)

Legislation

Digital Lending Guidelines, 2024

Data Protection and Privacy Act, Cap 97

Tier 4 Microfinance Institutions and Money Lenders Act, Cap 61

Data Protection and Privacy Regulations, 2021

General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Cases

Dr. Lagu Charles and 3 others vs Attorney General (Miscellaneous Cause No. 370 of 2020) [2023] UGHCCD 10 (31 January 2023)

Dissertation

M, Kityo et al, "A Critical Analysis of the Data Protection and Privacy Act, 2019 in Regulating Artificial Intelligence to Protect the Right to Privacy in Uganda" (LLB dissertation, Islamic University in Uganda, 2024).

Articles

Agaba Nicholas, 'Government Lists 59 Illegal Online Loan Apps' https://kampalapost.com/content/government-lists-59-illegal-online-loan-apps

Alex Mirugwe, Adoption of Artificial Intelligence in the Ugandan Health Sector: A Review of Literature (School of Public Health, Makerere University, Kampala 2024) <http://dx.doi.org/10.2139/ssrn.4735326>

Ali, Guma, Mussa Ally Dida, and Anael Elikana Sam. "Evaluation of key security issues associated with mobile money systems in Uganda." Information 11, no. 6 (2020): 309.

Busein Samilu, 'Online Money Lenders Preying on Ugandans,' Daily Monitor (31 August 2024), https://www.monitor.co.ug/uganda/news/national/online-money-lenders-preying-on-ugandans-4185722

C, Kalema and A, Kigozi, 'The Essential Role of Cost-Free Access to Personal Data in the Digital Age', Unwanted Witness, https://www.unwantedwitness.org/the-essential-role-of-cost-free-access-to-personal-data-in-the-digital-age/.

Centre for Human Rights and Global Justice (CHRGJ), Initiative for Social and Economic Rights (ISER), and Unwanted Witness. 'Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,' (2021), https://chrgj.org/2021-06-08-report-chased-away-left-to-die/.

Centre for Intellectual Property and Information Technology Law (CIPIT), "Privacy and Data Protection Practices of Digital Lending Apps in Kenya," Journal of Intellectual Property and Information Technology Law 1, no. 1 (2021), https://doi.org/10.52907/jipit.v1i1.68.

David Mwesigwa, "Cameras, Mobiles, Radios – Action!": Old Surveillance Tools in New Robes in Uganda Collaboration on International ICT Policy for East and Southern Africa (CIPESA), https://cipesa.org

Evans, Olaniyi. "Connecting the poor: the internet, mobile phones and financial inclusion in Africa." Digital Policy, Regulation and Governance 20, no. 6 (2018): 568-581.

L Noonan, '5 Damaging Consequences of Data Breach: Protect Your Assets' https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach

Makulilo, Alex Boniface, 'Protection of Personal Data in Sub-Saharan Africa' PhD dissertation, Universität Bremen, 2012, http://repository.out.ac.tz/2503/1/00102854-1.pdf.

Mona Minakshi et al, 'High-Accuracy Detection of Malaria Mosquito Habitats Using Drone-Based Multispectral Imagery and Artificial Intelligence (AI) Algorithms in an Agro-Village Peri-Urban Pastureland Intervention Site (Akonyibedo) in Unyama Subcounty,

Gulu District, Northern Uganda' (2020) 12(3) Journal of Public Health and Epidemiology 202.

MTN Group, 'Data Privacy and Protection,' March 2023, https://www.mtn.com/wp-content/uploads/2023/03/Data-Privacy-and-Protection-.pdf.

Muhangi, Kenneth. "Overview of the data protection regime in Uganda." Journal of Data Protection & Privacy 3, no. 1 (2019): 82-92.

Paul Murungi, "Money Lending Apps Asking for Too Much Data, Govt Says," Daily Monitor, August 2, 2023, https://www.monitor.co.ug/uganda/business/technology/money-lending-apps-asking-for-too-much-data-govt-says--4314756.

Privacy International, 'Fintech: Privacy and identity in the new data-intensive financial sector.' 2017 https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

Privacy International. 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector' (2017), https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

ShareAmerica, 'AI is Improving Africa's Harvests' (US Embassy, 26 March 2024) https://ug.usembassy.gov/ai-is-improving-africas-harvests/

T. Nalubega and D. E. Uwizeyimana,'Artificial Intelligence Technologies Usage for Improved Service Delivery in Uganda' (2024) 12 Africa's Public Service Delivery & Performance Review 11

Uganda Bankers' Association. "Series II: Digital Lending: The Supply Side, the Supporting Functions, and the Regulatory Environment." https://ugandabankers.org/wp-content/uploads/2024/07/Series-II-Digital-Lending-Article-The-Supply-side-the-Supporting-Functions-and-the-Regulatory-Environment.pdf.

Unwanted Witness. 'Championing an Inclusive, Trustworthy, and Accountable Approach to Uganda's ID Infrastructure and the Transition to a New Generation ID (Position Paper).' (2024), https://www.unwantedwitness.org/wp-content/uploads/2024/06/UW-position-paper-07.06.2024-Full.pdf

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4 (1890): 193-203.

Reports

UNESCO Uganda, Report on Training Workshops on Artificial Intelligence for Disaster Risk Reduction in Uganda 2021-2022 (August 2022)