MAKERERE UNIVERSITY

A CRITICAL ANALYSIS OF CRIMINAL LIABILITY UNDER UGANDAN DATA PROTECTION AND PRIVACY ACT, CAP 97: A CASE STUDY OF UGANDA'S DIGITAL LENDING SECTOR

BY

OYUA CHRIS CHARLES
22/U/21118/PSA

Contact:
Email: Chris.oyua@gmail.com
Phone: +256 772 587605

SUPERVISED BY

DR. ENGORU IVAN (PhD)

A DESERTATION SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF MAKERERE UNIVERSITY

JUNE 2026

DECLARATION

I Oyua Chris Charles declare that this research report is my original work and has never been submitted to any University for examination leading to any award.

Signature _____ Date 4th June 2026

Oyua Chris Charles

APPROVAL

This is to certify that the work presented in this dissertation is being submitted for examination in partial fulfilment of the requirements for the award of Bachelor of Laws Degree of Makerere University with my approval as the University Supervisor.

Signature : _____ Date : 4 JUNE 2026

Dr. Engoru Ivan (PhD)

DEDICATION

This research report is dedicated to my Late Father who wanted me to be a Lawyer and my family for their support and understanding during the period of undertaking the studies for a Bachelor of Laws Degree during a time of studying for a PhD in community development. It was overwhelming but the support and understanding of my family kept me going.

ACKNOWLEDGEMENT

First and foremost, I thank the almighty God for giving me opportunity to finally do this Bachelor of Laws Degree that I promised my late father I would do it and started the journey when he was still alive to witness it.

My Sincere appreciation goes to my Supervisor Dr. Engoru Ivan (PhD) for academic guidance and time taken off his busy schedule to supervise this research study.

Special thanks to respondents who accepted to give interviews during the research, I will not list them because they requested anonymity during the interviews. Without their cooperation and immeasurable contributions, this research would not have been easy to accomplish.

Lastly, I thank my course mates Kakaire Japheth, Onen Moses, Ssekubwa Ronald, Asibazuyo Harriet, Akiteng Racheal, Amodo Jesca, Daniel Mwanguzi, Diana Anzoa and Hilda Soki to mention but a few, who helped me a lot during this course.

May the Almighty reward you all!

ABSTRACT

This study examined the effectiveness of Sections 35 to 39 of the Data Protection and Privacy Act, Cap 97 in regulating criminal liability within Uganda's digital lending sector. The study specifically assessed the extent to which the Act establishes individual and corporate liability for unlawful processing of personal data, the enforcement challenges faced by the Personal Data Protection Office (PDPO), the deterrent effect of sanctions provided under the Act, and how Uganda's criminal enforcement model compares with the administrative enforcement framework under the European Union General Data Protection Regulation (GDPR).

The study adopted a descriptive cross-sectional research design using a mixed-methods approach combining qualitative interviews and secondary legal analysis. Data was collected from key informants including officials from the PDPO, the Criminal Investigations Directorate, the Uganda Microfinance Regulatory Authority, the Judiciary, and selected digital lending companies.

The findings reveal that while Sections 35 to 39 of the Act provide a strong legal foundation for criminal liability in data protection, enforcement remains limited due to institutional, technological, and jurisdictional challenges. The PDPO faces difficulties in investigating offshore and anonymous digital lenders, as well as, evidentiary constraints in prosecuting digital offences. Although sanctions under the Act, including imprisonment and fines, demonstrate strong legal deterrence in principle, their practical effectiveness is weakened by low monetary penalties and limited enforcement intensity. The study further finds that Uganda's enforcement model is more punitive compared to the GDPR's administrative approach, which prioritises compliance and corrective enforcement.

The study concludes that although Uganda's legal framework under the Data Protection and Privacy Act in regulating criminal liability within Uganda's digital lending sector is robust in design, its effectiveness depends on strengthened institutional capacity, clearer regulatory guidance, and improved enforcement coordination. Recommendations include strengthening PDPO capacity, clarifying consent standards, enhancing cross-border enforcement mechanisms, and adopting a more balanced enforcement pyramid combining administrative and criminal measures

LIST OF ACRONYMNS

AWS	Amazon Web Services
BoU	Bank of Uganda
Cap. 97	Data Protection and Privacy Act, Chapter 97 (Laws of Uganda)
CID	Criminal Investigations Directorate
DPP	Director of Public Prosecutions
GDPR	General Data Protection Regulation (European Union)
IDIs	In-Depth Interviews
KII	Key Informant Interview
ML	Money Lenders
ODPP	Office of the Director of Public Prosecutions
PDPO	Personal Data Protection Office
T4MFI	Tier 4 Microfinance Institutions
UMRA	Uganda Microfinance Regulatory Authority
UK	United Kingdom
USA	United States of America
CCTV	Closed Circuit Television
DDPA	The Data Protection and Privacy Act
DGPR	The General Data Protection Regulations
EC	European Commission
EU	European Union
GPS	Global Positioning System
ICT	Information Communication Technology
IDI	In-depth Interview
KII	key Informant Interview
LLC	Limited Liability Company
NITA U	National Information Technology Authority Uganda
OTT	Over-the Top
PDPO	Personal Data Protection Office
UGSC	Uganda Supreme Court
UGX	Uganda Shillings
UMRA	Uganda Microfinance Regulatory Authority

TABLE OF CONTENTS

DECLARATION i
APPROVAL ii
DEDICATION iii
ACKNOWLEDGEMENT iv
ABSTRACT v
LIST OF ACRONYMNS vi
TABLE OF CONTENTS vii

CHAPTER ONE: INTRODUCTION AND BACKGROUND TO THE STUDY 1
1.0 Introduction 1
1.1 Background and Rationale of the Study 1
1.2 Statement of the Problem 5
1.3 The Purpose and Objectives of the Study 6
1.4 Research Questions 6
1.5 Justification of the Study 7
1.6 Scope of the Study 8
1.7 Conceptual Framework 9
1.8 Theoretical Framework 11
1.9 Significancy of the Study 12

CHAPTER TWO: LITERATURE REVIEW 13
2.0 Introduction 13
2.1 The Concept of Criminal Liability in Data Protection 13
2.2 Digital Lending and the Privacy for Credit Trade off 14
2.3 Corporate Veil and Vicarious Liability Under Sections 38 and 39 15

CHAPTER THREE: METHODOLOGY 18
3.0 Introduction 18
3.1 Methodology 18
3.2 Population and Sample Size 18
3.3 Sample Selection 19
3.4 Data Collection Methods and Tools 19
3.5 Data Analysis 19
3.5 Ethical Considerations 20
3.6 Limitations of the Study 20

CHAPTER FOUR: PRESENTATION, ANALYSIS AND INTERPRETATION OF FINDINGS 21
4.0 Introduction 21
4.1 Effectiveness of Sections 35 to 39 of the DPPA in Regulating Criminal Liability. 21
4.2 Assessment of the Practical Challenges of the PDPO in Prosecuting Digital Lenders. 24
4.3 Assessment of Sanctions and Their Effectiveness in Deterring the Misuse. 25
4.4 Comparative Analysis of Uganda's DPPA and EU's GDPR. 28

CHAPTER FIVE: CONCLUSIONS AND RECOMMEDNATIONS 31
5.0 Conclusions 31
5.1 Recommendations 33

BIBLIOGRAPHY 37

APPENDICES 40
Appendix I: Interview Guide for Officials of the Personal Data Protection Office (PDPO) 40
Appendix 2: Interview Guide for CID Officers 41
Appendix 3: Interview Guide for UMRA Officials 42
Appendix 4: Interview Guide for Digital Lenders 43

CHAPTER ONE: INTRODUCTION AND BACKGROUND TO THE STUDY

1.0 Introduction

This chapter presents the background to the study, statement of the problem, the aim and objectives of the study, research questions, research design, the scope of the study, the theoretical framework, the conceptual framework, Justification of the study and the significance of the study.

1.1 Background and Rationale of the Study

The Data Protection and Privacy Act, Cap 97 (originally enacted as the Data Protection and Privacy Act, 2019) is Uganda's primary legislation for safeguarding personal information. It was enacted to give effect to Article 27(2) of the 1995 Constitution of Uganda, which protects the right to privacy. The law was consolidated as Chapter 97 (Cap 97) in the Laws of Uganda following a revision by the Law Reform Commission in 2023 under its constitutional mandate of revision and reform of legislation in Uganda[1].

What Triggered the Law: The Act was introduced to address several gaps in Uganda's legal and digital landscape. Uganda lacked a comprehensive law to protect personal data in the digital age. While the 1995 Constitution guaranteed a general right to privacy, there were no specific rules governing how modern organizations collected, used, or sold personal information and with the rapid growth of technology, data became a valuable commodity for businesses and government, the law was needed to prevent unjustified data collection and exploitation in the "information age. Another major reason for introducing the law was to bring Uganda's legal framework in line with International standards like the European Union's General Data Protection Regulation (GDPR)[2] and the African Union Convention on Cyber Security and Personal Data Protection[3].

The Debate of the Bill and Major Concerns Raised: The debate surrounding the Data Protection and Privacy Bill (which became Cap 97) when introduced at the parliament was extensive,

[1] Article 248 establishes the Uganda Law Reform Commission with a mandate to study and review the laws of Uganda to ensure their systematic development, modernization, and reform.
[2] Memorandum of Objects and Reasons, Data Protection and Privacy Act 2019 (Uganda).
[3] Ibid

spanning nearly four years from its introduction in 2015 to its passage in 2019[4]. Major commentaries from lawmakers, civil society, and legal experts focused on balancing state security with individual rights and ensuring the law was practical for Uganda's digital landscape. A central point of debate was the status of the regulatory authority. Critics and advocacy groups argued that the Personal Data Protection Office (PDPO) should be a fully autonomous body[5]. The law ultimately placed the PDPO under the National Information Technology Authority (NITA-U), leading to ongoing debates about whether it has sufficient independence to regulate other government agencies effectively. Analysts frequently highlighted the tension between the Bill's privacy protections and existing surveillance practices[6]. Analysts noted that while the Bill aimed to protect citizens, it needed to "balance the prerogatives of the State" in service delivery and national security.

There was specific debate regarding data collected without consent via private and government CCTV or drones, especially amidst proposals to link private security feeds to government networks. Legal analysts expressed concern that the Bill's enforcement mechanisms could be used to stifle legitimate speech[7]. They pointed out that "harsh penalties" in the Bill could potentially limit freedom of speech, journalistic work, and academic research if not clearly defined. During the legislative process, civil society pushed for the inclusion of modern digital rights that were initially missing or weak in the draft[8]. Debates centered on the absence of a "right to be forgotten" or "data portability," which are standard in international frameworks like the GDPR. Legislators and analysts debated how to handle the massive amounts of data already collected before the law existed.

How the Debate Changed the Bill: The legislative debate on the Data Protection and Privacy Bill significantly shifted its focus from being a purely human-rights-centric document to one that balances national security and state efficiency with individual privacy. Key changes from the original bill include: The original push for a completely autonomous commission was defeated.

[4] Uganda Parliament, *Report of the Committee on ICT and National Guidance on the Data Protection and Privacy Bill, 2015* (Parliament of Uganda, Kampala, 2018).
[5] Unwanted Witness Uganda, *Memorandum on the Data Protection and Privacy Bill, 2015* (Unwanted Witness Uganda, Kampala, 2018).
[6] Collaboration on International ICT Policy for East and Southern Africa (CIPESA), *State of Internet Freedom in Uganda Report* (various editions, especially 2018–2019).
[7] Article 19 Eastern Africa, *Uganda: Data Protection and Privacy Bill Analysis* (2018).
[8] CIPESA, *Analysis of the Data Protection and Privacy Bill* (2018)

Instead, the Personal Data Protection Office (PDPO) was established under the National Information Technology Authority (NITA-U). Critics argue this reduces the office's independence when investigating other government bodies. Lawmakers introduced broad exceptions for data processing without consent. Key justifications added or strengthened during the debate include national security, "public duty," and the prevention or detection of crimes. The final law solidified a requirement for all data collectors and controllers to register with the PDPO to create a regulated database of entities handling personal data[9]. Concerns over data misuse led to the inclusion of "harsh penalties," including heavy fines and imprisonment for unauthorized disclosure of data[10], which some legal analysts warn could have a "chilling effect" on investigative journalism[11].

In the process of compromising to pass the law, several core protections were diluted or omitted. For example, while data controllers must report breaches to the PDPO, there is no explicit mandatory requirement in the Act to inform the individuals (data subjects) whose data was actually compromised. Data Protection and Privacy Act, Cap 97, **Section 23** requires notification to the PDPO but does not expressly impose a general duty to notify affected data subjects. The final Act lacks clear, explicit exemptions for processing data for journalistic, artistic, or research purposes[12]. This omission is seen as a departure from the original intent of protecting all forms of expression. A key feature in international standards like the GDPR allowing users to easily move their data between service providers[13] was largely left out of the final Act. Critics argue that the final law is more concerned with regulating the industry through the PDPO than empowering the individual data subject to enforce their rights directly against powerful entities.

How the "new law" is affecting the lending sector: The way the Data Protection and Privacy Act was passed fundamentally changed criminal liability in the lending sector, turning traditional (and often aggressive) debt collection practices into prosecutable crimes. The law created a new level of personal risk for lenders who previously operated with impunity in a regulatory vacuum. Historically, debt collection disputes were handled as civil matters or simple regulatory breaches,

[9] Data Protection and Privacy Act, Cap 97, ss 29–30
[10] Data Protection and Privacy Act, Cap 97, ss 35–38.
[11] Article 19 Eastern Africa, *Uganda: Data Protection and Privacy Bill Analysis* (2018).
[12] CIPESA, *Analysis of the Data Protection and Privacy Bill* (2018).
[13] GDPR, art 20 (Right to Data Portability).

the Act changed this by making common practices like simply failing to register as a data collector with the PDPO, Public shaming of borrowers, Selling borrower data lists and Unauthorized data alteration a criminal violation of privacy. Another significant shift is that criminal liability is not just for the company, but for directors and senior managers personally. In July 2025, a director of Nano Loans Microfinance Ltd (Quickloan app) was convicted for using a borrower's photo and name in a WhatsApp video to threaten public exposure on TikTok[14]. The court ruled that using data for "shaming" is a criminal offense, not just a civil wrong. While some lenders feel that the Act makes it harder to recover debts, the law does not exempt borrowers from their financial obligations. Instead, it strictly regulates how lenders can pursue those debts, criminalizing "aggressive recovery" tactics that were previously standard in the industry.

Rationale of the Study

In Uganda, the fundamental right to informational privacy is protected under **Article 27** of the 1995 Constitution of the Republic of Uganda[15]. The protection under the Constitution is reinforced by the Data Protection and Privacy Act, Cap 97 and the Data Protection and Privacy Regulations, 2021, which regulate the collection, processing, use, storage, and disclosure of personal data[16]. The Data Protection and Privacy Act (DPPA), marks a significant milestone in Uganda's legal landscape by transforming data protection from a voluntary, "compliance checkbox" exercise into an area of enforceable criminal law[17]. The Act creates specific criminal offences for data collectors, processors, and controllers. The core criminal offences (Part VIII of the Act) covers specifically, sections 35-37. The Act creates both individual (personal) and corporate liabilities. Offences can lead to fines of up to 240 currency points (approximately UGX 4.8 million) or imprisonment for up to 10 years, or both. Corporations face substantial fines up to 2% of their annual gross turnover in addition to potential criminal convictions for their officers. In July 2025, the Personal Data Protection Office (PDPO) secured its first criminal conviction, in the case of ***Uganda v Mugulusi Ronald***[18] establishing that unauthorized use of personal data for

[14] Personal Data Protection Office (PDPO), *Press Release: PDPO Secures First Criminal Conviction under the Data Protection and Privacy Act, Cap. 97* (23 July 2025).
[15] P. Mbuga and R. Muhawe, 'Data Protection Laws of the World: Uganda', *DLA Piper* [online], 2020, https://www.dlapiperdataprotection.com/index.html?t=law&c=UG, accessed 6 February 2026.
[16] Ibid
[17] C. Kizito and A. Lule, 'Uganda's Personal Data Protection Office is getting serious: are you ready?', *Cliffe Dekker Hofmeyr* [online], 24 May 2024, cliffedekkerhofmeyr.com, accessed 29 January 2026
[18] Uganda v. Ronald Mugulusi, Criminal Case No. SUW-00-CR-CO-0070-2025

debt recovery such as sharing a debtor's photo on WhatsApp and threatening TikTok exposure constitutes a criminal offence. The director of the microfinance firm was fined, setting a precedent that, despite the criticisms above, the PDPO is ready to use criminal prosecution to enforce compliance.

Against this backdrop, this study analysed the strength and clarity of Sections 35 and 39 regarding individual and corporate criminal liability, It investigated the challenges the Personal Data Protection Office (PDPO) faces in prosecuting lenders, and critically examined the landmark cases of *Uganda v Mugulusi Ronald*[19] that resulted in PDPO's first conviction under the law. The study also assessed the sanctions (the fine and the threat of 10 years' imprisonment) examining whether these effectively deters lenders from using personal data of their borrowers (shaming borrowers) or they are seen merely as a cost of doing business. The study further drew a comparative analysis of Uganda's Data Protection and Privacy Act and the EU's GDPR that uses a reformed administrative model to enforce data protection.

1.2 Statement of the Problem

Despite the enactment of the Data Protection and Privacy Act, cap 97, which criminalizes the unauthorized disclosure and sale of personal data, Uganda's digital lending sector has witnessed a surge in aggressive debt recovery tactics that flagrantly violate borrower privacy. While **Sections 35-37** of the Act impose severe criminal penalties, including up to ten years' imprisonment for company directors, there remains a significant enforcement gap. Many digital lenders continue to harvest phonebook contacts and use shaming tactics like sharing borrower photos and debt status with third parties as a primary recovery tool. The Act contains significant "grey areas" that create legal and operational uncertainty for lenders. **Reporting verses Privacy Rights:** There is a persistent tension between a lender's duty to report defaulters and the data subject's right to object to processing. It is unclear if a borrower can use their right to object to data processing (Section 20) to legally block a lender from reporting them to the Credit Reference Bureau. **Jurisdictional Enforcement:** There is no clear mechanism for Ugandan authorities to enforce the Act against offshore digital lenders (OTTs) that claim they aren't actively targeting the local market. **Validity of Consent:** It remains questionable whether standard "click-wrap" agreements satisfy the Act's requirement for "specific and informed"

[19] Uganda v. Ronald Mugulusi, Criminal Case No. SUW-00-CR-CO-0070-2025

consent, particularly regarding sensitive data like phone contact lists. And **Cross-Border Data Transfers:** Many fintechs use centralized cloud servers (AWS, Google Cloud) located outside Uganda. Lenders face potential liability for using international cloud servers if the host country hasn't been officially "white-listed" by Uganda as having equivalent data protections. Without a critical analysis of these enforcement barriers and the recent judicial precedents (such as the Uganda v Mugulusi Ronald), the Act remains a "paper tiger," failing to deter high-tech privacy crimes while leaving millions of Ugandan borrowers vulnerable to digital harassment.

1.3 The Purpose and Objectives of the Study

The purpose of this study was to critically evaluate how criminal liability under the Ugandan Data Protection and Privacy Act, Cap 97 are being used to curb privacy abuses in the digital lending industry in Uganda. The main goal is to bridge the gap between the theoretical protections of the Act, and the practical, often predatory, digital lending environment.

Specific Objectives of the Study: The objectives of the study include:

1) To examine the effectiveness of Sections 35 and 39 of the Data Protection and Privacy Act, Cap 97 in establishing and enforcing criminal liability for unlawful data processing.
2) To assess the practical challenges faced by the Personal Data Protection Office (PDPO) in the prosecution of digital lenders.
3) To assess the sanctions (fines and the threat of 10 years' imprisonment) and their effectiveness in deterring lenders from misusing borrowers' personal data.
4) To conduct a comparative analysis of criminal liability under Uganda's Data Protection and Privacy Act and Administrative Enforcement under the EU General Data Protection Regulation (GDPR).

1.4 Research Questions

The study ultimately aims to answer the following research questions:

1. What are the strengths and weaknesses of Sections 35-39 of the Data protection and Privacy Act, Cap 97 regarding individual and corporate criminal liability?
2. What challenges and limitations does the Personal Data Protection Office (PDPO) face in enforcing the Act and how does the PDPO address the challenges and the limitations?
3. How are companies that deal in digital lending viewing the sanctions provided in the Act?

4. What are the key lessons learnt from the DPPA and the EU's GDPR and how can these lessons improve the legal framework for Data Protection and Privacy in Uganda?

1.5 Justification of the Study

The digital lending sector in Uganda is rapidly growing and has transitioned from a niche fintech service to a mainstream financial pillar, with loan disbursements skyrocketing by 110.8% to reach UGX 3.5 trillion in the 12 months leading to June 2025. According to the Bank of Uganda (BoU) 2024/25 Integrated Annual Report, the number of fintechs providing payment and lending services doubled between 2022 and 2024, reaching 43 regulated entities by December 2024. Experts project digital loan volumes could grow to UGX 17.7 trillion by 2029[20]. This explosive growth has created a parallel surge in systemic privacy abuses. Regulatory findings and judicial cases highlight that as the market scales, the "debt recovery" methods used by many providers increasingly rely on criminal data processing. For example, many apps force users to grant "blanket consent" to access contacts, photo galleries, and GPS data as a prerequisite for a loan, a practice explicitly banned by the 2024 Digital Lending Guidelines.

The first conviction under the Data Protection and Privacy Act (DPPA), Cap 97, the case of **Ronald Mugulusi** (Nano Loans/Quickloan) in July 2025, opened a new chapter in Ugandan jurisprudence. While it proved that data laws are enforceable, it raised several complex legal and procedural questions that warrant further analysis and this is the focus of this research. For example, the conviction was secured against a Director rather than the corporate entity alone. This raises questions about **The "Piercing of the Corporate Veil"** under what specific evidentiary thresholds will the Personal Data Protection Office choose to prosecute individual officers instead of the company? Also, under the legal principle of **Vicarious Liability,** to what extent can a director be held criminally liable for data breaches committed by lower-level employees (say a debt recovery agent) without their direct knowledge?

The PDPO's investigations into global giants like Google LLC have highlighted a massive enforcement gap. Majorly in the area of **Jurisdictional Enforcement:** How can Uganda enforce

[20] Uganda Bankers Association, 'Series II Digital Lending Article: The Supply-side, the Supporting Functions and the Regulatory Environment' [online], 2024, 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 13 April 2026.

criminal penalties (like imprisonment) against directors of lending apps that have no physical office or staff within the country? And **Data Sovereignty especially Cross-Border Data Transfers:** Does the current law provide enough "teeth" to compel foreign-domiciled entities to adhere to Ugandan criminal standards, or does it only penalize small, locally registered firms?

This research is therefore necessary because it not only addresses a "watershed moment" in Uganda's data privacy but also captures a historic pivot in Uganda's legal history, the moment data protection transitioned from a "paper tiger" to a penal reality.

1.6 Scope of the Study

The scope of the study is defined in the dimensions of the legal and regulatory scope, sectoral scope, institutional scope, geographical scope and the time it will take.

Legal and Regulatory Scope: The study will focus exclusively on the Data Protection and Privacy Act, Cap 97 and its accompanying 2021 Regulations. It will concentrate on the criminal provision in the Act (Sections 31-39) specifically examining transition of data breaches from civil torts to imprisonable offenses, the doctrine of vicarious criminal liability for corporate officers under section 38 and the extra-territorial reach of Ugandan law over foreign-based digital entities.

Sectoral Scope: The analysis will be confined to the Digital Lending Sector, a high-risk area characterized by "app-based micro-lending. The study will investigate the practice of "contact scraping" and unauthorized third-party data processing, it will also investigate the criminalization of "debt shaming" as an unlawful disclosure of personal data and it will investigate compliance levels among "ghost" lenders verses registered Tier 4 microfinance institutions.

Institutional Scope: The study will evaluate enforcement mechanisms and enforcement appetite of key Ugandan institutions including The Personal Data Protection Office as the primary regulator, The Criminal Investigations Directorate of the Uganda Police Force, The Uganda Microfinance Regulatory Authority and the Judiciary specifically focusing on landmark convictions in the *Nano Loan case*.

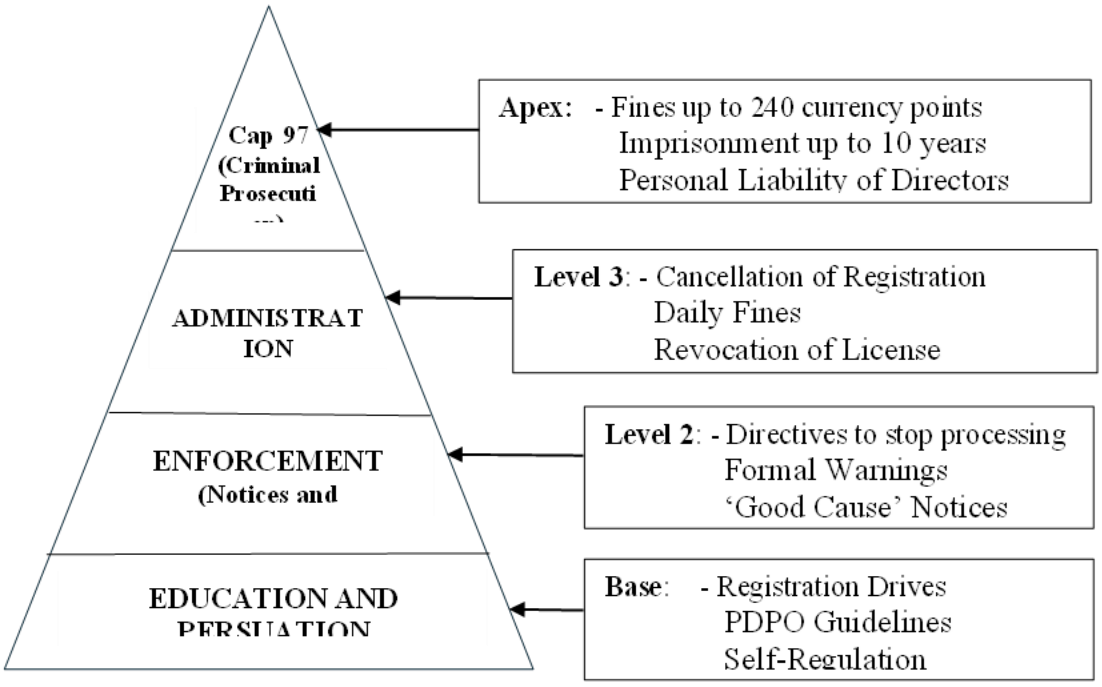
Geographical Scope: The research is limited to Uganda, though it considers the impact on international firms (like Google) that process data of residents withing Ugandan territory.

Time Scope: The study will primarily cover the period from the DPPA's commencement in 2019 through the landmark enforcement actions of July 2025 to February 2026.

1.7 Conceptual Framework

This study is anchored in the **Regulatory Governance Framework**, specifically examining how Uganda transitions from "soft" oversight to "hard" criminal enforcement to control the digital economy. The framework will adopt **Ian Ayres** and **John Braithwaite's** "Enforcement Pyramid." In the context of the DPPA Cap 97 as shown below:

The Enforcement Pyramid: DPPA Cap 97 Adaptation



The core philosophy of this model is that a regulator should be "gentle" at the base but "tough" at the apex, using the threat of the top levels to encourage compliance at the bottom. In application of this model:

- **Base:** At the commencement of the DPPA Cap 97, the PDPO should have focused on education and persuasion. ***Section 29*** provides for opening and maintaining the Data Protection Register. At this state, the PDPO would invite, persuade and every person, institution and public body collecting or processing personal data on the prescribed manner of making application to encourage them to register and implement the law promoting compliance through cooperation.
- **Level 2: Enforcement** – following the soft regulation at the base, the model encourages corrective actions as provided for under ***Section 23 Notification of data security breaches***. The PDPO issues a notice telling a lender to "stop scraping contacts" or "Delete illegally obtained data "within a specific time".
- **Level 3: Heavy Administrative Actions** – If a lender continues breaching data security, then PDPO can come in with heavy Administrative actions like sanctions like cancellation of Registration as provided for under ***Regulation 24***. PDPO can levy daily fines if the lender does not abide by set dates for taking a particular action they have been directed to take. PDPO can also revoke license of lenders that keep on breaching data security effectively shutting down the digital lender's legal right to operate.
- **Apex – Criminal Prosecution** - According to the philosophy of **Ian Ayres** and **John Braithwaite's** Enforcement Pyramid, criminal prosecution provided for under ***Sections 31-38*** should be reserved for egregious or repeat offenders.

The study will, using the **Ian Ayres** and **John Braithwaite's** Enforcement Pyramid model examine the operations of the PDPO. The *Nano Loan case* will be used to evaluation application of these levels and find out if PDPO skipped any level and the implication of skipping a level. John Braithwaite, along with Ian Ayres, argues that for the "base" of an enforcement pyramid (persuasion) to work, the "Apex" (severe, punitive sanctions) must be credible.

The Identification Theory will be used to bridge the gap between corporate acts and criminal intent. The study will investigate the "directing mind and will" of lending company (the directors) as the person who committee the data breach to understand the rationale for personal liability against corporate liability. Section 38 creates a legal bridge to hold a director personally liable for knowingly and willingly authorizing or permitting the contravention of offences under

the Act. For example, in the Nano Loan case, the director was held liable for the automated "scraping) algorithms programmed in their app.

1.8 Theoretical Framework

The study will be guided by integration of the Legal Positivism Theory, The Agency Theory and the Deterrence Theory to explain how the criminalization of data misuse reshapes the digital lending industry.

Legal Positivism (The Command Theory) - Anchored in the works of John Austin and H.L.A hart, this theory posits that the law is a system of commands backed by threats. The study will use this theory to analyse how the PDPO uses the DPPA as "the command" to transition from moral/ethical guidelines to punitive legal rule. The study will review sections 31-39 as the states ultimate tool to define "socially acceptable" behaviour in the digital lending industry. This theory is relevant to this study because it explains why the digital lending market norms likes debt-shaming are being forcibly replaced by legal norms.

The Agency Theory (Corporate Criminality) – This theory explores the relationship between the Principle (The corporation/ lender) and the Agent (the director/ manager). Traditionally, an agent's crime is seen as the company's problem. However, this study will apply the doctrine of identification, where the law identifies the director as the living embodiment of the company. Under Section 38 of the DPPA, the agency relationship is inverted. The director is no longer shielded by the corporate veil. This study will examine whether this personalization of liability is forcing directors to the application of the systems of their corporation more strictly.

General Deterrence Theory - proposed by Jeremy Bentham and Cesare Beccaria, the theory suggests that humans are rational actors who avoid crime if the pain of punishment outweighs the gain of the offense. According to Minjin Kim, digital lenders "rationally" choose to scrape data because the financial recovery (gain) is high and the risk is low (Kim, 2022). But it appears this is changing now; this study will analyse how PDPO's shift to criminal prosecution introduces "pain" like the threat of 10 years prison term and how that is affecting the profit-logic of predatory lending. The study will test whether the certainty and severity of the punishment are actually acting as a deterrent.

1.9 Significancy of the Study

The findings of this study will be specifically useful in the following dimensions.

- This study will contribute to the legal and jurisprudential value in Uganda's tech sector, in analyzing sections 31-39 of the DPPA, and the landmark case of *Uganda v Mugulusi Ronald* the study will highlight instances where the law can pierce the corporate veil making directors criminally liable for technical data breaches.
- For the digital lending sector, this study will clarify the redlines of data processing, registration with PDPO and the risks associated with not registration, tools that the industry uses like the scraped contact list. It will also provide insights on the safe methods of debt recovery and the effect of debt shaming on their business in Uganda.
- This study will highlight the restorative justice pathways of digital dignity. By analyzing the criminalization of data misuse, this study will provide insights for protecting vulnerable Ugandans from psychological and social harm caused by predatory lenders. This study will demonstrate that the law can finally catch up the digital wild west and it will open the eyes of Ugandan to seek justice through the PDPO and the police.
- This study will provide a case study for other African nations on how to use criminal law to force compliance from multi-national entities that lack a physical local presence to assert their digital sovereignty over global giants like Google LLC ruling.
- This study will provide insights into whether the current penal-heavy model is more effective than the administrative model used by the EU's General Data Protection Regulation (GDPR).
- This study will contribute to academic literature in the subject area of Data Protection and Privacy.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter offers an overview of significant literature published on the areas of: The Concept of Criminal Liability in Data Protection; The Ugandan Statutory Framework governing data protection and privacy; Digital Lending and the "Privacy-for-Credit" Trade-off; The Digital Lending Practices in Uganda; Corporate Veil and Vicarious Liability under Section 39; Enforcement challenges relating to the DPPA; and Comparative perspectives of the DPPA against similar legal frameworks.

2.1 The Concept of Criminal Liability in Data Protection

Criminal liability in data protection refers to the legal responsibility of individuals, such as employees and directors, for committing specific unlawful acts involving personal data that are punishable by criminal law[21]. Historically, data protection laws like the European Union's GDPR primarily used civil and administrative sanctions and fines[22]. Unlike civil liability, which focuses on compensating victims for harm, criminal liability aims to punish and deter the most serious violations, often leading to fines or imprisonment for individuals, employees and executives.[23]

The global landscape is shifting toward a "dual-track" approach where criminal and administrative law co-exist[24]. The criminalization of data protection marks a departure from purely civil remedies, driven by the need to deter crimes and address the unique harms of the digital age.

In Uganda, during the pre-colonial era, justice was primarily restorative, focusing on reconciliation and compensation like fines of livestock rather than punitive imprisonment[25]. The

[21] Nath, S. (2021) *Is There Criminal Liability Under GDPR? Section 170 Data Protection Act 2018*. Available at: https://www.nathsolicitors.co.uk/2021/03/05/is-there-criminal-liability-under-gdpr-section-170-data-protection-act-2018/ (Accessed: 2 May 2026).
[22] Ibid
[23] Ibid
[24] P. de Hert and G. Boulet, 'The co-existence of administrative and criminal law approaches to data protection wrongs', in D. Wright and P. De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Switzerland, Springer, 2016, p. 357–394.
[25] Katugugu, E. (2019) *Legal Alert: The Data Protection and Privacy Act is here*. Available at: https://www.pwc.com/ug/en/assets/pdf/legal-alert-data-protection-and-privacy-act.pdf (Accessed: 2 May 2026).

British introduced a formal criminal system during the colonial period (1894 – 1962) based on the Indian Penal Code of 1860 which became the basis for the Penal Code Act (Cap 120)[26]. Post independence, the 1995 Constitution of Uganda explicitly recognized the Right to Privacy under Article 27, prohibiting unlawful searchers and interference with communications[27]. The transition to digital governance necessitated specific laws to criminalize data misuse. Uganda developed the Computer Misuse Act (2011). This law marked an early move toward criminalizing digital harassment and unauthorized access, providing penalties of up to 10 years imprisonment for cyber offences. The land mark was the development of Data Protection and Privacy Act (2019), this Act transformed data privacy from a civil right into a criminal obligation. It established the PDPO to regulate data controllers and processors[28].

2.2 Digital Lending and the Privacy for Credit Trade off

Digital lending is the automated process of providing loans through online platforms and mobile apps, using technology for everything from customer acquisition to loan recovery. The privacy-for-credit trade-off is the exchange where borrowers share intensive personal data to prove creditworthiness in return for immediate financial access[29].

Digital lending relies on a fundamental trade-off including surrendering personal data in exchange for financial access[30]. While this enables credit for those without traditional collateral, it introduces significant privacy risks and potential exclusion.[31] To get digital loans, borrowers must grant intrusive app permissions. This data is often used not just for assessment but for aggressive debt collection, such as "social shaming" by contacting a borrower's phone contacts.[32] The key risks of privacy for credit trade-off for borrowers include data misuse. Personal

[26] Katugugu, E. (2019) *Legal Alert: The Data Protection and Privacy Act is here*. Available at: https://www.pwc.com/ug/en/assets/pdf/legal-alert-data-protection-and-privacy-act.pdf (Accessed: 2 May 20)
[27] Ibid
[28] *CyberLaws (Uganda)* (2026) Available at: file:///C:/Users/hp/Desktop/Cyber%20laws.pdf (Accessed: 2 May 2026).
[29] Ombija, S. and Chege, P. (2024) 'Time to take data privacy concerns seriously in digital lending', *Bowmans*, 14 May. Available at: bowmanslaw.com (Accessed: 2 May 2026).
[30] Uganda Bankers Association, 'Series II Digital Lending Article: The Supply-side, the Supporting Functions and the Regulatory Environment' [online], 2024, 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 13 April 2026.
[31] Ibid
[32] World Bank Group (2026) *Inclusive Digital Financial Services: Data Privacy*. Available at: [https://digitalfinance.worldbank.org/topics/digital-credit/data-privacy] (Accessed: 2 May 2026).

information can be leaked or sold, leading to identity theft or targeted fraud. Another risk is predatory practices like some apps use gathered data to identify "desperate" borrowers and charge interest rates exceeding 100%. Besides, most borrowers do not fully understand the long, complex "Terms and Conditions" they agree to, making meaningful consent nearly impossible[33].

2.3 Corporate Veil and Vicarious Liability Under Sections 38 and 39

The concepts of the Corporate Veil and Vicarious Liability represent two different legal pathways for assigning responsibility in a corporate setting. While the corporate veil generally protects individuals from the company's liabilities, vicarious liability does the opposite, often making the company responsible for the actions of its employees[34].

The "corporate veil" is a legal metaphor for the Separate Legal Personality of a corporation, a principle established in the landmark case of *Salomon v. Salomon & Co. Ltd*. It treats the company as a distinct legal entity from its shareholders and directors. However, courts may "pierce" or "lift" this veil to hold individuals personally liable, typically in cases of fraud, tax evasion, or when the company is a mere "sham" used to evade legal obligations[35]. Vicarious Liability is a doctrine that holds one party (the employer) responsible for the wrongful acts of another (the employee), provided those acts occur within the scope of employment. It requires a master-servant or principal-agent relationship and ensures victims can seek compensation from the employer, who typically has more resources ("deep pockets") and a duty to supervise[36].

Under the Uganda Data Protection and Privacy Act (Cap 97), the concepts of the Corporate Veil and Vicarious Liability are primarily operationalized through Section 38 (Offences by Corporations) and Section 39 (Regulations). While Section 39 itself focuses on the Minister's power to make regulations, it provides the administrative framework that enforces the liabilities established in the preceding sections. **Statutory Lifting of the Corporate Veil (Section 38).** The Act effectively "lifts" the corporate veil by holding individual officers personally liable

[33] World Bank Group (2026) *Inclusive Digital Financial Services: Data Privacy*. Available at: [Insert URL here] (Accessed: 2 May 2026).
[34] Peoplesafe (2023) *What is Vicarious Liability?* Available at: peoplesafe.co.uk (Accessed: 2 May 2026)
[35] Garrood, K. (2017) *Piercing or peeping round the corporate veil*. Available at: applebyglobal.com (Accessed: 2 May 2026).
[36] Catania and Catania Injury Lawyers (2026) *What is Vicarious Liability?* Available at: cataniaandcatania.com (Accessed: 2 May 2026).

alongside the corporation for specific data-related offences. If a corporation commits an offence under Sections 35, 36, or 37 (such as unlawful disclosure or sale of personal data), both the corporation and every officer who knowingly and willfully authorized the act are liable. This removes the "shield" of separate legal personality that might otherwise protect directors from the consequences of the company's data breaches. **Vicarious Liability (Sections 33 & 38)**. The Act establishes a form of vicarious liability where the corporation is held strictly responsible for the actions of its employees or agents. Under Section 38(2), a court can order a convicted corporation to pay a fine of up to 2% of its annual gross turnover, regardless of which specific employee committed the breach. Section 33 allows data subjects who suffer damage or distress due to a contravention to seek compensation directly from the data collector, processor, or controller (the company), even if the harm was caused by a subordinate's actions.

2.4 Jurisdictional Challenges and Offshore Digital Lender and "Ghost" Entities

Jurisdictional challenges with offshore digital lenders stem from their ability to operate across borders without a physical presence, making it difficult for local regulators to enforce consumer protection and interest rate laws. These "borderless" operations often create a mismatch between rapid technological innovation and slower-moving regulatory frameworks[37]. And Jurisdictional challenges involving "ghost" entities such as shell companies, dormant trademarks, or untraceable digital actors create significant hurdles for legal systems by obscuring accountability and complicating the service of process. These entities often exist only on paper or in digital form, making it difficult for courts to establish personal jurisdiction or enforce judgments[38].

Key Jurisdictional challenges with "ghost" entities include **Lack of Physical Presence**: Courts traditionally obtain jurisdiction through personal service or a defendant's physical ties to a forum. Ghost entities frequently lack a "brick-and-mortar" presence, leading to disputes over whether a court has the authority to hear a case. **Global Mobility**: Ghost companies can be registered in

[37]World Bank Group (2026) *Inclusive digital financial services: defining terms and delimiting jurisdiction*. Available at: [https://digitalfinance.worldbank.org/topics/digital-credit/defining-terms-and-delimiting-jurisdiction] (Accessed: 2 May 2026)
[38] PAIGE, S. (2024) Rethinking jurisdictional maximalism in the wake of Mallory. *Fordham Law Review*. 92 (6), pp. 2725–2763.

one country, marketed in another, and linked to bank accounts in a third, creating a "tangled web" that complicates cross-border legal action[39].

The primary jurisdictional hurdles with offshore digital lenders include **Lack of Physical Nexus**: Regulators like the Uganda Microfinance Regulatory Authority typically require lenders to be incorporated locally with a physical office to be licensed. Offshore lenders bypass this by hosting platforms in foreign jurisdictions, complicating legal service and oversight[40]. **Regulatory Gaps and Ambiguity**: In many regions, financial legislation only covers deposit-taking institutions. Offshore digital lenders often fall into these gaps, as they provide credit without accepting deposits, leading some countries (like Uganda) to explicitly expand their Central Bank's authority to include all digital credit providers[41]. **Enforcement Complexity**: Even if a local court finds an offshore lender's practices illegal, enforcing that judgment across borders is difficult. Conversely, some courts have ruled that the lack of a local license does not necessarily absolve a borrower from repayment, as seen in the Supreme Court of Uganda's ruling on syndicated cross-border lending in the case of ***Ham Enterprises Ltd & 2 Others v Diamond Trust Bank (U) Ltd & Anor (Civil Appeal No. 13 of 2021) [2023] UGSC 15***.[42] The judgment, delivered on June 6, 2023, clarified that foreign lenders do not require a local license to extend credit to Ugandan borrowers, effectively protecting the validity of over $1.5 billion in cross-border syndicated loans.

[39] Prescott, J. (2026) *Ghost Collateral: The Fragile Architecture of Global Banking*. [Berlin: epubli].
[40] Uganda Microfinance Regulatory Authority (2020) *What are the Regulatory Do's and Don'ts for Money Lending?* Available at: umra.go.ug (Accessed: 2 May 2026)
[41] World Bank (2026) *Defining Terms and Delimiting Jurisdiction*. Available at: worldbank.org (Accessed: 2 May 2026).
[42]Ssemyalo, R.N. and Karugaba, P. (2026) *Licensing of foreign lenders in Uganda: much ado about nothing*. Available at: ensafrica.com (Accessed: 2 May 2026).

CHAPTER THREE: METHODOLOGY

3.0 Introduction

This chapter presents the frame work under which the data collection and analysis will be carried out. It provides the methodology used in carrying out the study in terms of research design. Data source, sample size data collection methods, data analysis and the limitations of the study.

3.1 Methodology

This study employed descriptive research design, specifically cross-sectional survey design using both the quantitative and qualitative methods of data collection. Descriptive study enables the researcher to collect information from a cross-section of a given population[43] Descriptive, cross-sectional survey research method is preferred because it accurately portraits populations or phenomena at a single point in time, using structured, non-manipulative data collection to identify trends and characteristics. A mixed-methods approach (quantitative and qualitative, open-ended questions/interviews) provides both numerical analysis and contextual, in-depth meaning, offering a comprehensive snapshot[44].

3.2 Population and Sample Size

The target population for this study comprised key stakeholders in Uganda's digital lending sector, ensuring a representative sample that reflected the diverse voices and experiences relating to data protection and privacy in Uganda. A total of 10 interviews were conducted. Interviews were conducted with purposively selected respondents from the PDPO (2), The Criminal Investigations Directorate of Uganda Police Force (1), Uganda Microfinance Regulatory Authority (1), The Judiciary (A judge who has handled a case related to data privacy related crime) (1) and Senior Staff of Digital Lending Companies (5). These included: Reach Loans Uganda Ltd, Smart Loans Uganda, Mogo Uganda, Express Loans Uganda and Premier Credit Limited.

[43]M.D. Gall, W.R. Borg and J.P. Gall, *Educational research: an introduction*, 6th edn., White Plains, NY, Longman, 1996, p. 374.
[44] J.W. Creswell and J.D. Creswell, *Research design: qualitative, quantitative, and mixed methods approaches*, 5th edn, Thousand Oaks, CA, SAGE Publications, 2018, p. 150.

3.3 Sample Selection

The study adopted purposive and snowball sampling techniques to select the sample for the study. Both purposive and snowball sampling are non-probability qualitative techniques. While these sampling methods are staples of qualitative research, they are also frequently used in quantitative and mixed-methods descriptive studies[45]. Purposive (judgmental) sampling was chosen because it enabled the researcher to hand-pick respondents who possessed specific expert knowledge necessary for the study. Snowball (chain referral) sampling was also used, whereby the researcher began with respondents from the PDPO and the Uganda Microfinance Regulatory Authority, who then guided the researcher in identifying the digital lending companies that were interviewed.

3.4 Data Collection Methods and Tools

The study employed two main data collection methods: secondary data review and semi-structured interviews. The secondary data review formed the basis of quantitative data. A review of the Data Protection and Privacy Act, Cap. 97, and its 2021 Regulations was conducted to assess protection of personal data. The analysis provided an understanding of the statutory framework and identified gaps in data privacy, criminal liabilities, and their effects. Qualitative data was collected through semi-structured interviews using In-depth Interview (IDI) and Key Informant Interview (KII) tools. These interviews were conducted with purposively selected respondents listed under 3.2.

3.5 Data Analysis

The data collected was analysed using qualitative data analysis methods. Data from the IDIs and KIIs were coded using thematic analysis, as outlined by Braun and Clarke (2006)[46]. This involved identifying recurring patterns and variations in responses. Thematic analysis allowed a deep exploration of respondents' narratives, revealing insights into their understanding of and challenges related to criminal liability in data protection and privacy. The mixed-methods approach culminated in an integrative analysis combining insights from qualitative data and secondary data review. This analysis triangulated findings, validated results, and clarified

[45] A. Moser and I. Korstjens, 'Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis', *European Journal of General Practice*, vol. 24, no. 1, 2017, p. [pp. 9-18].
[46] V. Braun and V. Clarke, 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, vol. 3, no. 2, 2006, p. 87.

intersections between criminal liability, corporate liability, and effectiveness of the DPPA in protecting personal data.

3.5 Ethical Considerations

To ensure confidentiality of respondents' information and uphold ethical standards, the following measures were implemented by the researcher:

1. **Informed Consent**: Consent was obtained from respondents before interviews and respondents were fully informed about the purpose of the study, what their participation involves, and their right to withdraw at any time without penalty. all respondents declined pictures and the researcher abided by that and no pictures were taken during interviews.
2. **Confidentiality and anonymity**: Respondents were coded instead of using their names to protect their identities. All identifying details have been removed from the report and quotes have been frames in a way that they can not be traced back to individuals or institutions. This was made known to each respondent and it gave them confidence to speak. Three respondents refused to meet the researcher face to face; they preferred phone interviews for confidentiality.
3. **Data protection and secure storage**: Collected data was stored and continues to be stored securely only the researcher has access to it. The data will not be shared with unauthorised persons. Data will be destroyed after the approval of this research work by the supervisor. Care has been taken to not to disclose internal compliance weaknesses in a away that exposes companies that accepted to over interviews unfairly. Sensitive regulatory information obtained during the interviews have not been disclosed.

3.6 Limitations of the Study

In comparative terms, the survey was based on a small sample size that may not be fully representative of all digital lending companies in the country. While this does not significantly affect the validity of the study findings, it nevertheless suggests that some issues may require further investigation to obtain a more comprehensive understanding of the situation.

Another limitation was time and resources constraint. Scheduling interviews was quite challenging, key informants were not easily available in some instances the researcher had to call a different person to speak with the targeted respondent to give the researcher time for interviews and this worked well for four interviews. Financial constraint especially logistical costs were also a challenge two meetings took place at a restaurant, and the researcher paid the bills.

CHAPTER FOUR
PRESENTATION, ANALYSIS AND INTERPRETATION OF FINDINGS

4.0 Introduction

This study examined the effectiveness of Sections 35 to 39 of the Data protection and Privacy Act, Cap 97 regarding individual and corporate criminal liability; enforcement practicality through investigating the challenges the Personal Data Protection Office (PDPO) faces in prosecuting lenders; the sanctions (the fine and the threat of 10 years' imprisonment) and examine whether these effectively deters lenders from using personal data of their borrowers and drew a comparative analysis of criminal liability in Uganda's Data Protection and Privacy law and reformed administrative model in the EU's GDPR. This chapter presents the analysis of findings under each of the areas examined under this study.

4.1 Effectiveness of Sections 35 to 39 of the Data Protection and Privacy Act (DPPA), Cap. 97 in Regulating Criminal Liability.

The Data Protection and Privacy Act, Cap. 97 was enacted to operationalise the constitutional right to privacy under Article 27 of the 1995 Constitution, which protects individuals against unlawful interference with correspondence, communication, and personal data processing. Within this framework, criminal liability is primarily established under Part VIII (Offences), particularly: **Section 35** – unlawful obtaining or disclosure of personal data and **Section 39** – regulatory powers (Ministerial regulations supporting enforcement framework). Although Section 39 is not an offence-creating provision, it plays a structural enforcement role by enabling implementation mechanisms that indirectly affect criminal liability.

Strengths of Sections 35 to 39 in Regulating Criminal Liability

Section 35 provides clear criminalisation of core privacy violations. *Section 35(1)* prohibits unlawful obtaining of personal data, unlawful disclosure, and procuring disclosure of personal data. This aligns directly with the constitutional right to privacy under *Article 27* of the Constitution by criminalising conduct that interferes with informational privacy[47]. In this sense, the provision elevates data protection from a primarily civil and administrative obligation into a

[47] The 1995 Constitution of the Republic of Uganda (as amended), art 27.

criminally enforceable legal norm, thereby strengthening deterrence against unlawful data practices. The law further provides that a breach constitutes a criminal offence punishable by up to 10 years imprisonment, a fine, or both, reflecting the seriousness with which the law treats violations of personal data privacy[48].

Another strength of *Section 35* in regulating criminal liability is its broad applicability. It applies to individuals, data controllers, data processors, and data collectors[49]. This wide scope ensures that liability is not confined to corporate entities alone but extends to individuals (Directors and Managers of a company) involved in unlawful processing activities. In doing so, it reduces regulatory loopholes that may arise where responsibility is dispersed within organisational structures, thereby strengthening overall protection of personal data and privacy rights.

The law further enhances corporate liability. Under *Section 38*, offences committed under *Section 35* may extend to corporate bodies as well as Directors and Managers where the offence is committed with their consent, connivance, or attributable to their neglect[50]. This statutory attribution of liability strengthens accountability at institutional level by preventing corporations from shielding culpable decision-makers behind the corporate veil.

Section 39 complements this criminal liability framework by empowering the Minister to make regulations for the implementation of the Act, including procedural and administrative enforcement rules.[51] Although it does not itself create offences, it supports the legal infrastructure necessary for enforcement of offences under *Section 35*. In practical terms, Section 39 operationalises enforcement by enabling licensing and registration frameworks for data controllers, establishing procedural compliance requirements, and providing regulatory guidance for enforcement authorities. Without such regulations, the effective enforcement of Section 35 would be significantly constrained.

Section 39 also introduces flexibility into the regulatory framework. Given that data-related offences and risks evolve rapidly alongside technological change, it allows the Minister to adapt

[48] Data Protection and Privacy Act, Cap 97 s 35
[49] ibid
[50] Data Protection and Privacy Act, Cap 97 s 38.
[51] Data Protection and Privacy Act, Cap 97 s 39.

enforcement mechanisms without the need to amend the primary legislation.[52] This enhances the responsiveness of the legal regime and ensures that data protection law remains adaptable to emerging digital risks. Notwithstanding its strengths, Section 39 also raises concerns relating to broad regulatory discretion. Such discretion may result in inconsistent enforcement standards and may create regulatory uncertainty for compliance actors, particularly where regulations evolve unevenly or lack clear implementation consistency.

Limitations of Section 35 and 39 Regulating Criminal Liability.

Despite the strong statutory framework established under *Sections 35 and 39*, the effectiveness of the law in regulating criminal liability in practice is still emerging. Enforcement of data protection offences depends heavily on institutional capacity, particularly the Personal Data Protection Office (PDPO) established under the Act and investigative agencies such as The Criminal Investigations Directorate (CID) and the Office of the Director of Public Prosecution (ODPP) who are responsible for evidence gathering and prosecution. This law came into effect in 2019 and the first criminal conviction under the Act was in 2025 suggesting low enforcement intensity hence limiting the deterrent effect of the law. ***The researcher raised this finding from secondary data review in the interviews with the PDPO and CID, the respondents in those agencies agreed there are challenges with enforcement capacity and added that it is still developing*.**

Practical enforcement faces technical and evidentiary challenges, including attribution of digital conduct, cross-border data flows, and the complexity of proving unlawful access or disclosure beyond reasonable doubt as required under *Section 35*. These challenges can make prosecution of data-related offences difficult even where statutory provisions are clear. As a result, while the legal framework is robust in design, its operational effectiveness depends on the development of investigative expertise, regulatory coordination, and sustained enforcement practice.

Sections 35 and 39 can be assessed as strong in normative design but still consolidating in practical enforcement, with their full effectiveness contingent on institutional capacity of the PDPO, CID and ODPP and consistent application in Uganda's evolving digital regulatory environment.

[52] ibid

4.2 Assessment of the Practical Challenges of the Personal Data Protection Office (PDPO) in Prosecuting Digital Lenders.

The digital lending sector in Uganda is rapidly expanding, resulting in increased risks to the protection and privacy of personal data, particularly through unlawful data processing, intrusive debt collection practices, and non-compliance with regulatory requirements under the Data Protection and Privacy Act, Cap. 97.

The Personal Data Protection Office (PDPO) faces significant challenges in investigating and prosecuting digital lenders. These include institutional, technological, evidentiary, and regulatory challenges. PDPO staff interviewed identified **the widespread operation of unlicensed and unregistered digital lenders** as a major practical challenge. This finding aligns with information from the Uganda Microfinance Regulatory Authority (UMRA). During a Key Informant Interview (KII) with a staff member of UMRA, the official reported that numerous online loan applications operate in contravention of the Tier 4 Microfinance Institutions and Money Lenders Act, 2016 and the Tier 4 Digital Lending Guidelines, 2024. The official stated that these entities "mostly employ mobile applications and social media platforms to lure the public into borrowing from them," and further noted that their activities constitute "an abuse of customer data privacy."

PDPO staff interviewed reported that many digital lenders operate anonymously, frequently change application names, or rely on cross-border digital infrastructure, **making identification and attribution of criminal conduct difficult**. This undermines enforcement because prosecution under *Sections 35 and 38* of the Act requires proof linking unlawful processing to identifiable person or corporate entities. In *Ssekamwa Frank & Others v Google LLC*[53], the respondent argued that compliance obligations arise only where there is a physical presence in Uganda. However, the regulatory position is that foreign digital service providers targeting users in Uganda must comply with local data protection obligations or face sanctions for non-compliance.

Another major challenge relates to **unlawful data collection and excessive access permissions by digital lenders**. Officials at the PDPO revealed that many lending applications request access

[53] Ssekamwa Frank and 3 others v Google LLC (Complaint No. 08/11/24/6683) [2025] PDPO 2 (18 July 2025)

to borrowers' contacts, galleries, and other personal information beyond what is reasonably necessary for loan processing. A member of staff at the PDPO stated that "money lending apps are asking for too much data" and noted that many borrowers are unaware of their rights and the repercussions of granting broad permissions. This creates enforcement difficulties because borrowers often technically consent to data processing during application installation, even where such consent is not fully informed, freely given, or specific as required by the Act.

The prosecution of digital lenders also presents significant **evidentiary and technological challenges**. Digital evidence is often stored electronically, transmitted across multiple jurisdictions, or controlled through third-party platforms and cloud-based systems. Establishing the origin of unlawful disclosures, tracing communications, and preserving electronic evidence in a manner admissible in court requires advanced digital forensic capacity and inter-agency coordination. These challenges place pressure on the PDPO, which often relies on collaboration with the Criminal Investigations Directorate (CID) and the Office of the Director of Public Prosecutions (ODPP) during investigations and prosecutions.

Another challenge concerns **public awareness and borrower vulnerability**. Many individuals who utilise digital lending applications are financially vulnerable and may prioritise immediate access to credit over privacy concerns.

In conclusion, although the PDPO has shown increasing willingness to investigate and prosecute unlawful practices in the digital lending sector, its effectiveness remains constrained by technological complexity, evidentiary burdens, low public awareness, institutional capacity limitations, and the rapidly evolving nature of digital lending platforms. While the Data Protection and Privacy Act provides a strong basis for criminal liability, sustained enforcement will require strengthening institutional capacity, improving inter-agency coordination, enhancing public awareness, and ensuring consistent prosecution of non-compliant digital lenders.

4.3 Assessment of Sanctions (Fines and Potential 10-Year Imprisonment) and Their Effectiveness in Deterring the Misuse of Borrowers' Personal Data by Lenders.

The Data Protection and Privacy Act, Cap. 97 establishes criminal liability for unlawful handling of personal data under ***Section 35, 36, 37 and 38***. Under *Section 35,* a person who unlawfully

obtains, discloses, or procures disclosure of personal data is liable upon conviction to a fine not exceeding 240 currency points or imprisonment not exceeding 10 years, or both. Similar penalties apply under *Sections 36 and 37* for unlawful destruction or sale of personal data. *Section 38* further extends liability to corporate actors, holding companies and responsible officers criminally accountable where offences are committed in a corporate context. These provisions are designed to create both individual and corporate deterrence, particularly relevant in sectors such as digital lending, where large-scale automated processing of personal data is routine.

Effectiveness of Sanctions in Deterring the Misuse of Borrowers' Personal Data by Lenders

In 2025, the Personal Data Protection Office (PDPO) secured its first criminal conviction under the Act, involving unlawful processing of borrowers' personal data through a digital lending application ("Quickloan"). The offender was fined UGX 300,000 following prosecution in collaboration with the CID and the Office of the Director of Public Prosecution.

This case has had a significant regulatory and behavioural impact on digital lenders in Uganda. In an interview with a senior staff member at Reach Loans Uganda Ltd, who requested anonymity, it was clear that the sanctions have had a deterrent effect on digital lenders. The respondent narrated that prior to the conviction of the Director of Quickloan, many fintech and digital lenders operated under the assumption that app-based lending was lightly regulated and that enforcement was weak or unlikely in practice. The conviction of the Director of Quickloan changed that perception by confirming that digital lending is fully subject to data protection law and attract criminal liability in cases of non-compliance. The respondent further noted that following the conviction, many companies rushed to register with PDPO. This observation was corroborated by the PDPO, which reported an increase in the registration of digital lending companies following the conviction.

Smart Loans Uganda and Express Loans Uganda reported that following the enactment of the DPPA, the PDPO intensified its crackdown on shaming tactics used by digital lenders in debt collection. The respondents explained that a common practice in Uganda's digital lending sector involved contacting borrowers' relatives and friends, sending threatening messages, and using edited images and videos to shame defaulters. They further reported that after the conviction of

the Director of Quickloan, digital lenders became more aware that such conduct amounts to unlawful processing of personal data. As a result, firms began instructing staff to avoid such tactics in order to prevent legal sanctions and enforcement action. It was further observed that lenders have become more cautious, recognising that even in cases of borrower default, debt enforcement must comply with the law. The PDPO reported that following the ruling, it warned lenders that violations of privacy rights would be prosecuted rather than merely mediated.

Mogo Uganda and Premier Credit Limited reported that there is increasing compliance pressure on fintech and digital lenders. The respondents stated that they now receive visits from officials of the PDPO, which has placed pressure on them to ensure compliance with the law. They further reported that digital lenders now face higher operational expectations. The respondent from Premier Credit Limited explained that the company has made adjustments to its operational systems, including ensuring that consent is explicit and documented, limiting the use of borrowers' personal data to loan processing purposes, and training staff on internal compliance policies, including cross-border data handling. The respondent further noted that the company has reduced aggressive mobile data access permissions and contact scraping practices previously used for repayment enforcement, and now employs alternative approaches. However, when asked by the researcher to specify those approaches, the respondent declined to provide further details.

Limitations of Sanctions in Deterring the Misuse of Borrowers' Personal Data by Lenders

Although the conviction of the Director Quickloan represented a landmark step in the enforcement of data protection law, the relatively low monetary penalty of UGX 300,000 raises concerns about whether the sanctions available under the Act are sufficiently punitive to discourage unlawful conduct by digital lenders. Experts have argued that the fine appears disproportionately low when compared to the scale and profitability of many digital lending operations and this weakens the punitive and deterrent purpose of sanctions under the DPPA. The low sanction may also undermine the principle of general deterrence. General deterrence operates on the assumption that penalties imposed on one offender will discourage similar conduct by others within the industry. However, where sanctions are minimal, other digital lenders may conclude that even if they are prosecuted, the financial consequences are manageable and commercially tolerable. As a result, some companies may continue engaging in

unlawful practices such as contact scraping, public shaming of borrowers, and unauthorised sharing of personal data because the economic benefits of such practices outweigh the legal risks. However, despite the low fine, the case still produced some deterrent effect because of its symbolic and precedential value. It was the first criminal conviction under the DPPA and demonstrated that the PDPO, CID, and DPP are willing to investigate and prosecute digital lender.

4.4 Comparative Analysis of Criminal Liability under Uganda's Data Protection and Privacy Act and Administrative Enforcement under the EU General Data Protection Regulation (GDPR).

The regulatory approaches adopted by Uganda and the European Union (EU) in the field of data protection reflect two distinct enforcement philosophies. Uganda's approach relies on criminal liability for unlawful acts involving personal data, whereas the EU primarily adopts an administrative enforcement regime under the General Data Protection Regulation (GDPR). Although both systems aim to safeguard the right to privacy and ensure the lawful processing of personal data, they differ significantly in enforcement design, institutional mechanisms, and deterrence strategy.

Uganda's Criminal Liability-Centred Enforcement Approach

Uganda's Data Protection and Privacy Act, 2019 establishes a hybrid enforcement framework that includes both administrative oversight by the Personal Data Protection Office (PDPO) and criminal sanctions for specific offences. Under the Act, unlawful processing of personal data, obstruction of lawful data protection functions, and other violations may attract criminal penalties, including fines and imprisonment. This reflects a more traditional regulatory approach in which serious violations of privacy obligations are treated not only as regulatory breaches but as offences against the state. The involvement of criminal law elevates the seriousness of non-compliance and is intended to deter deliberate misconduct, particularly in contexts where data misuse may result in harm such as identity theft, fraud, or unauthorized disclosure.

However, enforcement in practice faces structural challenges. For example, in cases involving digital lending applications operating without clear physical presence or frequently changing digital identities, regulators struggle to identify the natural or legal persons responsible for

unlawful processing. This complicates the attribution required for criminal prosecution, which generally demands proof beyond reasonable doubt linking the offence to a specific accused person or entity. As a result, although criminal liability exists on paper, its practical effectiveness depends heavily on investigative capacity, cross-border cooperation, and digital traceability.

EU GDPR: Administrative Enforcement Model

In contrast, the EU GDPR adopts a predominantly administrative enforcement system, implemented through national Data Protection Authorities (DPAs) across Member States. Rather than relying on criminal courts as the primary enforcement mechanism, the GDPR empowers supervisory authorities to impose a wide range of corrective measures and administrative fines.

These measures include: warnings and reprimands, orders to comply or cease processing, temporary or permanent bans on processing, and significant administrative fines depending on the severity of the infringement.

A key example of GDPR enforcement is the action taken by several European DPAs against large technology companies for violations relating to transparency and consent requirements. In such cases, regulators have imposed substantial administrative fines and required changes to data practices without necessarily resorting to criminal prosecution. Importantly, the GDPR allows Member States discretion to introduce criminal penalties in their domestic laws, but the regulation itself does not rely on criminal liability as its primary enforcement tool. Instead, it prioritizes regulatory supervision, rapid corrective action, and compliance-oriented enforcement.

Key Points of Divergence

The Ugandan approach and the EU system diverge in three main respects as analysed below:

(a) Nature of enforcement: Uganda incorporates criminal sanctions as a core enforcement mechanism, whereas the GDPR relies mainly on administrative sanctions.

(b) Threshold for liability: Criminal liability under Uganda's framework generally requires proof of unlawful conduct meeting criminal standards, making enforcement more procedurally demanding. The GDPR's administrative model allows regulators to act on a lower threshold of proof, enabling faster intervention.

(c) Enforcement objectives: Uganda's model emphasizes punishment and deterrence through criminal law, while the GDPR emphasizes compliance correction and regulatory control through supervisory authorities.

Convergence and practical implications

Despite their differences, both systems share a common objective: ensuring lawful, fair, and transparent processing of personal data. In practice, the GDPR's administrative model has proven particularly effective in addressing large-scale or systemic violations, especially in the digital economy where speed of enforcement is critical.

Uganda's approach, while potentially stronger in signaling seriousness through criminal penalties, may face limitations where offenders operate across borders or where evidentiary challenges hinder prosecution. This is particularly relevant in emerging digital markets where service providers may lack clear jurisdictional anchoring.

In conclusion, the comparison reveals two distinct regulatory philosophies. Uganda's Data Protection and Privacy Act integrates criminal liability as a deterrent mechanism, reflecting a more punitive enforcement orientation. The EU GDPR, by contrast, adopts an administrative enforcement model that prioritizes regulatory efficiency and compliance management over criminal sanctioning.

Both approaches have strengths and limitations. The effectiveness of Uganda's model depends significantly on enforcement capacity and investigative reach, while the GDPR's model depends on strong institutional regulators and consistent application of administrative powers. Together, they illustrate the broader global tension between criminalisation and administrative regulation in modern data protection law.

CHAPTER FIVE: CONCLUSIONS AND RECOMMEDNATIONS

5.0 Conclusions

This study assessed the effectiveness of Sections 35 to 39 of the Data Protection and Privacy Act, Cap 97 in regulating criminal liability within Uganda's digital lending sector, the enforcement challenges faced by the Personal Data Protection Office (PDPO), the deterrent effect of sanctions, and a comparative analysis with the EU GDPR framework. The following conclusions are drawn from the findings.

First, the study concludes that Sections 35 to 39 of the Data Protection and Privacy Act provide a **legally strong and normatively clear framework for criminal liability in data protection**. Section 35 clearly criminalises unlawful obtaining, disclosure, and processing of personal data, while Section 38 extends liability to corporate officers, effectively piercing the corporate veil. Section 39 strengthens enforcement through regulatory empowerment, ensuring that the legal framework remains adaptable to technological developments. Collectively, these provisions establish a comprehensive statutory basis for criminal accountability in data protection.

Second, despite the strength of the legal framework, the study concludes that **practical enforcement remains limited and still developing**. Evidence from both institutional interviews and secondary sources shows that enforcement is constrained by low prosecution intensity, technical complexity, and evidentiary challenges. The gap between legal design and enforcement reality weakens the overall deterrent effect of the Act, particularly in fast-evolving sectors such as digital lending.

Third, the study concludes that the Personal Data Protection Office (PDPO) plays a **central but constrained enforcement role**. While the PDPO has demonstrated increasing regulatory activity, including collaboration with CID and ODPP and securing the landmark conviction in *Uganda v Mugulusi Ronald (2025),* it continues to face significant challenges. These include difficulty in identifying anonymous or offshore digital lenders, limited digital forensic capacity, and reliance on inter-agency cooperation for prosecution.

Fourth, the study concludes that **digital lenders in Uganda continue to engage in unlawful data processing practices**, including contact scraping, unauthorized data sharing, and borrower shaming. These practices persist despite the existence of criminal sanctions, largely due to enforcement gaps, limited awareness among borrowers, and the historical perception of weak regulatory oversight in the sector.

Fifth, the study finds that the sanctions under the Act, including fines and imprisonment of up to ten years, have a **mixed deterrent effect**. The landmark conviction of 2025 has had a strong symbolic and behavioural impact, prompting increased compliance, registration with PDPO, and reduction of overtly abusive practices. However, the relatively low monetary penalties imposed in practice weaken the perceived severity of enforcement and may reduce long-term deterrence.

Sixth, the comparative analysis concludes that Uganda's enforcement model is **more punitive but less administratively efficient** compared to the EU GDPR framework. While Uganda relies on criminal liability to enforce compliance, the GDPR prioritises administrative sanctions, corrective supervision, and regulatory intervention. The EU model demonstrates greater flexibility and faster compliance correction, whereas Uganda's model depends heavily on investigative and prosecutorial capacity.

Finally, the study concludes that the digital lending sector in Uganda operates within a **structural privacy-credit imbalance**, where borrowers exchange extensive personal data for access to credit without meaningful understanding or control. This imbalance continues to expose borrowers to privacy risks despite the existence of legal safeguards under Cap 97.

5.1 Recommendations

Based on the findings and conclusions of this study, the following recommendations are made:

Finding 1: Weak enforcement capacity of PDPO, CID, and ODPP limits effective implementation of Sections 35–39 of the DPPA.

Recommendation:

The Government should strengthen the institutional and technical capacity of the PDPO, CID, and ODPP through increased funding, investment in digital forensic infrastructure, recruitment of specialised cyber and digital forensic experts, and continuous training for investigators and prosecutors handling data protection offences. This recommendation is founded on the findings under section 4.1 and 4.2 which revealed that enforcement is constrained by technological complexity, evidentiary burdens and limited institutional capacity, resulting in low prosecution intensity.

Finding 2: Digital lenders are difficult to trace and prosecute due to anonymity, cross-border operations, and rapidly changing digital identities.

Recommendation:

Regulators should enhance inter-agency coordination between PDPO, CID, UMRA, and telecommunications regulators, establish a joint compliance and monitoring framework and formal cross-border cooperation mechanisms to facilitate identification, tracking, and prosecution of unlicenced digital lending platforms operating online and offshore. This recommendation is based on findings in section 4.2 which revealed that lenders frequently use anonymous structures and foreign infrastructure to evade regulatory oversight.

Finding 3: Many digital lending applications operate without proper licensing and regulatory approval.

Recommendation:

UMRA and NITA-U should partner directly with Google and Apple to enforce strict app-store screening, where by the tech giants must require developers targeting the Ugandan market to upload both a valid UMRA license and a PDPO registration certificate before any financial app can be published on the Play Store or App Store, while simultaneously restricting mobile money gateways, blocking intrusive device APIs, and mandating local corporate agents to eradicate

unregulated digital lending. This recommendation is grounded in section 4.2 findings which show widespread operation of unregistered and unregulated digital lending platforms.

Finding 4: Digital lenders frequently collect excessive personal data beyond what is necessary for loan processing.

Recommendation:

Regulators should develop strict guidelines limiting the type and scope of personal data that digital lenders can access particularly restricting access to contacts, photos, and unrelated device data. In addition, standardised consent forms should be introduced to ensure that users clearly understand what data is being collected and for what purpose. This recommendation is based on findings in section 4.2 which revealed excessive data harvesting practices by digital lending applications.

Finding 5: Borrowers often give consent without fully understanding the implications of data sharing.

Recommendation:

The PDPO should implement nationwide public awareness campaigns on digital data protection rights, targeting users of digital lending platforms. These campaigns should focus on improving understanding of consent, data rights, and risks associated with unrestricted data access. This recommendation arises from section 4.2 findings which show that borrower vulnerability and low awareness significantly undermine effective enforcement of consent requirements.

Finding 6: Jurisdictional and Technical Barriers to Data Enforcement.

Recommendation:

UMRA and NITA-U must partner directly with Google and Apple to mandate local data localization hosting compliance, while utilizing international mutual legal assistance treaties and AI-driven Regulatory Technology tools to monitor offshore cloud networks and criminally target extraterritorial operators. This recommendation is based on section 4.2 findings which identified cross-border data flows, cloud storage systems, and technical complexity as major enforcement barriers.

Finding 7: The first conviction created deterrence, but the fine imposed was very low.

Recommendation:

Parliament should review the sanctions framework under Sections 35–38 of the DPPA to ensure that penalties are proportionate to the economic benefits derived from unlawful processing of personal data, including higher fines linked to company turnover or profits derived from unlawful data processing, especially for corporate offenders. This recommendation is based on section 4.3 findings which show that low financial penalties weaken general deterrence.

Finding 8: Criminal sanctions alone are insufficient to ensure timely and effective enforcement against digital lenders.

Recommendation:

The Ministry of Justice and Constitutional Affairs should initiate amendment of the DPPA to grant the PDPO expanded powers to issue immediate, direct administrative financial penalties, while codifying a mandatory co-regulatory mechanism with telecom providers and global app stores to instantly sever a non-compliant platform's operational infrastructure. This recommendation is grounded in section 4.3 and 4.4 findings which highlight the limitations of relying solely on criminal liability compared to administrative enforcement systems like the GDPR.

Finding 9: Enforcement actions, especially the conviction of the Director of Quickloan, has led to improved compliance and behavioural change among digital lenders.

Recommendation:

To capitalize on both the symbolic and practical deterrent effects of regulatory oversight, the PDPO and UMRA must institutionalize a policy of public naming-and-shaming by widely publishing high-profile enforcement decisions and structural compliance audits, thereby establishing a strong industry-wide legal precedent while physically disabling the digital infrastructure of rogue platforms. This recommendation is based on section 4.3 findings which show that enforcement actions have both symbolic and practical deterrent effects.

Finding 10: Section 39 of the DPPA grants broad regulatory discretion, which may lead to inconsistent enforcement and legal uncertainty.

Recommendation:

Regulations under Section 39 should be developed through inclusive multi-stakeholder consultation involving PDPO, industry actors, civil society, and legal experts, and should be accompanied by clear enforcement guidelines to ensure consistency, transparency, and predictability. This recommendation is based on section 4.1 findings which highlight concerns about regulatory discretion and implementation inconsistency.

Finding 11: Uganda's reliance on criminal liability makes enforcement slower and more difficult compared to administrative enforcement models like the EU GDPR.

Recommendation:

Uganda should adopt a hybrid enforcement model that strengthens administrative enforcement mechanisms similar to those employed under the GDPR while retaining criminal sanctions for serious violations. This would allow faster regulatory action while maintaining criminal deterrence for severe offences. This recommendation is based on section 4.4 findings which show that administrative enforcement (as in the GDPR) is more efficient and responsive than purely criminal enforcement systems.

BIBLIOGRAPHY

Ross, Jeremy. "What is Data Protection and Privacy?" Cloudian. 2023. Accessed January 30, 2026. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/.

Seynhaeve, Jeroen. "The Ethics of Data Privacy." PhD diss., Stellenbosch University, 2022. https://philarchive.org/rec/SEYTEO-3.

Kosinski, Matthew, and Amber Forrest. "What Is Data Privacy?" IBM. 2024. Accessed February 2, 2026. https://www.ibm.com/think/topics/data-privacy.

Zervos, A. and Belke, M., 'The development of data protection - from the GDPR to global standards', *2B Advice* [online], 29 January 2025, https://2b-advice.com/en/2025/01/29/the-development-of-data-protection-from-the-gdpr-to-global-standards/ (accessed 2 February 2026).
Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1.

Reding, V., 'The European data protection framework for the twenty-first century', *International Data Privacy Law*, vol. 2, no. 3, 2012, pp. 119–129, oup.com (accessed 5 February 2026).

Mbuga, P. and Muhawe, R., 'Data Protection Laws of the World: Uganda', *DLA Piper* [online], 2020, https://www.dlapiperdataprotection.com/index.html?t=law&c=UG (accessed 6 February 2026).

Kizito, C. and Lule, A., 'Uganda's Personal Data Protection Office is getting serious: are you ready?', *Cliffe Dekker Hofmeyr* [online], 24 May 2024, cliffedekkerhofmeyr.com (accessed 29 January 2026).

Kukunda, L., 'The dubious practices of digital money lenders', *D+C Development and Cooperation* [online], 26 August 2024, https://www.dandc.eu/en/article/customers-complain-about-dubious-methods-used-money-lending-apps-claim-their-money-back (accessed 6 February 2026).

Uganda Bankers Association, 'Series II Digital Lending Article: The Supply-side, the Supporting Functions and the Regulatory Environment' [online], 2024, 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 13 April 2026).

de Hert, P. and G. Boulet, 'The co-existence of administrative and criminal law approaches to data protection wrongs', in D. Wright and P. De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Switzerland, Springer, 2016, pp. 357–394.

Nath, S. (2021) *Is There Criminal Liability Under GDPR? Section 170 Data Protection Act 2018*. Available at: https://www.nathsolicitors.co.uk/2021/03/05/is-there-criminal-liability-under-gdpr-section-170-data-protection-act-2018/ (Accessed: 2 May 2026).

Katugugu, E. (2019) *Legal Alert: The Data Protection and Privacy Act is here*. Available at: https://www.pwc.com/ug/en/assets/pdf/legal-alert-data-protection-and-privacy-act.pdf (Accessed: 2 May 2026).

CyberLaws (Uganda) (2026) Available at: file:///C:/Users/hp/Desktop/Cyber%20laws.pdf (Accessed: 2 May 2026).

Ombija, S. and Chege, P. (2024) 'Time to take data privacy concerns seriously in digital lending', *Bowmans*, 14 May. Available at: bowmanslaw.com (Accessed: 2 May 2026).

World Bank Group (2026) *Inclusive Digital Financial Services: Data Privacy*. Available at: [https://digitalfinance.worldbank.org/topics/digital-credit/data-privacy] (Accessed: 2 May 2026).

Peoplesafe (2023) *What is Vicarious Liability?* Available at: peoplesafe.co.uk (Accessed: 2 May 2026)

Garrood, K. (2017) *Piercing or peeping round the corporate veil*. Available at: applebyglobal.com (Accessed: 2 May 2026).

Catania and Catania Injury Lawyers (2026) *What is Vicarious Liability?*. Available at: cataniaandcatania.com (Accessed: 2 May 2026).

PAIGE, S. (2024) Rethinking jurisdictional maximalism in the wake of Mallory. *Fordham Law Review*. 92 (6), pp. 2725–2763.

World Bank Group (2026) *Inclusive digital financial services: defining terms and delimiting jurisdiction*. Available at: [https://digitalfinance.worldbank.org/topics/digital-credit/defining-terms-and-delimiting-jurisdiction] (Accessed: 2 May 2026)

Prescott, J. (2026) *Ghost Collateral: The Fragile Architecture of Global Banking*. [Berlin: epubli]

Uganda Microfinance Regulatory Authority (2020) *What are the Regulatory Do's and Don'ts for Money Lending?* Available at: umra.go.ug (Accessed: 2 May 2026).

World Bank (2026) *Defining Terms and Delimiting Jurisdiction*. Available at: worldbank.org (Accessed: 2 May 2026).

Ssemyalo, R.N. and Karugaba, P. (2026) *Licensing of foreign lenders in Uganda: much ado about nothing*. Available at: ensafrica.com (Accessed: 2 May 2026).

Gall, M.D., Borg, W.R. and Gall, J.P. (1996) *Educational research: an introduction*. 6th edn. White Plains, NY: Longman

Creswell, J.W. and Creswell, J.D. (2018) *Research design: qualitative, quantitative, and mixed methods approaches*. 5th edn. Thousand Oaks, CA: SAGE Publications.

Moser, A. and Korstjens, I. (2017) 'Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis', *European Journal of General Practice*, 24(1), pp. 9–18. doi: 10.1080/13814788.2017.1375091.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi: 10.1191/1478088706qp063oa.

APPENDICES

Appendix I: Interview Guide for Officials of the Personal Data Protection Office (PDPO)

Introduction

Thank you for giving me your time, my name is Oyua Chris Charles, I am a fourth year Law Student at Makerere University. As part of the fulfilment of requirements for the Award of the Degree of Bachelor of Laws of Makerere University, I am conducting a study titled: ***"An Assessment of the Effectiveness of Criminal Liability under the Data Protection and Privacy Act, Cap. 97 in Regulating the Use of Borrowers' Personal Data by Digital Lenders in Uganda."***

The purpose of this interview is to obtain information regarding the enforcement of the Data Protection and Privacy Act, particularly in relation to digital lenders. The information provided will be treated confidentially and used solely for academic purposes. Your participation is voluntary. You may decline to answer any question or withdraw from the interview at any time without any adverse consequences. Do you have any questions before I start?

Interview Questions

1. Could you briefly explain the mandate of the PDPO under the Data Protection and Privacy Act, and how Sections 35–39 of the Act support enforcement of data protection obligations, particularly in relation to digital lenders?
2. In your view, how effective has the criminal liability framework under the Act been in promoting compliance among digital lenders, and to what extent do existing penalties deter misuse of borrowers' personal data?
3. What practical, investigative, and evidentiary challenges does the PDPO face when identifying and investigating digital lenders suspected of unlawfully processing personal data?
4. What challenges arise when dealing with digital lenders operating through foreign-based platforms or cross-border digital infrastructure, and how effective is cooperation between PDPO and other institutions such as CID, ODPP, UMRA, and telecommunications providers?
5. What impact, if any, has the first criminal conviction under the Data Protection and Privacy Act had on compliance among digital lenders, and what reforms would you recommend to strengthen enforcement of the Act?
6. Are there any additional observations you would like to share?

Appendix 2: Interview Guide for CID Officers

Introduction

Thank you for giving me your time, my name is Oyua Chris Charles, I am a fourth year Law Student at Makerere University. As part of the fulfilment of requirements for the Award of the Degree of Bachelor of Laws of Makerere University, I am conducting a study titled: ***"An Assessment of the Effectiveness of Criminal Liability under the Data Protection and Privacy Act, Cap. 97 in Regulating the Use of Borrowers' Personal Data by Digital Lenders in Uganda."***

The purpose of this interview is to obtain information regarding the enforcement of the Data Protection and Privacy Act, particularly in relation to digital lenders. The information provided will be treated confidentially and used solely for academic purposes. Your participation is voluntary. You may decline to answer any question or withdraw from the interview at any time without any adverse consequences. Do you have any questions before I start?

Interview Questions

1. Based on your experience, what types of complaints involving misuse of borrowers' personal data by digital lenders are most frequently reported to CID?
2. What practical challenges do CID investigators encounter when investigating alleged violations of the Data Protection and Privacy Act, and how are suspects identified and linked to unlawful processing of personal data?
3. What evidentiary and technical challenges are commonly encountered when collecting, preserving, and presenting digital evidence in data protection cases, and are existing digital forensic resources sufficient for effective investigations?
4. What challenges arise when investigating digital lenders operating through foreign-based platforms or cross-border digital infrastructure, and how effective is cooperation between CID and other institutions such as PDPO, ODPP, UMRA, and telecommunications providers?
5. What lessons, if any, has CID learned from the first conviction under the Data Protection and Privacy Act regarding investigation of digital lending cases, and what reforms would you recommend to strengthen enforcement of data protection offences?

Appendix 3: Interview Guide for UMRA Officials

Introduction

Thank you for giving me your time, my name is Oyua Chris Charles, I am a fourth year Law Student at Makerere University. As part of the fulfilment of requirements for the Award of the Degree of Bachelor of Laws of Makerere University, I am conducting a study titled: ***"An Assessment of the Effectiveness of Criminal Liability under the Data Protection and Privacy Act, Cap. 97 in Regulating the Use of Borrowers' Personal Data by Digital Lenders in Uganda."***

The purpose of this interview is to obtain information regarding the enforcement of the Data Protection and Privacy Act, particularly in relation to digital lenders. The information provided will be treated confidentially and used solely for academic purposes. Your participation is voluntary. You may decline to answer any question or withdraw from the interview at any time without any adverse consequences. Do you have any questions before I start?

Interview Questions

1. How would you describe the current digital lending landscape in Uganda, and how do digital lenders comply with licensing and operational requirements under the applicable legal and regulatory framework?
2. What challenges does UMRA face in overseeing digital lenders in Uganda, and how significant is the problem of unlicensed or unregistered digital lenders?
3. What complaints or concerns has UMRA encountered regarding the use of borrowers' personal data and debt recovery practices by digital lenders?
4. In practice, how effective are the existing laws and regulatory measures, and how effective is UMRA's cooperation with other institutions such as the PDPO, CID, and other relevant agencies in addressing unlawful practices by digital lenders?
5. What challenges does UMRA face in regulating digital lenders operating from outside Uganda, and what reforms would you recommend to strengthen oversight and protection of borrowers' personal data? Are there any additional observations you would like to share?

Appendix 4: Interview Guide for Digital Lenders

This interview schedule was used with respondents from:

- Reach Loans Uganda Ltd
- Smart Loans Uganda
- Express Loans Uganda
- Mogo Uganda
- Premier Credit Limited

Introduction

Thank you for agreeing to participate in this study. My name is Oyua Chris Charles, a fourth-year Law Student at Makerere University. As part of the fulfilment of the requirements for the Award of the Degree of Bachelor of Laws of Makerere University, I am conducting a study titled: **"An Assessment of the Effectiveness of Criminal Liability under the Data Protection and Privacy Act, Cap. 97 in Regulating the Use of Borrowers' Personal Data by Digital Lenders in Uganda."** The purpose of this interview is to obtain information regarding compliance with, and enforcement of, the Data Protection and Privacy Act in relation to digital lending practices in Uganda. The information provided will be treated confidentially and used solely for academic purposes. Your participation is voluntary. You are free to decline to answer any question or withdraw from the interview at any time without any penalty or adverse consequences.

Do you have any questions before I begin?

Interview Questions

1. How does your company obtain and document borrowers' consent for the collection and use of their personal data?
2. What internal measures does your company have in place to ensure compliance with the Data Protection and Privacy Act, and what challenges do you face in implementing these requirements?
3. How does your company conduct debt recovery in cases of default, and what types of borrower information are used in the process?
4. What changes, if any, has your company made to its data handling and debt recovery practices following enforcement of the Data Protection and Privacy Act, particularly after the conviction of the Director of Quick Loan?
5. In your view, how effective are the sanctions under the Data Protection and Privacy Act in influencing compliance among digital lenders, and what improvements would you suggest to the current regulatory framework?
6. Are there any additional comments you would like to make regarding digital lending and the use of borrowers' personal data?