AN EVALUATION OF THE EFFECTIVENESS OF THE DATA PROTECTION AND PRIVACY ACT IN PROTECTING THE RIGHT TO PRIVACY IN UGANDA

COMFORT RUTAYA MURUHURA

BS21B11/234

A DISSERTATION SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF UGANDA CHRISTIAN UNIVERSITY

December, 2025

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, Muruhura Comfort Rutaya, do hereby declare that this dissertation is original and has not been submitted for an award of a degree or any other qualification in any University.

.....

MURUHURA COMFORT RUTAYA

DATE 11/12/2025

APPROVED BY

.....

MR. EDRINE WANYAMA

(SUPERVISOR)

DATE 11/12/2025

DEDICATION

To my God, my country at large and family for the endless support and encouragement have been my strength.

ACKNOWLEDGEMENT

I am deeply grateful to my supervisor Mr. Edrine Wanyama, thank you for sparing your time and effort to contribute to my academic journey May the Almighty God bless you.

To my God-given parents who have invested time, money, and love in me, I pray that your efforts will not be in vain and may God grant you long life to see your seed bear fruit.

My siblings who have been instrumental in shaping me as a person. Thank you to each and every one of you.

To Ms. Judith Nansubuga legal project officer at Greenwatch for your guidance, encouragement, and constructive feedback throughout the process of developing this dissertation. May God bless you.

LIST OF ACRONYMS

DPPA: Data Protection and Privacy Act.

NITA: National Information Technology Authority.

PDPO: Personal Data Protection Offices

DPPR: Data Protection and privacy Regulations

UPDF: Uganda People's Defence Force.

GOU: Government of Uganda.

GDPR: General Data Protection Regulation

CSV: Comma Separated Values.

MoJCA: Ministry of Justice and Constitutional Affairs.

UCC: Uganda Communications Commission.

EU: European Union.

AU: African Union.

Cap: Chapter.

TABLE OF CONTENTS

LIST OF AUTHORITY

Cases

Bassajjabaka Yusuf v MTN Uganda (HCCS. NO. 100 OF 2012)

Charles. Onyango. Obbo & Andrew. Mwenda Via. A.G (Constitutional Petition No.15 of 1997)

European Commission v. Federal Republic of Germany (CJEU, C-518/07)

Green watch (U) Ltd Vs. A.G & Anor [2002] UGHCCD 23.

Sserunjogi v Guinness Transporters limited Ta safe boda [Labour Dispute Reference 47 of [2022] [2024] UGIC 49(16 August 2024)

LIST OF LEGISLATION

National legislation

Acts and statutory instruments

The 1995 Constitution of the Republic of Uganda (As Amended)

The Data Protection and Privacy Act, Cap 97

The Computer Misuse (Amendment) Act, 2002

Regional legislation

African Charter on Human and People's Rights (Date of adoption: June, 1981, Entry into force: October 21, 1986.)

Council of Europe's Convention 108 in 1981

Declarations by the African Commission

General Data Protection Regulations

International legislation

The Universal Declaration of Human Rights (UDHR), 1948

The International Covenant on Civil and Political Rights (ICCPR), 1966

OECD Guidelines on Data Protection and Privacy

ABSTRACT

This study explores the effectiveness of the Data Protection and Data Privacy Act in protecting the right to privacy in Uganda. The right to privacy is a fundamental human right enshrined in both international human rights instruments and national constitutions. In Uganda, the enactment of the Data Protection and Privacy Act, cap 97 marked a significant step in addressing emerging privacy challenges in an increasingly digital society. With the employment of the Doctrinal research method This dissertation critically examines the effectiveness of the Data Protection and Privacy Act in safeguarding the right to privacy in Uganda, particularly in the context of rapid technological advancements, expanding digital surveillance, and data-driven governance in relation to one's right to privacy.

The study therefore explores regional, international and national legal, institutional, and practical frameworks on data protection and data privacy for instance the General Data Protection Regulation (GDPR) and the African Union Convention on Cyber Security and Persona Data Protection (Malabo Convention) , assessing their adequacy in ensuring the protection of personal data and the enforcement of privacy rights, the rights of data subjects and the role of the different stake holders such as the Personal Data Protection Officer (PDPO).

The dissertation looks into the several enforcement challenges and limitations integrated into the national, legal, institutional and policy frameworks. These challenges and limitations range from limited public awareness, weak penalties imposed by the law, inexperienced and incompetent data protection officers, political interference and lack of independence among others and how these challenges have negatively affected the enjoyment of the right to data privacy in Uganda.

In conclusion the study highlights the critical need for consorted efforts in protecting and upholding the right to data privacy and protection in Uganda.

It further gives several recommendations focused at integrating the legal and institutional structures for data protection that: promote public awareness by applying countrywide campaigns to enhance interpretation of data protection rights, promote accountability by strengthening implementation mechanisms to make sure data controllers and processors act in accordance with DPPA including stricter oversight and penalties, support SME compliance by providing subsidies and simplified guidelines to allow small and medium enterprises adopt stable data practices, address technological challenges by improving cyber security infrastructure and mandate secure data storage to combat breaches and unaccredited access, revise legal provisions by amending the DPPA to clarify exemptions and strengthen penalties, combat surveillance by putting in place judicial oversight for surveillance activities and whistleblower protections to escape abuse and ensure transparency and lastly provide financing for CSOs to increase advocacy by distributing resources to civil society organizations.

CHAPTER ONE

GENERAL BACKGROUND

1.1 Introduction

This chapter establishes the analytical framework for evaluating the DPPA's effectiveness by examining the legal, institutional, and practical challenges facing data protection in Uganda, situating this analysis within broader scholarly debates about privacy rights, regulatory effectiveness, and technological governance in developing country contexts all presented in the background of the study, statement of the problem, objectives of the study, research questions, significance of the study, justification of the study, scope of the study, and literature review.

1.2 Background of the Study

Privacy Rights in Constitutional Theory; The concept of privacy in constitutional law encompasses multiple, sometimes competing theoretical foundations. The earliest and most cited theory is from Samuel Warren and Louis Brandeis's formulation of privacy as the "right to be let alone"[1] from their 1890 Harvard law review Article which provides one framework about privacy because it focused on personal autonomy and protection from personal exposure.

Later on, scholars like Daniel Solove in Understanding Privacy Harvard University Press, May 2008[2] developed a broader theory that offers a comprehensive overview of the difficulties involved in discussions of privacy and ultimately provides a provocative resolution. He argues that no single definition can be workable, but rather that there are multiple forms of privacy, related to one another by family resemblances such as; informational privacy which controls over personal data, physical privacy majorly for bodily integrity, associational privacy which focuses on freedom to associate privately, and communicative privacy which focuses on freedom to control personal communication.

Privacy as a constitutional value; In the Ugandan constitutional context, Article 27 of the Republic of Uganda 1995 as amended the protection of "privacy of person, home and other property" reflects this multidimensional understanding but requires interpretation in light of technological developments unforeseen by the

[1] https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
[2] https://www.danielsolove.com/understanding-privacy/

constitutional framers. The Constitutional Court's approach in Charles Onyango Obbo v Attorney General 2000[3] suggests a preference for balancing privacy against other constitutional values like freedom of expression rather than treating privacy as absolute, but the court has not yet developed comprehensive doctrine for informational privacy specifically which means that data protection cases are left to statutory interpretation rather than constitutional guidance.

A strong data protection framework is one that deals with personal privacy and systematic digital risks (Solove, 2006). This is an urgent matter in Uganda considering the underdeveloped judicial interpretation of data privacy as seen in the narrow ruling of Charles Onyango Obbo v Attorney General. Additionally, the theory of contextual integrity by Nissenbaum (2009) posits that geographical features determine privacy expectations in Uganda. For example, sharing personal data within a clan is acceptable but a normative breach within a telecom company. Uganda's Data Protection and Privacy Act require sector specific guidelines needed to navigate these challenges, thus justifying the need for more adaptive legal principles.

The International Covenant on Civil and Political Rights approved by the Ugandan government in 1995 works co-currently with article 17 of the national constitution to tackle cases of arbitrary privacy breaches. Article 27 of the Ugandan National Constitution prevents interference through enhanced correspondence and communication strategies despite the fact that the applicability of digital data remains untested by the courts. A comparative look at article 31 of Kenya suggests that purposive interpretation is possible which can improve consistency in enhancing data privacy if adopted by DPPA.

The limitation of rights that are prescribed by law and reasonably justifiable in a democratic society poses a serious constitutional challenge that arises from article 43. The exemptions by DDPA on National security and public interest in section four could propagate excessive state surveillance. DPPA requires stronger oversight mechanisms like mandatory judicial warrants which will help the body adequately balance state powers with the fundamental right to privacy.

[3] Charles Onyango Obbo v Attorney General

1.2 Statement of the Problem

The computer misuse amendment act of 2022 undermines Uganda's constitutional right to privacy according to the country's 1995 constitution. This leads to the abuse of digital rights like freedom expression. For instance, a one Dr. Stella Nyanzi who is commonly known as an academic and social critic was arrested for insulting president Yoweri Kaguta Museveni in a social media post in 2019, she was convicted of cyber harassment contrary to section 24 [4]of the Computer Misuse Act but acquitted of offensive communications, which is provided for under section 25[5].She was given an 18-month prison sentence, but the Court of Appeal cleared her, ruling that the trial magistrate lacked the authority to convict her of cyber harassment and that the prosecution's evidence was insufficient. Other people have been subject to the same law's wrath, including former presidential candidate Henry Tumukunde, who was detained for allegedly making unreasonable remarks in radio and television interviews, the comedy group Bizonto, who were detained for allegedly posting offensive and sectarian content, and author Kakwenza Rukirabashaija who was detained and prosecuted over offensive communication against the president Yoweri Kaguta Museveni and his son Muhoozi Keinerugaba of which these people that were arrested are obtained through accessing of their private details like homes, phones to access their current location without their consent which violates their enjoyment of their right to privacy.

The effectiveness of Uganda's historic Data Protection and Privacy Act Cap 97, which protects people's right to privacy, in preserving personal information in the digital age has thus been called into question. Significant implementation and enforcement gaps still exist in Uganda's Data Protection and Privacy Act (DPPA), despite its enactment. Unregulated data processing activities by both public and private entities remain persistent for example The Wall Street Journal an international media claimed that Huawei which is a giant telecommunication company was helping the government of Uganda to hack into Hon Kyagulanyi

[4] Computer misuse(amendment) act 2022
[5] ibid

Robert alias Bobi wine's WhatsApp and skype communications [6]thus undermining the Act's objectives.[7]

This study evaluates the effectiveness of Uganda's Data Protection and Privacy Act, 2019. It scrutinizes the law's alignment with international standards, its capacity to regulate emerging technologies, and the strength of its enforcement mechanisms, particularly concerning oversight and public awareness, to identify critical areas for legal improvement.

1.3 Objectives of the Study

1.3.1 General Objective

To evaluate the effectiveness of the Data Protection and Privacy Act Cap 97 in protecting the right to privacy in Uganda.

1.3.2 Specific Objectives

1. To discuss the theoretic framework on data protection and privacy
2. To discuss the international and regional legal and institutional framework on data protection and privacy.
3. To discuss the Uganda's legal and institutional framework on data protection and privacy.

1.4 Research questions

The study will be guided by the following questions.

1. What is the theoretic framework on data protection and privacy.
2. What is the international and regional institutional and legal framework on data protection and privacy?

[6] https://nilepost.co.ug/news/52067/wsj-reports-huawei-helped-uganda-government-to-hack-bobi-wines-whatsapp-skype-conversations

[7] Angelo Sewanonda Data Protection in Uganda: Assessing the Impact of the Data Protection and Privacy Regulations of 2021 on the Data Privacy Regulatory Framework and Data Protection in Africa

3. What is Uganda's legal and institutional framework on data protection and privacy and the challenges faced while implementing these legal and institutional instruments?
4. What are the major study findings, conclusions and recommendations

1.5 Significance of the study

This study critically analyses the Data Protection and Privacy Act of Uganda thus offering multifaceted significance. It addresses literature gaps on data privacy, provides actionable insights for strengthening the law and its enforcement for policymakers and regulators like NITA-U.

1.6 Justification of the study

This study addressed the gap between the legal structure of the 2019 Uganda Data Protection and Privacy Act as well as its poor implementation strategies and public awareness programs. This research gives timely, practical recommendations to strengthen the law's implementation, empower Ugandans, and ensure the country's data governance aligns with international standards like the GDPR, which is crucial for digital trade and security.

1.7 Scope of the study

1.7.1 Content Scope

This study mainly focused on the legal, institutional, and practical aspects of data protection and privacy in Uganda, with specific reference to the Data Protection and Privacy Act cap 97. It further assesses other relevant foreign data protection laws, evolving trends in data management, privacy and security.

1.7.2 Geographical Scope

Primary Focus

The research primary focuses and centres on Uganda as the geographical context, analysing the relevance and application of Data Privacy and Data protection Act within the country. It also investigates data crimes and breaches in Uganda, considering jurisdictional challenges discussed at the Brussels International Conference on Computer Privacy and Protection in January 2015. The conference highlighted the global nature of the internet and the territorial limitations of legal

systems. This study focuses specifically on Uganda, the first African country to implement a national data protection law.

Secondary focus

This dissertation might as well briefly examine the differences in how urban and rural areas access and experience the Data Protection and Privacy Act cap 97. This can include considerations of digital access and privacy risks faced in different regions of the country, this is because the ratio of data subjects and users is greatly proportionate in urban areas of Uganda than the rural areas.

1.7.3 Thematic/Subject Scope

This study analyses the legal framework of Uganda's Data Protection and Privacy Act, 2019. It investigates the constitutional foundation of this right under Article 27 of the 1995 Constitution and its adaptation to digital challenges. It critically assesses the Act's key provisions such as the definition of personal data, digital user rights and the mandate of digital controllers. The study is grounded on data protection frameworks like lawfulness, transparency and references related statutes, including the Access to Information Act, 2005 and the Computer Misuse Act, 2011.

1.7.4 Temporal Scope/ (Time-Based)

This study was conducted from 2019- 2025 focusing on the post enactment era of the Uganda Data Protection and Privacy Act, 2019. This time scope was the most suitable for critically assessing the law's implementation, enforcement, and distinct impact.

1.8 Literature Review

1.8.1 Privacy Rights and Data Protection Scholarship

This review is built upon four themes that evaluate Uganda's framework: the theoretical roots of privacy, comparative data protection models, constitutional privacy in common law nations, and regulatory performance in developing economies. It identifies a critical research gap concerning the contextual application of these themes to Uganda's unique socio-legal landscape. The study clarifies how Uganda's Data Protection and Privacy Act, 2019 (DPPA) transforms the

constitutional assurance in Article 27 of the 1995 Constitution into an enforceable regulatory measure, addressing a major gap in studies on operationalizing privacy in developing nations.

1.8.2 Theoretical Foundations of Privacy Rights

1.8.2.1 Classical Privacy Theory

This theory was developed by Warren and Brandel in 1890 has proven to be insufficient in modern data governance. The data control concept initiated by Westin in 1967 provided a more relevant framework for digital contexts. A significant literature gap remains on the applicability of these theories in the Ugandan context. This study therefore seeks to evaluate structural risks like data aggregation by telecoms, under Uganda's Data Protection and Privacy Act, 2019.

1.8.2.2 Contemporary Privacy Theory

Privacy is viewed as a social good by modern day scholars with Regan (1995) and Cohen (2013) emphasizing its value in democracy and human development. According to the theory of contextual integrity developed by Nissenbaum, data validity with in specific social settings is a powerful assessment tool for Uganda's Data Protection and Privacy Act, 2019. This study addresses critical theoretical gaps by exploring how the contemporary theory can be merged with Ugandan societal norms, where information sharing at clan level is acceptable but not with commercial entities.

1.8.3 Comparative Data Protection Law

Global Models and Transplantation

Scholars like Greenleaf (2014) note key variations in implementation across nations. Makulilo (2015) critiques the transfer of European standards into Africa, warning that it overlooks local contexts. This critique lays the foundation for the study by assessing the the fit between the GDPR-inspired DPPA and Uganda's context, using empirical data like the low number of complaints (200 cases in 2025) to identify any potential challenges of adaptation (NITA-U, 2023).

African Regional Developments

At continental level, the Malabo Convention initiated by the African Union targets a tailored system but scholars claim it's enforcement and ratification levels are low (Makulilo & Ng'ong'ola, 2018). Similar studies by Rinsloo & Kaliisa, 2024 report

similar implementation challenges in East Africa. This research fills a gap by moving beyond legal text to assess the DPPA's practical effectiveness, using incidents like the 2019 NIRA breach to evaluate its actual impact in the world.

1.8.4 Constitutional Privacy Rights in Common Law Systems

Interpretive Approaches

Constitutional privacy interpretation in common law varies. Roach (2014) examines Canada's proportional approach, which is relevant for Uganda's similar Article 27. Murray (2007) notes the common law tendency for interest-balancing, depends on how Ugandan courts deal with digital privacy. A significant literature gap exists on how statutes like the DPPA operationalize constitutional guarantees in African common law states, a gap this study addresses.

Technology and Constitutional Adaptation

Kerr (2010) argues that constitutional policies are technologically backward highlighting the key role of legislation like the DPPA. There is limited research on how Uganda’s constitutional privacy adapts to new technologies like biometrics. This research study expands on the body of knowledge by evaluating the DPPA’s capacity to bridge this technological-constitutional gap.

1.8.5 Regulatory Effectiveness in Developing Countries

Implementation Challenges

Scholars identify political will, resources, and institutional capacity as important factors for regulation in developing nations (Baldwin, Cave, & Lodge, 2012). Greenleaf and Cottier (2020) confirm that data protection laws often surpass implementation abilities. There is a lack of a systematic analysis on the real-world impact of DPPA. This study addresses this gap by evaluating enforcement evidence and institutional constraints like NITA-U's underfunding.

Institutional Design Issues

The design of regulatory bodies is paramount. Raab and Koops (2009) establish that independence, resources, and strong powers are prerequisites for an effective data protection authority. A significant literature void concerns how institutional structures like Uganda's Personal Data Protection Office (PDPO) influence

outcomes. This study bridges that gap by analysing the PDPO's structural limitations.

1.9 Methodology of The Study

This study applied majorly secondary method of collecting data. This study extensively employed desktop research with reliance on reviewing and analysing of primary legal instruments including the 1995 constitution of the Republic of Uganda, the DPPA, regional and international legal human rights instruments, relevant case law and already published and unpublished works, journals articles, therefore this study is dominated by secondary data analysis.

1.10 Desktop Research

The study relied on desktop research method, also known as secondary research which involves gathering information and data from existing sources, such as books, journals, articles, websites, reports, and other published materials. It requires a user to analyse and synthesize information from already available information. This research method was used to review existing literature on data protection and privacy where most of the literature was traced in legal instruments like the constitution, published and unpublished works. Accordingly, textbooks, reports, and online resources especially from regional and international websites. The diverse literature reviewed enabled the researcher to enrich the study through making comparisons of different writings on data protection and privacy across the world and also best understand the data on the protection of the right to privacy.

Desktop research method was so beneficial as it provided quick insights since information from existing literature was gathered in less time unlike conducting interviews, tests and panels which take time. It was also cost effective, created access to diverse resources which enabled the user to not get limited by one source of information.

1.10.1 Conclusion

This research addresses these gaps by providing a comprehensive constitutional analysis of the DPPA's effectiveness, systematically evaluating implementation outcomes, and offering a framework for adapting international models to Uganda's context, alongside evidence-based recommendations for regulatory enhancement.

However, significant gaps exist in constitutional analysis of data protection effectiveness and systematic evaluation of implementation outcomes in African contexts. This research addresses these gaps while contributing to broader scholarly understanding of constitutional privacy protection in digital contexts.

CHAPTER TWO

THEORETICAL FRAMEWORK ON THE RIGHT TO PRIVACY

2.0 Introduction

This chapter provides an in-depth philosophical analysis of privacy, grounding the legal right to privacy in foundational theories. These theoretical positions offer a structured framework to critically examine whether the Data Protection and Privacy Act, cap 97 of Uganda sufficiently protects the multifaceted right to privacy. The framework is built on six dominant philosophical theories that is the non-intrusion theory, the right to be left alone, control theory, limited access theory, informational privacy theory, and contextual integrity. These theories are drawn from both classical liberal thought and modern digital rights scholarship, enabling a holistic and contextualised analysis of privacy in Uganda.

2.1 Non-Intrusion Theory of Privacy

The non-intrusion theory sees privacy primarily as protection from unwanted physical, visual, or digital encroachment. As originally formulated in liberal philosophy and jurisprudence, this theory asserts that privacy is the moral and legal right of individuals to be free from direct interference in their personal space. Warren and Brandeis were pioneers in articulating this idea in a classical Article that so many scholars have regarded to be the seminal work of privacy, proposing privacy as a freestanding right in their 1890 article.[8] They viewed privacy violations as harm in themselves unjustified intrusions on a person's personal life.

In Uganda, Article 27 of the Constitution upholds this principle by prohibiting unlawful search, seizure, and interference with personal communications. This aligns with global standards found in Article 17 of the International Covenant on Civil and Political Rights. Yet, in practice, police and other agencies are known to intercept communications and conduct home raids without valid court orders. This mismatch between constitutional theory and administrative practice demonstrates that the non-intrusion principle, while enshrined in law, is inconsistently applied.

[8]SD Warren and LD Brandeis, The Right to Privacy, 1890 Harvard Law Review 193

In an increasingly digitised environment, the scope of non-intrusion has expanded beyond physical spaces. State surveillance systems, biometric registration programs, and facial recognition technologies present new forms of intrusion. These require updating traditional privacy frameworks to reflect digital realities, where presence and control extend into data clouds, servers, and algorithmic systems.

2.2 Seclusion theory of privacy and the Right to Be Left Alone

Under the seclusion theory of privacy, Ruth Gavison while giving remarks described a person to be enjoying perfect privacy when that person is completely inaccessible meaning that one has to be secluded from others something that confuses privacy with solitude because seclusion suggests that the more alone one is the more privacy one in this scheme it would follow that a person stranded on an island in which there are no human inhabitants would have complete privacy.

While the non-intrusion theory focuses on external interference, the right to be left alone extends privacy to decisional and psychological domains. It encompasses the individual's liberty to make decisions, form thoughts, and live without coercion or surveillance.[9] This theory is especially important in protecting choices related to sexuality, religion, lifestyle, and identity.

2.3 Control Theory of Privacy

According to Charles fried, privacy is not simply an absence of information about us in the minds of others rather it is the control over information we have about ourselves in 1990. Arthur Miller embraces a version of the control theory when he describes privacy as the individual's ability to control the circulation of information relating to him. Also, Alan Westin by endorsing the same version of the control theory reframes privacy as the ability of individuals to decide when, how, and to what extent their personal information is communicated to others.[10] the emphasis here is on autonomy and informed consent values at the core of democratic societies. Westin's vision has strongly influenced modern data protection statutes globally, including Uganda's Data Protection and Data Privacy Act cap 97.

[9] SD Warren and LD Brandeis, The right to privacy, 1890 Harvard Law Review
[10] AF Westin, Privacy and freedom 1967

The Act embraces consent as a legal ground for data processing. However, the challenge arises in operationalising genuine consent in a context marked by digital illiteracy and power asymmetries. However, consent doesn't give room for authentic user autonomy. There is need to adopt Westin's conceptual framework where legitimate consent is voluntary, fully informed, context specific and readily revocable.

Systems employing automated decision making must afford individuals a clear right to explication and the opportunity to challenge decisions thus safeguarding personal sovereignty.

To align with control theory, the law should mandate plain language consent forms, periodic reaffirmation of consent, and default privacy-protecting settings. Furthermore, automated decision-making systems must be accompanied by the right to explanation and objection to maintain individual sovereignty.

2.4 Limited Access Theory

Sissela Bok's limited access theory of privacy frames the concept as an individual's capacity to govern the extent of exposure to others.[11] Far from equating privacy with outright secrecy, Bok emphasises the deliberate management of the circumstances under which one's person, spaces, interactions and data become accessible. In this view, privacy emerges as the prerogative to modulate access to the body, private domains, conversations and personal information.

The limited access theory and African societal value system posit that the flow of information is socially determined. Uganda's Data Protection and Privacy Act, 2019 reflects this by emphasizing the need and regulation of data collection for specific purposes (Section 26). However, the inconsistences in enforcement within rural communities that are digitally illiterate undermines this principle. For this theory to take effect, the law must spell out more clear boundaries in key sectors like healthcare and education. Furthermore, comprehensive privacy training for public servants should be implemented to avoid unintended disclosures and strengthen compliance.

2.5 Informational Privacy Theory

This theory identifies informational harm as arising from unauthorised collection, surveillance, profiling, or sharing of personal data. This theory has become

[11] S Bok, Secrets; On the ethics of concealment and Revelation [Harvard University Press 1983

dominant in the digital age, particularly in the development of data protection laws worldwide.

Uganda's Data Protection and Privacy Act cap 97 includes key principles of this theory data minimisation, transparency, accuracy, purpose limitation, and data subject rights. These aim to regulate the life cycle of personal data and protect individuals from identity theft, profiling, and misuse of sensitive data as it was seen in the safe boda case where the National Information Technology Authority Uganda (NITA-U) after completing its investigations into allegations of unlawful sharing of Safe Boda users' personal information without their consent by Guinness Transporters Limited Trading as Safe Boda, and issued a report on the same.

The investigations were commenced following a complaint made by Mr. Obedgiu Sammy and it was carried out pursuant to the powers upon NITA in section 32 of the Data Protection & Privacy Act of 2019, to investigate complaining alleging either non-compliance with the provisions of the Act or breaches.

This investigation, arguably the first investigation under the provisions of the Data Protection and Privacy Act, cap 97 concluded that:

The Safe Boda's Privacy Policing and Data Protection Policy version of 2017 and 2019 respectively did not provide information on recipients with whom its users personal data will be shared;

Safe Boda's disclosure of its users' personal data to Clever Tap a data processor that offered Software as a Service for customer lifestyle management and mobile marketing contravened the Data Protection and Privacy Act, since the consents relied upon for the disclosure were not specific neither were they informed, given that the users were not informed of the extent of the personal data collected and the potential disclosure of their personal data with Clever Tap.

Safe Boda was therefore directed to address all the areas of non-compliance identified within four months[12]

However, the increasing use of digital identity systems, biometric registration, and financial technology services creates new privacy vulnerabilities that current laws inadequately address.

[12] https://www.kaa.co.ug/safeboda-has-been-investigated-on-allegations-of-unlawful-sharing-of-users-personal-data/

2.6 Contextual Integrity

Helen Nissenbaum's theory of contextual integrity defines privacy as the suitable flow of information according to the norms of specific social contexts (Nissenbaum, 2009).

The Uganda's Data Protection and Privacy Act, 2019 fails to give appropriate measures for evaluating relevance of data disclosure which often increases chances of abuse. The contextual integrity theory acknowledges the cultural fluid nature of privacy norms which may violate expectations in an urban commercial setting. Joint implementation of DPPA and the contextual integrity theory will require flexible regulations and actionable steps to align the law with diverse communal expectations.

2.7 Integrative Analysis and Legal Reform Proposals

A synthesis of privacy theories reveals it as a multifaceted right anchored in autonomy, dignity, and cultural context. While Uganda's Data Protection and Privacy Act, 2019 incorporates these principles, its implementation is inconsistent. To bridge this theory-practice gap, key reforms are essential: bolstering the Personal Data Protection Office's capacity with more resources; mandating clear, revocable consent mechanisms; creating sector-specific codes for contexts like healthcare; launching public data literacy campaigns; and engaging community leaders to legitimize privacy norms.

2.8 Conclusion

The 2019 Uganda Data Protection and Privacy Act give a foundational structure but lack the institutional capacity for full implementation. For this act to be fruitful, it may require incorporation of key theoretical principles with legal reforms, implementation measures and public awareness campaigns. In the long run, DPPA's legal framework will become effective in advocating for human rights in a digital era.

CHAPTER THREE

INTERNATIONAL AND REGIONAL LEGAL AND INSTITUTIONAL FRAMEWORK ON DATA PROTECTION AND PRIVACY

3.0 Introduction

This chapter provides an in-depth examination of the legal and institutional framework governing data protection and privacy on a regional and international level. It outlines the legal foundation for the right to privacy, evaluates the key provisions of relevant laws that impact data protection and also explores the roles of institutions responsible for enforcing data privacy on regional and international standards that influence Uganda's data protection and privacy regime.

International Legal Regime on Data Protection and Privacy

3.1 The Universal Declaration of Human Rights

The Universal Declaration of Human Rights provides for the right to privacy of the person under Article 12 which states that **"**No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. 'It is important to note that Uganda has ratified to this instrument[13].

Uganda is also a signatory to the International Covenant on Civil and Political Rights[14] whose Article 17 (1) provides that; **''**No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation; and (2) everyone has the right to the protection of the law against such interference or attacks**"**[15]

Resolution adopted by the General Assembly on 18 December 2013[16] calling upon member states to observe the right to privacy. Additionally United Nations Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018. Personal data protection and privacy principles, which elucidated on the data protection principles to be adopted.

[13] The Universal Declaration of Human Rights
[14] International Covenant on Civil and Political Rights
[15] Ibid
[16] [on the report of the Third Committee (A/68/456/Add.2)]

In Africa, data protection laws are enshrined in declaration of principles on freedom of expression and access to information in Africa[17].Perhaps a more direct and binding instrument, the Declaration of Principles on Freedom of Expression and Access to Information in Africa is sourced from the African Charter on Human and Peoples' Rights (ACHPR). The ACHPR which all African countries are parties to and obligated to abide by is the most primary human rights instrument in Africa. Article 9 of the Charter provides for the right to freedom of expression and access to information, which has in turn produced more guidelines on both rights in the digital age. Principle 40 of the Declaration provides for the protection of people's personal information. Principles 41 and 42 address privacy and communication surveillance and establish the legal framework for the protection of personal information in Africa.

3.2 International Covenant on Civil and Political Rights (ICCPR)

Article 17[18]of the International Covenant on Civil and Political Rights states that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor unlawful attacks on his honour and reputation and that the right to the protection of the law against such interference or attacks is to be enjoyed by every person. In addition, General Comment number sixteen to the ICCPR provides additional specification on data protection necessities under Article 17 which states that the collection and storage of personal information on computers, in data bases or other devices, whether by public or private bodies must be regulated by law; to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive effective measures must be taken by states, process and use it; information usage for purposes incompatible with the Covenant must be prevented; the right to determine what information is being held about individuals and for what purposes and to request rectification or elimination of incorrect information belongs to those exact individuals; any interference with these rights must only take place on the basis of law which must comply with the Covenant. These requirements are complemented by the storing body's duty of transparency

[17] Declaration of principles on freedom of expression and access to information in Africa,2019
[18] International Covenant on Civil and Political Rights

concerning data processing, in particular the provision of information, rectification and elimination as vital data protection principles.

3.3 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

In respect to privacy, the OECD Privacy Guidelines are the first internationally agreed-upon set of privacy principles which are recognized globally as a minimum standard for privacy and data protection. They are a huge foundation for building effective protection and trust for individuals, and also for developing common international approaches to transborder data flows. Promotion of respect for privacy is essential for an operational digital economy therefore when individuals have confidence in the protections surrounding their personal data, they are more likely to engage in online activities, share information, and participate in the digital economy which in turn drives economic growth, fosters innovation, and encourages the free flow of data across borders

Since their adoption, they have influenced legislation and policy in OECD countries and beyond and they include national and international principles of application.

Basic Principles of National Application [19] Below are the outlined fundamental principles that member countries should adopt to regulate and protect the processing of personal data from collection to disposal stage which are provided for under Part II.

Collection Limitation Principle**:** The collection of personal data should be fair and lawful and, wherever appropriate, done with the consent of the data subject. Consent is not necessary for situations like criminal investigations or routine updates of mailing lists. This principle also applies to data subjects who are minors, mentally disabled, or in similar cases and are represented by a third party.

Data Quality Principle**:** The personal data should be complete, accurate, and kept up-to-date. It should also be necessary and relevant to the purposes it is collected for. Historical data may be collected or retained for archival activities social and historical research.

[19]https://www.bitraser.com/article/oecd-guidelines-privacy-personal-data-protection.php?srsltid=AfmBOooVY_hwgTAEbRjBz-ZzMmb9PEBeptN1KIrmPme-6feo_DkH_DtT

Purpose Specification Principle; The goal of data collection should be stated at every stage of change and at the very least when the data is being collected. The use of the data should also align with the reason it was gathered. Unauthorized duplication, theft, and other risks make it necessary to erase, destroy, or anonymize data that is no longer needed or of no interest. Software such as Bitraser file eraser is advised for data minimization, to destroy unnecessary, Redundant, Obsolete, and Trivial (ROT) data, along with maintaining proof of data destruction. Certificates of destruction serve as an audit trail and help in achieving compliance with OECD data privacy guidelines.

Use Limitation Principle: Unless given consent by the data subject or authorization by the law, the personal data should not be used, disclosed, or made available for unspecified purposes.

Security Safeguards Principle: Adequate security and privacy measures ought to be implemented to stop data loss, illegal disclosure, use, access, alteration, or destruction of personal information. Organizational safeguards like access privileges, informational safeguards like enciphering, and physical safeguards like ID cards are also included.

Openness Principle: A general policy of openness on developments and practices of personal data should be established. Along with the identity and residence of the data controller, means should be made available to establish the nature and existence of personal data, and the purposes for their use.

Individual Participation Principle: The rights of an individual should include: obtaining confirmation of the data held by the data controller or another entity; receiving information about the data in an understandable format within a reasonable timeframe and at a reasonable cost; receiving an explanation for the denial of the aforementioned requests and challenging the denial; and challenging related data and having their data completed, amended, rectified, or erased upon successful challenge.

Accountability Principle: under the accountability principle it is the data controller's responsibility to adhere to the aforementioned principles, even in cases where a third party performs the processing.

The OECD Basic Principles of International Application

These guidelines encourage cross-border, subject to certain limitations, personal data sharing among participating nations for the benefit of the general public. The key points discussed in Part III are outlined below. These include the requirement that member nations consider the effects of domestic processing and re-exporting of personal data on other nations and take all necessary and reasonable measures to guarantee safe and continuous transborder flows of personal data, a member country should not impose restrictions on the transborder flow of personal data with another member country, including transit through that country, unless doing so would violate its domestic privacy laws or the other country is not yet adhering to these rules. A member nation may impose restrictions on specific categories of personal data if its domestic privacy legislation includes regulations considering the type of data, but the other member nation does not offer comparable protection., lastly the member countries should avoid developing laws, policies, and practices in the name of protecting privacy and individual liberties that hinder the transborder flow of personal data, exceeding requirements for such protection.

Regional legal framework

3.4 The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018, and governs the protection of personal data in EU and EEA Member States. The Data Protection and Privacy Act cap 97 which came into force in May 2019, is the primary piece of data protection legislation in Uganda and has been supplemented with the Data Protection and Privacy Regulations, 2021 ('the Regulations'), which were introduced on 12 March 2021. The Act and Regulations share several similarities with the GDPR in terms of overarching principles and the general regulation of data controllers, processors, and data subject rights. Furthermore, similar to the requirement under the GDPR to provide for a data protection authority responsible for monitoring the application of the GDPR, the Regulations provide for the establishment of the Personal Data Protection Office ('PDPO') within the National Information Technology Authority - Uganda ('NITA-U'), with the PDPO responsible for the overall implementation of the Act and the Regulations. However, there are also significant differences between

the frameworks, particularly in relation to the obligations of organisations. Notably, the Regulations have introduced additional provisions, particularly in relation to data processing records, Data Protection Impact Assessments ('DPIA'), data protection officer ('DPO') appointment, and data transfers. However, in general terms, the provisions within the Act and its Regulations are slightly less detailed than those found within the GDPR. Article 5[20] provides for the GDPR Principles relating to personal data processing and it states that personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject, collected for specified, explicit and legitimate purposes and not further processed in a way that is not in line with those purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1)[21], not be considered to be incompatible with the initial purposes, adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed data minimisation, accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay accuracy, kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

According to Article 6 of the GDPR, it provides for Lawfulness of processing which states that processing shall be lawful only if and to the extent that at least one of the following applies; the data subject has consented to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a legal obligation to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing is necessary for the purposes

[20] General Data Protection Regulation
[21] ibid

of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.5 The African Union's Malabo Convention on Cyber Security and Personal Data Protection

The African Union's Convention on Cyber Security and Personal Data Protection which was adopted after nine years on 27th of June, 2014 also known as the Malabo convention came into force and became the only binding regional treaty on data protection outside Europe but it considerably mirrors a number of standards from Europe both from the Council of Europe Convention for the protection of individuals with regard to the processing of personal data and GDPR

The scope of application of the Malabo Convention is territorial meaning that the Convention applies when any data processing whether automated or non-automated is undertaken in the territory of State parties by individuals, the State, local communities, or private actors as per Article 9[22].

The Malabo Convention under Article 13[23] contains six basic principles governing personal data processing and the first principle is consent which requires that the consent of the data subject or right holders must be sought before any processing of data. Second, the processing must be lawful and fair which means that, any processing, collection, recording, storage and transmission of personal data must be conducted fairly, and lawfully. The third principle relates to purpose or relevance which dictates that data must be collected for specific purposes or uses only. Accuracy of data is another principle, data controllers are required to take reasonable steps to make sure the collected data is up-to-date, and also to erase or amend it whenever it appears to be inaccurate or incomplete. Also, the Malabo Convention requires that data must be processed in a transparent manner meaning that data controllers or the States must disclose information concerning processing of personal data. The last principle is confidentiality which, *inter alia*, requires controllers to process personal data in secure and confidential ways.

[22] The African union's Malabo Convention on Cyber Security and Personal Data Protection
[23] ibid

Additionally, the Malabo Convention lays down specific principles for processing sensitive data under Article 14 and the interconnection of personal data files under Article 15.

The putting in place of the Convention is a huge milestone to realization of data privacy in the digital age in Africa. The Convention has a huge effect since African countries commenced digital trade within and beyond Africa. However, as a framework treaty, it lacks detailed rules, and procedures on data processing and protection, in turn, make it a lacklustre regional treaty. As such, the African Union should enact enabling legislation that clarifies general statutory provisions.

3.6 Declaration of Principles of Freedom of Expression and Access to Information in Africa by African Commission

During the African Commission on Human and people's Rights 65th Ordinary Session, which took place in Banjul, The Gambia, from October 21 to November 10, 2019, the African Commission[24] adopted the amended Declaration of Principles of Freedom of Expression and Access to Information in Africa. The updated Declaration superseded the 2002 Declaration of Principles of Freedom of Expression in Africa, and its adoption was a historic step that clarified Article 9[25] of the African Charter on Human and Peoples' Rights and helped to raise the bar for digital rights, freedom of expression, and information access in Africa by international norms and human rights. The 66th Ordinary Session of the African Commission was supposed to introduce the Declaration, but the COVID-19 pandemic caused it to be postponed.

The declaration was amended in light of the advancements in digital rights, access to information and freedom of express that made the 2002 declaration outdated. Notable developments included the 2013 law model on access of information for Africa, the 2017 guidelines on elections and access to information in Africa, and the African unions judicial and quasi-judicial bodies' jurisprudence on issues pertaining to freedom of expression and access to information.

[24] African commission on human and people's rights
[25] African charter on human and people's rights

Additionally, the rights to access information and freedom of expression were profoundly altered because of the advancements in information and communication technologies (ICTs)

The African commission adopted resolutions 222, 350, and 362 in response to these, directing the special rapporteur to update the declaration to reflect the aforementioned developments and to incorporate issues pertaining digital rights and access to information as they relate to Article 9 of the African charter.

Among the general principles enshrined in the amended declaration were the importance of the rights to freedom and access of information, non-interference with the freedom of opinion, non-discrimination, protection of digital rights to freedom of expression and access to information, protection of human rights defenders, and the development of children's capacities.

The freedom of expression principles pertaining to media diversity and pluralism, media independence, community media, private media, self-regulation and co-regulation, regulatory bodies for broadcast, telecommunications, and the internet, and the safety and protection of journalists and other media professionals. Regarding information access, the amended Declaration contained guidelines for proactive and maximum disclosure, information management, procedures for accessing information and the relevant exemptions, oversight, whistleblower protection, and the importance of access to information laws. The section on internet access and freedom of expression covered topics like internet access, internet intermediaries and access providers, privacy and the safeguarding of personal data, and privacy and communication monitoring.

The declaration states that 'states may only limit the exercise of the freedom of expression and access to information if the limitation is prescribed by the law; served a legitimate aim and is a necessary and proportionate means to achieve the stated aim in a democratic society.' This clause applies to restrictions on the right to access information and freedom of expression.

The African Commission reaffirmed in the amended Declaration and the essential significance of information access and freedom of expression as individual human rights, pillars of democracy, and facilitators of the exercise of other human rights.

Article 9 of the African Charter guaranteed the fundamental human rights of freedom of expression and information access. Other African Union documents, including the African Charter on the Rights and Welfare of the Child, the African Union Convention on Preventing and Combating Corruption, the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Persons with Disabilities in Africa, and the African Charter on Statistics, also recognized them, The African Charter on Democracy, Elections, and Governance; the African Charter on the Values and Principles of Public Service and Administration; the African Youth Charter; and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa.

3.7 Conclusion

Uganda's Data Protection and Privacy Act Cap 97 can be evaluated by comparing it to well established regional and international standards for data protection. The Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17) both affirm privacy as a basic human right obligating states like Uganda to enact legislation that shields personal data from arbitrary intrusion. Africa's Malabo Convention (2014) aims to harmonize rules but suffers from weak ratification and enforcement. The 2019 revision of the African Commission's Declaration of Principles on Freedom of Expression and Access to Information, which addresses privacy in the context of developing ICTs as previously mentioned, further reinforces digital rights under Article 9 of the African Charter.

CHAPTER FOUR
DISCUSSES UGANDA'S LEGAL AND INSTITUTIONAL FRAMEWORK ON DATA PROTECTION AND PRIVACY

4.1 Introduction

This chapter critically examines the Uganda's legal and institutional framework governing data protection and privacy right from the mother law 1995 constitution of the republic of Uganda to the Data Protection and Privacy Act cap 97 and its supplementary regulations and principles. It also discusses complementary legislation such as the Computer Misuse (Amendment) Act 2022, the role of key institutions including the Personal Data Protection office, the National Information Technology Authority (NITA-U), the Ministry of Information and Communications Technology, the Uganda Communications Commission and the Judiciary with an integration of the challenges and limitations challenging the enforcement of the DPPA in the analysis of each legal and institutional mechanism.

4.2 The 1995 Constitution of the Republic of Uganda

The right to privacy is a fundamental right guaranteed under Article 27[26] which guarantees a right to privacy of a person, home and other property. This has been strengthened further with the parliament passing other privacy related laws. These include the Computer Misuse Act 2011, Electronic Transactions Act, 2011, and the more recent which is elaborative is the Data Protection and Privacy Act cap 97.

In furtherance, Article 27(2) (supra) stipulates that no individual shall be subjected to the intrusion of the privacy of that individual's home, correspondence, communication, or other property. For Instance, in 2014, Uganda's government through the National Information Technology (MoICT) and the Ministry of Justice and Constitutional Affairs (MoJCA) issued a draft Data Protection and Privacy Bill for public comment and it was enacted into law in February 2019.

Article 27(supra) protects an individual's right to privacy of person, home, and other property, and thus prohibits any form of an unlawful search of the home, property, and individual's person. This Article further bars unlawful entry into a

[26] The Constitution of The Republic of Uganda ,1995 as amended

person's premises and interference with the privacy of a person's home, communication, or other property, illegal in the case of Charles. Onyango Obbo and Andrew Muwenda vs. AG[27] illustrated that Activities that restrict the right to privacy such as surveillance and censorship can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued as elaborated by Honorable Justice Manyindo.

Article 41(1) of the 1995 Constitution of the Republic of Uganda (as amended) stipulates that every citizen has a right of access to information in the possession of the state or any other organ or agency of the state except where the release of the information is likely to prejudice the security or sovereignty of the State or interfere with the right to the privacy of any other person.

Article 41(supra) provides for a more elaborate assertion for an efficient, effective, accountable, and transparent government and gives effect to this which aims at protecting individuals from disclosing information as well as empowering the public to effectively scrutinize and participate in Government's decisions that affect them. Thus, it is the power of the parliament to make laws providing for the classes of information referred to in clause (1) of Article 41 (supra) and the mechanism for obtaining access to that information in fulfillment of this mandate; parliament enacted the Access to Information Act in 2005.

In general, the Act reaffirms all citizens' constitutional rights to information but significantly increases access to updated information. Article 41(2) (supra) mandates Parliament to make laws that provide the classes of information referred to in Article 41 (1) (supra) and the mechanism for obtaining access to such information. The main aim of Article 41 has been transcribed into law with the pronouncement of the Data Protection and Privacy Act Cap 97, Access to Information Act of 2005, Computer Misuse Act, among others all aimed at protecting ones right to privacy.

However, the constitutional protection under Article 27 faces significant enforcement challenges that undermine its practical application. The judicial system of Uganda lacks a precedent on digital data correspondence and

[27] Constitutional Petition No.15 of 1997) [1997] UGCC 7

communication strategies thus creating a constitutional ambiguity. This, combined with the DPPA's broad national security exemptions (Section 4) justified under Article 43, permits disproportionate state surveillance, as evidenced by the 2019 Pegasus spyware incident (The Wall Street Journal, 2019).

4.3 The Data Protection and Privacy Act Cap 97

Uganda's Data Protection and Privacy Act, 2019 is the primary law regulating personal data. It grants individuals rights to access and correct their data according to sections 7 & 9 and imposes obligations on data handlers. However, the law is critically weakened by its lack of mandatory data breach notifications and trivial fines, capped at just 2% of annual turnover (Section 38). This is a fraction of the GDPR's 4% global turnover penalty, making fines an acceptable business cost, as seen in the *Sserunjogi v Guiness Transporters Ltd* (Safe Boda) case.

Furthermore, the act barely gives opportunity to individuals who withdraw their consent though it was initially given. This makes people lose control over their own data which is lost in the so called “informed consent principle” which the law claims to uphold.

This Act remains silent in regard to the management of personal data gathered without consent particularly through private surveillance tools such CCTV systems or drones which is a growing concern in an age of widespread private monitoring. Section 22(3) offers only a vague directive that data controllers must adhere to generally accepted information security practices, ‘thereby imposing heavy responsibility without furnishing practical, enforceable standards. Fake security rules permit unsafe practices like unencrypted data storage, increasing breach risks.

Furthermore, section 23 fails to pronounce clear penalties and prevents the Personal Data Protection Office from imposing meaningful sanctions, as demonstrated by its limited response to the 2024 Airtel Uganda data leak.

Having established the legal framework of the Data Protection and Privacy Act Cap 97, it is essential to examine the data protection principles enshrined within it

which form the foundation for effective implementation and enforcement of the Act.

Section 3[28] stipulates the data protection principles and it states that a data collector, data processor or data controller or any person who collects, processes, holds or uses personal data to abide and implement these principles which I will proceed and explain in detail,

The Accountability Principle; Section 3(1)(a)[29] under the DPPA cap, 97 is to the effect that the data controllers, collectors and processors shall be accountable to the data subject for the data collected, held or used, this is known as the accountability principle. The accountability principle requires the active implementation of measures by the controllers to promote and safe guard data protection in their activities.

Additionally, controllers are responsible for and be able to demonstrate compliance of their processing operations with the data protection law they should further have documentation ready which proves to the data subject and to the supervisory authorities that measures have been taken to achieve adherence to the data protection Laws.

For example, in case of a high risk, processing, the data controller must carry out a privacy impact Assessment and, in some cases, consult the competent supervisory Authority[30] .It may be possible to demonstrate compliance and comply with other obligations under the law by registering with the National Data Protection Office which has the national register for data controllers. This is depicted under section 5(1)(d)[31] which is to the effect that the National Data protection office shall register and maintain data protection and Privacy register.

The Principles of Transparency; The principle of transparency is depicted from section 3(1) (f)[32] which is to the effect that data controllers, collectors and processors shall ensure transparency and participation of the data subject in the

[28] The Data Protection and Privacy Act cap 97
[29] Ibid
[30] Ibid
[31] The Data Protection and Privacy Act cap 97
[32] ibid

collection, processing, use and holding of the personal data. The transparent processing requires that the data subject be informed of the existence of the processing operation and its purposes[33].At the time of collecting their data, people must be informed clearly about a at least ,who the controllers are ,including their contact details, and those of the data officer if any ,why the controller will be using their personal data ,the categories of the personal data concerned ,the legal justifications for processing their data ,for how long will the data be kept ,who else might receive it ,that they have a right to a copy of that data and the basic right in the data protection law[34] .

This is illustrated by Airtel when it attempted to comply with the rule of transparency, Airtel Uganda sent a text message to its subscribers about the separation and transfer of Airtel Money Business to Airtel Money Commerce and it informed the subscribers that the continued use of the service would imply that they consent to the terms and conditions and proof that the subscribers agree to the sharing of registration information with Airtel Commerce Uganda. This statement was ambiguous and unclear and hence it not meets the requirements of transparency. The telecommunication company was criticized by the Data Protection and Privacy Activists like, Unwanted witnesses and so many data protection Legal scholars.

Security Principles; The Data collectors and Data processors are supposed to observe security safeguards in respect of the data[35].The security and confidentiality of personal data are key to preventing adverse effects for data subjects these measures can be both technical or organizational. It is further depicted under section 20[36]that among the security measures, the data controllers are required to take appropriate, technical and organization measures to ensure to prevent loss, damage, destruction or unauthorized destruction or unlawful access, or unauthorized processing of the personal data. Section 23(1)[37] requires the data controller to immediately notify the National Information Technology Authority about any breach, or unauthorized access to personal data

[34] The Data Protection and Privacy Act cap 97
[35] ibid
[36] ibid
[37] ibid

Some of the security measures include, pseudonymization is one of the examples of technical and organizational measures that are recommended, and other technical measures include holding data in a secure physical environment, limit access control, logins and protecting the communications of data with strong cryptography.

Principles Of Fairly and Lawful Processing ; This is depicted under section 3 (1) (b)[38] which is to the effect that data controllers and processors shall ensure that they process and use data fairly and lawfully, in otherwise personal data can be processed if they meet the criteria provided for under the action the basis of free, specific, informed and unambiguous consent of the data subject or of some other legitimate interests laid down by the law. These are provided for example under section 7(1) (2)[39]

The Principle of Retention; The collectors, controllers and processors are supposed to retain personal data for the period authorized by law or for which the data is required. This depicted under section3 (1)(d)[40]. Section 18(1)[41] states that Subject to subsections (2) and (3), a person who collects personal data shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data is collected and process. The act stipulates the exceptions to this rule and they include among others; retention authorized by law, for lawful purpose contract between parties to the contract, consent to retention, national security and so many other exceptions depicted there under.

This principle is also known as storage limitation and it makes it necessary to delete or anonymize data as soon as they are no longer needed for the purpose for which they were collected and exceptions from the above principle must be set out by law and need special safeguards for the protection of data subject. However, there are so many insistences where different data controllers have abused this principle, for example the government of Uganda collected people's personal information like, National identification Number, phone numbers, their occupation and place of resident so that it could send them Covid-19 relief,

[38] The Data Protection and Privacy Act cap 97
[39] Ibid
[40] Ibid
[41] Ibid

This information was shared with Post-Bank Uganda which was supposed to remit the money, but up to date, the government is still retaining that personal information yet it had already served its purpose, and the National Information Technology Authority has done nothing to control this abuse yet it is its mandate. This information can be used by the government for other purposes.

The Quality Principle; This is depicted under section 3(1)(e) [42] which is to the effect that, data controllers, processors, and collector shall ensure quality of information collected, processed, used or held. Data may need to be checked regularly and kept up to date to secure accuracy. This is further depicted under section 15(1)[43] which is to the effect that data controllers, collectors and processor shall ensure that the information is accurate, complete and up-to-date. The data subject is also under an obligation under section 15(2)[44]to ensure that the collected is complete, accurate, up-to-date and not misleading.

It is hence an obligation for the data controllers holding personal data to information not to use information without taking steps to ensure with reasonable certainty that the data is accurate and this obligation must be seen in the context of the purpose of the data processing.

To illustrate, if somebody wants to conclude a credit contract with a bank, the bank will usually check credit worthiness of the prospective customer, for this purpose, there are special data bases available containing data on the credit history of private individuals. If such a data base provides incorrect or outdated data about an individual, this person may suffer negative consequences.

The question is how often do banks update their data base?

Data Minimization Principle; This is to the effect that data collectors, controllers and processors shall collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data, this is depicted under section 3(1)(c)[45].Section 14(1)[46] is more definitive about the data minimization principle. It

[42] The Data Protection and Privacy Act cap 97
[43] Ibid
[44] Ibid
[45] ibid
[46] Ibid

is to the effect that data controller or data processer shall only process the necessary or relevant personal data. The categories of the data chosen for processing must be necessary in order to achieve the declared overall aim of the processing operation. Section 14(2)[47] prohibits the processing of personal data in excess of the data which is authorized by law or required for a specific purpose.

The mandate to enforce compliance to these data protection principles is under the control of the National Information Technology Authority of Uganda as per section 3(2) of the Data Protection and Privacy Act[48] but one might ponder whether the authority has fulfilled its obligation, basing on the fact that it is a government agency ,and hence one would ponder whether it has the ability to be impartial in its investigations most especially concerning the use of personal data by the government public bodies.

It is hence vital to note that the , growing privacy concerns have prompted advocacy for tighter regulations ,in addition they have placed companies responsible for safe guarding personal data under greater scrutiny .This was depicted by the investigations that were carried out against the Guinness transport Company commonly known as a Safe Boda .The investigation was carried by NITA – U and found that Safe Boda shared users data with a US behavioral analysis company .NITA's finding was that safe Boda's disclosure of its' users Personal Data to Clever Tap contravened the Data Protection and Privacy Act cap 97. Since the "consent" relied upon for the disclosure was not specific neither were they informed, given that the users were not informed of the extent of the personal data collected and the potential disclosure of their personal data with Clever tap. The act also establishes the National Data Protection office under section4 (1)[49]which shall be headed by the National Personal Data protection director who is currently Ms. Stella Alibatesa .Section 5[50] stipulates the functions of the Data Protection office and which among others include; to oversee the implementation of and be responsible for the enforcement of the act, to promote the protection and observance of the right to the privacy and of personal data ,monitor

[47] The Data Protection and Privacy Act cap 97
[48] ibid
[49] ibid
[50] Ibid

,investigate and report on the observance of the right to privacy and of personal data and to establish and maintain a data protection register,

The office in performing its function shall have powers necessary and shall not be under the control and direction of any person or authority[51].In a persuasive case of European Commission v. Federal Republic of Germany[52], the CJEU stressed that the supervisory authorities are 'the guardians' of rights related to personal data processing. Thus, their establishment in Member States is considered "as an essential component of the protection of individuals with regard to the processing of personal data"[53].The CJEU concluded that "when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence by public authorities". Hence it is important NITAU should borrow a leaf from that persuasive decision which is not binding on Uganda but rather persuasive.

4.4.3 Data Protection and Privacy Regulations, 2021

The Data Protection and Privacy Regulations provide the specific rules, procedures, and administrative details for implementing the Data Protection and Data Privacy Act Cap 97 and these include regulations on data retention periods, procedures for registration of data collectors, processors, and controllers, and the process for handling complaints and breaches.

The Data Protection and Privacy Regulations, 2021, intended to operationalize the DPPA, fail to rectify its enforcement weaknesses. Section 14(1) neglects to define specific data retention timelines, permitting entities like Post Bank to hold personal information indefinitely. Furthermore, the Regulations omit protections for marginalized groups, as Article 30 and Schedule 3 lack safeguards for persons with disabilities or intersex individuals, undermining equitable enforcement.

[51] The Data Protection and Privacy Act cap 97
[52] CJEU, C-518/07, European Commission v. Federal Republic of Germany [GC], 9 March 2010, para. 27
[53] Ibid

4.4 Computer Misuse (Amendment) Act, 2022

The Uganda Computer Misuse Act passed in 2011 with the goal of improving safety and security in the increasingly digitalized world. This includes preventing unauthorized access, abusing, or misusing computers and information systems, as well as protecting electronic transactions. But this law has been used in a variety of ways over the years to stifle digital rights, such as the freedom of speech and the ability to obtain information. Academic and social critic Dr. Stella Nyanzi, for example, was arrested for defaming the president on social media in 2019, she was convicted of cyber harassment contrary to section 24 [54]of the Act but acquitted of offensive communications, which is prescribed under section 25[55] she was given an 18-month prison sentence, but the Court of Appeal cleared her, ruling that the trial magistrate lacked the authority to convict her of cyber harassment and that the prosecution's evidence was insufficient. Other victims of the same law include author Kakwenza Rukirabashaija, who was arrested, the comedy group Bizonto, who were arrested for allegedly offensive and sectarian posts, and former presidential candidate Henry Tumukunde, who was arrested for allegedly making reasonable statements in radio and television interviews, convicted and imprisoned for sending offensive messages against president Yoweri Kaguta Museveni and his son Muhoozi Keinerugaba.

Before being sent to the Parliamentary Committee on Information and Communications Technology for review and public comment, the Computer Misuse (Amendment) Bill, 2022, a private member's bill, was first introduced in Parliament in July 2022. Proponents of the bill contended that current laws "are not adequate to deter the vice" or "do not specifically address regulation of information sharing on social media.". One of the amendment's stated goals is to improve the rules regarding unauthorized access to data or information, prohibits the sharing of any information relating to a child without authorisation from a parent or guardian, prohibits the sending or sharing of information that promotes hate speech, prohibits the sending or sharing of false, malicious and unsolicited information,

[54] Computer misuse(amendment) act 2022
[55] ibid

and to restrict persons convicted of any offence under the Computer Misuse law from holding public office for a period of 10 years.

The computer Misuse Act has really wide-ranging rules that make it even harder to enforce the DPPA properly because it lets the government grab personal data without much real checking. There is no straightforward way to sort out the clashes either so regular people end up exposed to privacy invasions from very authorities supposed to protect them.

4.5 Institutional Framework of data protection and privacy in Uganda

4.5.1 The Personal Data Protection Office

The Personal Data Protection Office (PDPO) in Uganda sits under NITA-U but is supposed to operate independently. It's the go to body for enforcing Data Protection and Privacy Act Cap 97 as laid out in sections 4 and 5 of the 2021 regulations. They've been active especially after the 2022 data breach at the Uganda securities Exchange. The incident showed just how shaky the stock market's data systems were, so the PDPO gave USE a strict three-month deadline to fix the technical problems and on top of that they have linked agreements with the Uganda Communications Commission and the NGO Registration Board to tighten up data protection across different sectors.

Notwithstanding the endeavours to fortify data protection frameworks, a number of obstacles persist, including individuals' ignorance and incomprehension of their data protection rights. Numerous people are unaware of their rights as owners of personal data, and organizational comprehension of data protection issues varies widely. Furthermore, the true expenses of putting data protection compliance tools into practice are frequently unknown, especially in settings with lax technological regulatory frameworks, which renders their implementation phantom.

As an individual, data protection and privacy are important to you because they help safeguard your identity and finances from being accessed or used without your consent.

By understanding your rights and the laws in place, you can take steps to protect yourself and ensure your personal data is kept safe.

Some of the tips to help protect your data and privacy by the PDPO include;

Being cautious about sharing personal information online or with unfamiliar organizations.
Reviewing the privacy policies of the apps and websites you use, and adjust your privacy settings accordingly.

Using strong, passwords for your accounts and enable two-factor authentication whenever possible.

4.5.2 National Information Technology Authority Uganda (NITA-U)

This body is obligated to implement the Data Protection and Privacy Act, 2019. However, its effectiveness is hampered by insufficient funding and technical capacity. Furthermore, the Personal Data Protection Office lacks autonomy as it operates under NITA-U, making it vulnerable to political interference.

4.5.3 Ministry of Information and Communications Technology and National Guidance

The ministry formulates overarching ICT policy and integrates data protection into national digital strategies. However, its effectiveness is constrained by inadequate funding and poor coordination with NITA-U. Critically, the Ministry has not updated the Data Protection and Privacy Act, 2019 to address emerging threats like AI profiling and biometric data misuse, leaving the legal framework outdated.

4.5.4 Uganda Communications Commission (UCC)

This entity regulates the telecommunications sector, enforcing data protection rules through operator licenses. However, it’s rendered ineffective by the Data Protection and Privacy Act, 2019, which lacks robust cybersecurity mandates. This resulted in limited enforcement following the 2024 Airtel data leak, demonstrating the law's inadequate penalties.

4.5.5 Judiciary

Uganda's judiciary interprets the Data Protection and Privacy Act, 2019 and adjudicates privacy violations, thereby setting legal precedents and overseeing state and private actors. However, its effectiveness is hampered by case backlogs, a shortage of judicial expertise in technology, and limited public access to justice, which collectively delay redress for data breach victims.

4.5.6 Conclusion

Though the Uganda Data Protection and Privacy Act 2019 established a significant framework, its implementation is limited by fake provisions, weak penalties, and an under-resourced, non-independent regulator. This creates inconsistent protection, disproportionately affecting rural and marginalized communities. Closing these gaps requires legal reforms, institutional strengthening, and public awareness campaigns.

CHAPTER FIVE
SUMMARY OF MAJOR STUDY FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

This chapter synthesizes the findings from the preceding chapters to evaluate the effectiveness of the Data Protection and Privacy Act, Cap 97 (DPPA) in safeguarding the right to privacy in Uganda.

5.1 Summary of Major Study findings

Data analysis reveals that Uganda's Data Protection and Privacy Act, 2019 provides a solid legal foundation aligned with international standards like the GDPR. However, its effectiveness is severely limited by weak enforcement, indefinite exemptions, and a lack of regulatory independence. The law's benefits are disproportionately enjoyed by urban populations, while rural communities containing a population of 70% are largely excluded. Systemic vulnerabilities are evidenced by major data breaches at NIRA (2019) and Airtel (2024), and a mere 200 complaints filed with NITA-U in 2025, indicating low public awareness and trust. Opportunities for enhancement include adopting privacy-enhancing technologies like blockchain and forging international partnerships for capacity building.

5.2 Conclusions

The 2019 Data Protection and Privacy Act in Uganda represents a significant legal achievement, operationalizing constitutional privacy rights and establishing a rights-based framework. However, its real-world impact is severely limited. A deep digital divide and communal traditions restrict its reach in rural areas, while institutional weaknesses like under-funded NITA-U and a non-autonomous Personal Data Protection Office make implementation difficult. Consequently, the law primarily protects urban, digitally-literate citizens, failing to curb systemic issues like mass surveillance and data breaches. Effective protection requires a holistic strategy that simultaneously strengthens legal enforcement, bridges socio-economic gaps, and boosts public awareness.

5.3 Recommendations

Institutional capacity should be strengthened through expanding the annual budget to at least 10 billion UGX drawn from national ICT allocations to endorse upgrades and strengthen compliance tracking mechanisms for example through planting offices in Gulu, Mbarara and Mbale before 2028 which will significantly improve service delivery and redress avenues for data subjects residing in remote areas.

A special five-member tribunal should be created to handle complaints and assist the Director of Public Prosecutions in bringing to justice criminals involved in data breaches. The tribunal should comprise five members with expertise in ICT law, human rights and cybersecurity, appointed through a transparent process by the judicial service commission.

Data protection officers should be trained on how to preserve information through NITA- U's partnerships with international bodies like the European Data Protection Board. This will help address current AI needs and skill gaps.

Revise Legal Provisions through establishing a privacy review board, comprising judges and civil society representatives to approve surveillance requests with 48 hours, increasing fines and prison sentence terms for criminals involved in data breaching.

NITA-U and the Personal Data Protection Office should launch various public awareness campaigns across different cultures targeting 60% public recognition by 2028. This involves training 30,000 rural residents annually through Civil Society Organizations' partnerships and releasing a breach-reporting mobile app for one million users within urban settings by 2027.

Uganda must enact whistleblower protection laws by 2026 to combat unwarranted surveillance and corruption. Mandatory parliamentary reporting on surveillance warrants and an independent anti-corruption unit within the Personal Data Protection Office are essential to ensure impartiality and uphold the right to digital privacy as affirmed by UN General Assembly Resolution 68/167 (2014).

BIBLIOGRAPHY

BOOKS

Westin A F, Privacy and Freedom (Atheneum 2017)

Solove D J, Understanding Privacy (Harvard University Press 2008)

Lyon D, Surveillance Society: Monitoring Everyday Life (Open

University Press 2001)

Halsbury's Law of England, 'The Data protection principles and the seventh Data

Protection Principles, Confidence and Data Protection' volume 8(1) (2018).

Bygrave L, Data Privacy Law: An International Perspective (Oxford University Press 2014)

Sanjay S, Data Privacy and GDPR Handbook (Wiley 2022)

Westin, A; Privacy and Freedom New York NY, Atheneum 2017.

Black's law dictionary 11th Edition.

JOURNAL/ ARTICLES

Warren S D and Brandeis L D, The Right to Privacy (1890) 4 Harvard Law Review 193

Van der Hoeven W, The Harm of Privacy Violations in Information Privacy in the Digital Age (Springer 2012)

Meacham D and Shasha J, Database Access Control and Encryption Techniques for Privacy in Proceedings of the International Conference on Data Protection (2009)

Richard, Holis. 'Data security part 1 five factors leading to Data Compromise Privacy and Data Protection', Volume 10, Issue 2, December 2018.

Cuijpers A, De Hert P, and Gurtwirth S, A Private Law Approach to Privacy: Mandatory Law Obliged (2015)

De Hert P and Gurtwirth S, Data Protection and Privacy Law (2009)

Schermer B, Custers B, and Van der Hof S, The Ethics and Practicalities of Consent in Data Protection (2015)

Cowan Z, The Private Man (1970) 24 Inst Pub Affairs Rev

Betty Ndagire Daily Monitor "Personal Data Protection still low" Saturday, February/ 04/2023

Unwanted witness analysis of the Data Protection and Privacy Act, page 9

UN General Assembly Resolution 68/167 (2014) - *The right to privacy in the digital age*

UNPUBLISHED WORKS AND REPORTS

NITA-U (2023), Annual Report on Data Protection in Uganda

Makulilo A B, Privacy and Data Protection in Africa: A State-of-the-Art International Privacy Law (2012) Vol 2

Kyogabirwe L (2022), Safeguarding Digital Rights in Africa's Growing Digital

ONLINE RESOURCES

American Civil Liberties Union (ACLU), Brandon Mayfield (2004) https://www.aclu.org accessed 27 April 2025.

Rinsloo, P., & Kaliisa, R. (2024). Comparative Analysis of Data Protection Regulations in East African Countries. Emerald Insight. https://www.emerald.com/insight/content/doi/10.1108/dprg-06-2024-0120/full/html accessed 28 April 2025.

Privacy and personal data protection in Africa Advocacy toolkit https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Privacy_and_personal_data_protection_in_Africa_advocacy_toolkit.pdf accessed 11 May 2025

National Information Technology Authority Uganda (NITA-U) Data Protection & Privacy Notice https://www.nita.go.ug/services-and-guidelines/data-protection-and-privacy accessed 11 May 2025

September 2018 CIPESA Challenges and Trends in Uganda Privacy and Personal Data Protection: https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Uganda-2018.pdf accessed 13 May 2025.

What is data privacy?https://searchcio.techtarget.com/definition/data-privacy-information-privacy

GDPR in practice Experiences of data protection authorities https://fra.europa.eu/en/news/2024/lack-resources-undermine-eu-data-protection-enforcement accessed 16 May 2025

Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 updatehttps://fra.europa.eu/en/publication/2023/surveillance-update accessed 06 June 2025

In a world increasingly dependent on digital systems https://genevasolutions.news/science-tech/as-itu-turns-160-our-interconnected-world-needs-cooperation-more-than-ever accessed 23 June 205

New study exposes data protection challenges in Uganda https://observer.ug/news/new-study-exposes-data-protection-challenges-in-uganda/ accessed 26 May 2025

The OECD privacy and personal data protection guidelines https://www.bitraser.com/article/oecd-guidelines-privacy-personal-data-protection.php?srsltid=AfmBOooVY_hwgTAEbRjBz-ZzMmb9PEBeptN1KIrmPme-6feo_DkH_DtT accessed 23 May 2025

African Union's Convention on Cyber Security and Personal Data Protection also known as Malabo Convention published 15th of June , 2023. https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/ accessed 24 May 2025

African commission revised Declaration of Principles of Freedom of Expression and Access to Information in Africa https://www.chr.up.ac.za/tech4rights-news/2056-african-commission-publishes-revised-declaration-of-principles-of-freedom-of-expression-and-access-to-information-in-africa-amid-covid-19-crisis#:~:text=As%20a%20case%20in%20point%2C%20in%20South,virus%20through%20means%20such%20as%20contact%20tracing. Accessed 10 may 2025

The Wall Street Journal Report about Huawei helping the government to hack Hon Kyagulanyi's WhatsApp and skype communications by Nile Post published on Thursday August 15th 2019 https://nilepost.co.ug/news/52067/wsj-reports-huawei-helped-uganda-government-to-hack-bobi-wines-whatsapp-skype-conversations accessed 15 July 2025

Sserunjogi v Guinness Transporters limited Ta safe boda [Labour Dispute Reference 47 of [2022] [2024] UGIC 49(16 August 2024) https://www.kaa.co.ug/safeboda-has-been-investigated-on-allegations-of-unlawful-sharing-of-users-personal-data/ accessed 6 August 2025

Muruhura Comfort

AN EVALUATION OF THE EFFECTIVENESS OF THE DATA PROTECTION AND PRIVACY ACT IN PROTECTING THE RIGHT...

Quick Submit

Quick Submit

Uganda Christian University

Document Details

Submission ID
trn:oid:::1:3426696906

Submission Date
Nov 28, 2025, 1:45 PM GMT+3

Download Date
Nov 28, 2025, 1:58 PM GMT+3

File Name
MURUHURA_COMFORT_RUTAYA_LLB_THESIS.docx

File Size
290.2 KB

58 Pages

13,858 Words

81,419 Characters

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

Muruhura Comfort

AN EVALUATION OF THE EFFECTIVENESS OF THE DATA PROTECTION AND PRIVACY ACT IN PROTECTING THE RIGHT...

Quick Submit

Quick Submit

Uganda Christian University

Document Details

Submission ID
trn:oid:::1:3426696906

Submission Date
Nov 28, 2025, 1:45 PM GMT+3

Download Date
Nov 28, 2025, 1:57 PM GMT+3

File Name
MURUHURA_COMFORT_RUTAYA_LLB_THESIS.docx

File Size
290.2 KB

58 Pages

13,858 Words

81,419 Characters

26% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

219 Not Cited or Quoted 25%
Matches with neither in-text citation nor quotation marks

9 Missing Quotations 1%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

21% Internet sources
17% Publications
15% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.