EVALUATING THE ETHICAL IMPLICATIONS OF MASS SURVEILLANCE ON INDIVIDUAL RIGHTS IN UGANDA

SHAFICK SSEKANDI

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

May, 2025

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, Shafick Ssekandi, declare that this dissertation is my original work and has not been submitted for a degree or diploma at any university or institution of higher learning. All sources of information used in the dissertation have been duly acknowledged.

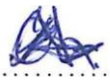
Signed:  .....

SHAFICK SSEKANDI

Date: 22/05/2025.....

APPROVAL

This dissertation has been prepared under my close supervision and guidance as the University supervisor.

SIGNATURE  .....

MR. DANIEL KISA

DATE 9.5.2025.....

DEDICATION

I dedicate this research paper to the following people who have ensured that my education is a success.

I sincerely express my gratitude toward my supervisor Mr. Daniel Raymond Kisa for the great work he has done in supervising my research work without giving me any hardship and ensuring that this research is complete and a success. I therefore pray that God blesses him and the works of his hands now and always.

I am profoundly honored and exceedingly humbled to express my gratitude towards my beloved Father Hajji Weraga Haruna and Mother Hajjat Ssanyu Aidah who have been able to finance my academics throughout my education. May the good Lord bless them abundantly and also bless the work of their hands.

ACKNOWLEDGMENT

I wish to express my sincere gratitude to the following people because this work would not have been possible without them.

I wish to thank the Almighty God who has given me knowledge, wisdom, life and protected me throughout my academic struggle.

My gratitude goes to my supervisor Mr. Daniel Raymond Kisa for his support and dedication in making everything possible as far as this research paper is concerned. I also extend my appreciation to the Faculty of Law at Uganda Christian University for equipping me with the tools necessary for academic and professional growth. Special thanks to my family and friends for their unwavering encouragement and support throughout this journey.

ABSTRACT

This dissertation explores the ethical implications of mass surveillance on individual rights in Uganda. With the increasing digitization of society, governments are implementing surveillance technologies ostensibly to ensure national security, in Uganda; these efforts have raised concerns regarding the protection of privacy, data security, and civil liberties. The study investigates the extent of surveillance, assesses its impact on individual freedoms, and evaluates the existing legal and ethical frameworks. Using a qualitative research methodology, the research analyses laws such as the Computer Misuse Act (2011),the Regulation of Interception of Communications Act (2010),and Ant-Terrorism Act (2002),and juxtaposes these against human rights principles. Findings show that while surveillance has benefits, such as crime prevention, it often lacks oversight, transparency, and accountability, leading to abuses of power. The study concludes that Uganda's current surveillance regime disproportionately prioritizes state security over individual rights, creating an ethical imbalance. Recommendations include strengthening legal safeguards, judicial oversight and enhancing public awareness on digital rights.

Table of Contents

1.0 CHAPTER ONE

1.1 INTRODUCTION

The government of Uganda demonstrated a strong curiosity about obtaining this information and applying it for unidentified purposes, despite claiming that it was using it for national security motives. Digital technologies transformed our daily lives by producing incredibly detailed records.1 This study examined Uganda's widespread use of digital surveillance and the right to privacy. The nature of surveillance, the origins of widespread digital surveillance, the right to privacy2 were all examined, mass digital surveillance, whether it's legal, the consequences of mass digital surveillance and the recommendations.

1.2 BACKGROUND

Many African governments have established legislations Uganda inclusive like, The Computer Misuse Act 20113, Electronic Transactions Act 20114, and Electronic Signatures Act 20115. Meanwhile, most of the laws are seen by people as a way of restricting their rights. Following the controversial 2011 re-election of President Yoweri Museveni, the state violently suppressed the protests that were led by Dr.Kizza Besigye, killing at least nine unarmed civilians, injuring over 100 and

[1] Neil M Richards, "The Dangers of Surveillance " https://harvardlawreview.org accessed 15th April,2025
[2] Article 27 of The Constitution of the Republic of Uganda 1995
[3] The Computer Misuse Act 2011
[4] Electronic Transactions Act 2011
[5] Electronic Signatures Act 2011

arresting hundreds. The government launched Operation “Fungua Macho (Open Your Eyes)” in Swahili to spy on opposition leaders, journalists, and government insiders using advanced malware.

The Ugandan Chieftaincy of Military Intelligence (CMI) and Uganda police force (UPF) purchased and deployed Fin Fisher malware from Gamma International GmbH (

At the same time, there is growing concern among some members of the public regarding the compulsory SIM card registration and the national ID initiative managed by the National Identification and Registration Authority. These individuals fear that the personal data gathered through these processes could potentially be misused by the government for surveillance purposes.6

In the 21st century, the intersection between national security and individual privacy has become a defining issue for states navigating technological advancement. Around the world, governments are increasingly turning to surveillance as a tool for law enforcement, intelligence gathering, and crime prevention. Uganda is no exception.

The push for more mass digital surveillance in Uganda gained more momentum following a series of high profile security incidents. Among these was the attempted assassination of General Katumba Wamala in June 2021, during which his daughter and driver were tragically killed. Similar incidents involving targeted killings of high ranking security officers and politicians created an atmosphere of insecurity and panic. In response, President Yoweri Kaguta Museveni announced stringent measures

[6] https://www.unwantedwitness.org/unlawful-sim-card-validation-exercise-is-a-threat-to-anonymity-and-privacy/#:~:text=One%20of%20such%20measures%20is%20the%20SIM,to%20abuse%20without%20collection%20and%20protection%20safeguards. accessed on 15th April,2025

to improve surveillance and state intelligence capabilities. The government subsequently engaged in a contract with Joint Stock Company Global Security, a Russian firm, to supply and implement an extensive vehicle tracking system throughout the country.

The ITMS as introduced mandated that all vehicles, motorcycles and boats be fitted with tracking devices connected to a centralized command center under government control. This system enables authorities to monitor, in real time, the movement of citizens and vehicles across Uganda's territory. Although framed as a tool for fighting violent crime and terrorism, the program essentially grants the state an unprecedented level of access to the daily movements of millions of Ugandans.

From a human rights perspective, this development raises critical questions. The right to privacy enshrined under Article 277 which prohibits unlawful searches and guarantees the confidentiality of private correspondence, communication and property.

Uganda is also a party to several international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples Rights, both of which affirm the right to privacy. Domestically, The Data Protection and Privacy Act, and the Data Protection and Privacy Regulations, 2021, aim to safeguard personal data, establish principles of lawful processing, and provide mechanisms for data subject consent and redress.

[7] The Constitution of the Republic Of Uganda 1995

Critics argue that the mass collection of data without adequate legal oversight or judicial review contravenes both domestic and international human rights standards.

Another major concern is the political context in which these surveillance measures are being implemented. Uganda has a long standing record of suppressing political opposition and civil society activism through both legal and extra judicial means. In this environment, there is a real risk that surveillance technologies could be used not just for legitimate security purposes, but also to monitor, intimidate, and silence critics of the regime.

Regionally, Uganda's adoption of mass surveillance technologies reflects a broader trend across Africa, where governments are increasingly leveraging digital tools to monitor populations. While such technologies can play a role in public safety, their deployment without robust legal frameworks and democratic safeguards risks entrenching authoritarian practices and eroding fundamental rights.

In conclusion, as Uganda continues to embrace digital transformation, it is imperative that surveillance technologies be governed by principles that honor the inherent value of human life and democratic principles. Ensuring a proper coordination between national safety and individual confidentiality is crucial for safeguarding human rights and fostering a free and open society.

1.3 PROBLEM STATEMENT

The Ugandan government implemented extensive surveillance measures, citing national security and crime prevention as justification. However, concerns were raised about the ethical considerations of such surveillance, including potential misuse of collected data, infringement on citizens' rights, and lack of robust legal safeguards. This research analyzed the ethical dilemmas posed by mass surveillance in Uganda and its effect on individual privacy rights.

1.4 OBJECTIVES OF THE STUDY

1.4.1 GENERAL OBJECTIVE

To evaluate the ethical implications of mass surveillance on individual privacy rights in Uganda.

1.4.2 SPECIFIC OBJECTIVES

To examine the extent and nature of mass surveillance and what legal and policy frameworks exist to govern the surveillance in Uganda?

To assess the effect of surveillance on individual privacy rights and other freedoms.

To propose recommendations for balancing national security and privacy rights.

1.5 RESEARCH QUESTIONS

What are the main surveillance mechanisms used and what legal protections exist to regulate such surveillance in Uganda?

How does mass surveillance affect individual privacy rights and civil liberties?

How can Uganda attain harmony between security and personal privacy?

1.6 SIGNIFICANCE OF THE STUDY

This research enhanced the ongoing discussion on privacy and monitoring by providing comprehensive analysis of Uganda's surveillance landscape. The findings proved valuable to policy makers, human rights activists, and legal scholars in shaping ethical and legal frameworks that protect privacy while addressing security needs.

1.7 JUSTIFICATION OF THE STUDY

This research is justified by the increasing use of mass surveillance in Uganda and its impact on privacy rights .It examined the legal gaps and balance between security and personal freedoms .The findings informed policies to ensure ethical surveillance while protecting human rights.

1.8 HYPOTHESIS

Mass surveillance policies in Uganda priory's national security over individual privacy, creating an ethical dilemma between state interests and human right

1.9 SCOPE OF THE STUDY

This research generally emphasized mass surveillance by the government on the population and the effects it has on the freedoms of people in Uganda especially in the central region.

1.10 TIME SCOPE

The study focused on the mass surveillance by the government and its implications on the rights of the people in Uganda between 2011 to present times.

1.11 LITERATURE REVIEW

During the research, a compilation of literature will be required, which will consist of textbooks, articles, journals, and other pertinent materials related to the topic. This compilation will be created by examining the author, the title of the book, the publisher, the location of publication, and the year of publication for each piece of literature.In an article by "The East African" headed "Scrap surveillance system, HRW tells Uganda" 8concerns regarding Uganda's Intelligent Transport Monitoring System (ITMS). HRW asserts that this system, which enables immediate tracking of all in the country, infringes on confidentiality rights and poses threats to freedoms of association and expression. However the article does not incorporate perspectives that will have access to the data, and what safeguards are in place to prevent misuse is crucial. This is particularly important considering past instances where private

[8] The East African " Scrap surveillance system, HRW tells Uganda" https://www.theeastafrican.co.ke >accessed on 15th ,April,2025

companies mishandled personal data, as seen in the case of Safe Boda unlawfully sharing clients' data with a US company.

The DW Akademie[9] The article "If surveillance is a daily thing, people start to think twice before going online" offers a valuable perspective on the psychological and behavioral consequences of mass surveillance. While it brings much needed attention to the chilling effects of surveillance, a closer examination reveals several strengths, limitations, and gaps that merit discussion. The article effectively captures the voices of individuals and experts who have directly experienced or studied digital surveillance, adding a personal and relatable dimension to the topic.

Focus on the chilling effect; it convincingly outlines how constant surveillance deters free expression, particularly in authoritarian contexts. This helps highlight a crucial yet often overlooked consequence of surveillance.

The article also touches on surveillance in different geopolitical contexts, showing that the issue transcends borders and affects both democratic and authoritarian states.

However, while the article makes strong claims about the behavioral impact of surveillance, it lacks empirical data or statistical evidence to support its assertions. For instance, the extent to which online activity decreases in monitored environments is not quantified, which limits the articles credibility in academic contexts.

The article also tends to generalize the psychological effects of surveillance without adequately considering demographic, cultural, or regional differences. Not everyone

[9] https://akademie.dw.com accessed 18th April ,2025

responds to surveillance in the same way, and factors such as education, digital literacy, and socio economic status may influence individual behavior.

Although the article hints at the role of the state and corporate actors, it does not thoroughly examine the legal frameworks that permit or regulate surveillance. This leaves a significant gap in understanding the structural enablers of digital monitoring.

The article offers the problem of surveillance convincingly but offers few concrete recommendations or solutions .There's no mention of digital rights advocacy, privacy enhancing technologies, or legal reforms that could address these issues.

" No To Big Brother : The Legality and Implications of Mass Digital Surveillance in Uganda"10 The article provides a thorough legal critique of Uganda's plan to implement mass digital surveillance through vehicle tracking systems, justified as a matter of national security. It examines the legal from work, especially the Constitution, Data Protection and Privacy Act, and international treaties. The author concludes that Uganda's proposed mass surveillance would be unconstitutional, unjustifiable in a democratic society, and lacking legal safeguards.

Despite its strengths, the article has a few notable gaps; there is little discussion on how the existing data protection frameworks are actually enforced in Uganda (e.g. resources, institutional challenges, capacity).

[10] Nasser Nkonge ," No to Big Brother: The legality and implications of mass digital surveillance in Uganda" https://iuea.ac.ug/ accessed 15th April, 2025

Although the article recommends targeted surveillance, it does not flesh out concrete proposals, such as community based intelligence, judicial oversight mechanisms, or technical standards for lawful interception.

The article gives little discussion on how the existing data protection frameworks are actually enforced in Uganda for example institutional challenges.

The article doesn't also present quantitative evidence or case studies from Uganda to support claims for example crime rates before and after SIM registration in Uganda.

The article titled COVID 19 Surveillance in Kenya and Uganda is Reducing Peoples Rights 11examines how government surveillance practices during the pandemic seriously undermined basic rights like privacy, the right to information access and freedom of expression. Throughout COVID-19 pandemic, Kenya and Uganda, like many other nations, ramped up surveillance efforts to monitor and curb the transmission of the virus. These efforts included digital contact tracing, biometric surveillance and partnerships with telecom companies to track individual's movements.

International human rights law permits such actions during emergencies, but only if they are legal, necessary, and proportionate. The report argues standards were not met in either country.

Kenya and Uganda collected sensitive personal data without establishing clear rules or oversight mechanisms. There was little to no transparency about how data was gathered, stored, or used. Though all countries had data protection laws on paper,

[11] COVID 19 Surveillance in Kenya and Uganda is Reducing Peoples Rights https://www.article19.org accessed on 19th April,2025

their enforcement agencies were either non-existent or lacked independence or resources. This left the public vulnerable to abuse of their data.

However the article is advocacy driven and lacks real-world examples or quantitative data.it does not provide victim stories or testimonies, reports on how many people were monitored etc. Without empirical data it's hard to assess the magnitude or real-life impact of surveillance systems.

The article doesn't analyze whether certain groups were more targeted such as political opposition, human rights defenders or journalists and the psychological, social and economic impact of being monitored. This overlooks how surveillance disproportionately harms already vulnerable or marginalized groups.

The article also only discusses surveillance during COVID 19 with no examination of whether emergency surveillance measures were reversed, institutionalized or expanded post-COVID and whether such surveillance is becoming the new norm. Therefore the article fails to address the danger of "function creep" –where surveillance introduced for a crisis becomes permanent.

The article titled "State Seeks Court Approval to Hack Dr.Kizza Besigye's Phone" 12reports that the government of Uganda has requested the Nakawa Chief Magistrates Court to allow them to access and retrieve electronic information from the mobile phones of imprisoned opposition leader Dr. Kizza Besigye and two of his colleagues. Officials claim that the information stored on these devices may be crucial for constructing a treason case against the individuals.

[12] ADMINI " State seeks Court Approval To Hack Dr. Kizza Besigye's Phone" March 10th ,2025 >https://theinsider.ug accessed on 19th April,2025

This development raised significant concerns regarding surveillance practices and how they affect fundamental freedoms, particularly the entitlement to personal privacy. Nonetheless, the article mentions that the state is seeking judicial authorization to access Dr.Kizza Besigye's phone but fails to elaborate on:

The article doesn't also show us whether the application meets constitutional thresholds of necessity, proportionality, and legality and what standard or precedents the court might use to assess such a request.

Without this, the article misses a vital opportunity to inform the public about the limits (or lack thereof) of state power in surveillance.

The article reports the states intention to access Besigye's phone, it does not mention Article 2713 that safeguards the right to privacy. It also does not refer to International treaties like the ICCPR or African Charter on Human and Peoples Rights that Uganda is a signatory to. This absence is critical, especially in a country where digital surveillance is growing. The public deserves clarity on how such actions align with their constitutional rights.

The article does not also talk about who oversees the surveillance process and ensures it isn't abused.it also does not clarify whether the Ugandan intelligence agencies are subject to independent judicial or parliamentary oversight. Surveillance without accountability mechanisms opens the door to abuse especially in politically sensitive cases like this.

[13] The Constitution of The Republic of Uganda 1995

While this article raises an important and urgent issue, it ultimately lacks depth in its legal, human rights, and contextual analysis.it misses key opportunities to interrogate the legitimacy, proportionality, and political effects of surveillance in the country. A more comprehensive approach would have enriched public understanding and enhanced its journalistic value.

In conclusion, while the above literature sheds light on critical issues surrounding mass surveillance in Uganda, addressing these gaps would provide a more balanced and actionable analysis. Incorporating diverse perspectives, examining legal frameworks, detailing implementation processes, contextualizing within broader surveillance practices, and offering constructive recommendations would significantly strengthen the literature's impact and credibility.

1.12 RESEARCH DESIGN

The research preferred the qualitative method of analysis over quantitative because it gives in depth exploration of perceptions and experiences (allows for a deep understanding of how individuals perceive, experience and respond to mass surveillance) which might not be evident in quantitative data.

CONCLUSION

In conclusion, while mass surveillance helps prevent crimes, the research aims at evaluating the ethical implications of mass surveillance on individual rights in Uganda.

2.0 CHAPTER TWO

2.1 METHODOLOGY

The chapter explains the approach to research that was utilized to investigate the ethical implications of mass surveillance on individual rights in Uganda. The methodology outlines the design, approach, demographics, sampling methods, data gathering tools, data quality assurance, measurements, and analytical processes, while also reflecting on the specific contextual sensitivities of researching state surveillance in Uganda.

2.2 Research Design

The research employed both descriptive and exploratory research methodologies. The descriptive aspect focused on documenting the nature, extent, and characteristics of mass surveillance mechanisms in Uganda such as CCTV camera networks, PS vehicle trackers, biometric registration, and SIM card surveillance. For instance, Uganda's use of license plate recognition cameras in urban centers were documented examples of surveillance infrastructure.

The exploratory aspect facilitated a deeper investigation into emerging ethical concerns around surveillance practices especially those not explicitly addressed in current Ugandan law. For example, while the Regulation of Interception of

Communications Act (2010)14 provided for some regulation of state supervision, its enforcement and accountability mechanisms remain largely unexplored, thus necessitating empirical insights from civil society and legal experts.

The design did not seek to test a statistical hypothesis but rather to uncover nuanced insights into how mass surveillance is impacting fundamental rights like privacy, freedom of expression, and association in Uganda.

2.3 Research Approach

A qualitative research approach was employed. This approach enabled a rich and contextual understanding of subjective experiences, ethical concerns, and legal perspectives that couldn't be captured through numerical or statistical data. Unlike quantitative surveys that use closed questions, qualitative interviews allow participants to express personal experiences such as being afraid to attend protests due to surveillance which offers depth and complexity to the research.

This approach was especially appropriate given the sensitive and political nature of mass surveillance. Many individuals affected by or familiar with government surveillance couldn't feel safe discussing their experiences in rigid quantitative formats. Through semi structured interviews, participants were encouraged to narrate their experiences and opinions in a safe and guided environment.

[14] Regulation of Interception of Communications Act (2010)

2.4 Geographical Area of Study

The research was conducted in the Central Region mainly Kampala City .This area was strategically selected for relevance of this topic. Kampala is an administrative and political capital, hosting the Uganda Communications Commission (UCC), Ministry of ICT, National Guidance, Uganda Police Force, and major media and civil society offices. It is also where state surveillance technology like CCTV traffic cameras and biometric digital ID verification terminals are concentrated.

2.5 Study Population

The study's target population consisted of individuals and institutions that were either directly impacted by surveillance or had expert knowledge in the field .This included:

Human rights defenders e.g. Unwanted Witness

Journalists from independent media houses such as Next Media.

Legal practitioners and scholars from Uganda Law Society and academic institutions

Citizens who have encountered government surveillance directly (e.g. activists monitored during protests, boda boda riders fitted with trackers)

This population provided legal, ethical, and experiential perspectives.

2.6 Sampling Strategies

Given the limited accessibility and sensitivity of participants in surveillance related issues, the study utilized:

Purposive sampling was used to select participants with critical knowledge or exposure to surveillance, such as lawyers who had handled privacy related litigation, or journalists whose phones were tapped during 2021 elections.

Snowball sampling allowed the researcher to identify hard to hard reach participants through referrals, especially in cases where individuals feared being publicly associated with surveillance discourse.

2.7 Data Collection Methods

Instruments

A document review checklist was used to analyze legal statutes, NGO reports, government policies, and media publications relevant to the surveillance.

Secondary sources including the Ugandan laws e.g., The Regulation of Interception of Communications Act (2010), Computer Misuse Act (2011), and The Anti-Terrorism Act (2002), National Policy papers, government reports, Findings by global human rights bodies like Human rights Watch and Privacy International, academic journals, conference papers, and relevant digital archives were reviewed and coded for thematic analysis.

This helped contextualize Uganda's legal and ethical environment in the global surveillance discourse.

Data Analysis

The qualitative data underwent analysis using thematic content analysis.

Transcripts and notes were coded and organized into themes such as privacy violations, legal gaps, state accountability, ethical concerns, and human rights implications.

Doctrinal analysis involved comparing Ugandan legal provisions in accordance with global human rights norms.

2.8 Ethical consideration

Researching state surveillance was inherently sensitive and ethically delicate. This study adhered strictly to ethical guidelines to ensure participant safety and moral integrity.

3.0 CHAPTER THREE

GOVERNMENT SURVEILLANCE MECHANISMS AND LEGAL PROTECTIONS IN UGANDA

3.1 Introduction

In recent years, Uganda has significantly expanded its surveillance infrastructure. Driven by political, security, and socio-economic factors, the government has implemented a wide array of surveillance mechanisms, often justified as necessary for public security. However, these efforts have raised critical questions about privacy, human rights, and the legal framework. This paper examines the major surveillance mechanisms employed by the Ugandan government, the legal frameworks intended to regulate them, and provides a critical assessment of their effectiveness and limitations.

3.2 Main Surveillance Mechanisms used by the Ugandan Government

3.2.1 CLOSED –CIRCUIT TELEVISION (CCTV)

The CCTV monitoring system was set up in 2007 in anticipation of the Commonwealth Meeting. This system was deployed in the streets of Kampala and Entebbe, focusing

on the major intersections and junctions along the routes used by the delegates; however, its effectiveness has been called into question.15

In response to the rise of violent murders in and around the Kampala metropolitan area, as well as in other regions of the country in 2017, the President mandated the placement of CCTV cameras on major roads, in towns, and across cities nationwide to aid in crime prevention. The setup of these CCTV cameras in Kampala commenced in July 2018.16 .

The installation of CCTV surveillance security cameras was premised on helping the Uganda Police Force and other security agencies curb the growing crime in the country.17 The need for the installation of CCTV cameras was accelerated by the deaths of two prominent Ugandans i.e. Arua Municipality MP –Ibrahim Abiriga and AIGP Felix Kaweesa.18 The President of Uganda thus gave a directive for the implementation of the project.19

Regrettably, the acquisition and deployment of the cameras is hidden from public oversight, which may lead to violations of human rights. For instance, the Wall Street Journal highlighted how Huawei technicians clandestinely assisted security forces in monitoring political adversaries.20

[15] https://www.independent.co.ug/chogm-spy-cameras-now-mere-scarecrow/ accessed on 29th April,2025
[16] https://twitter.com/ntvuganda/status/1036696599504801792 accessed on 29th April,2025
[17] ibid
[18] https://newslexpoint.com/government-starts-cctv-camera/ accesses on 29th April 2025
[19] https://ugandaradionetwork.net/story/president-museveni-directs-installation-of-security-cameras accessed on
[20] ibid

Huawei supplied CCTV equipment and completed the installation in stages. The initial stage was finished, and the National CCTV system was inaugurated by President Museveni. This system is situated at the police headquarters in Naguru, featuring 83 monitoring centers, 522 operators, and 50 commanders.21

The efficiency rate of Uganda's National CCTV Surveillance System currently ranges from 85% to 95%, with several districts operating at full capacity, as indicated by Hon. David Muhoozi, Minister of State for Internal Affairs. In a progress report on the project, Muhoozi stressed that the system, which has been in place since 2018, has significantly contributed to national security by allowing law enforcement to effectively handle 42,417 occurrences driven by intelligence and operations.22

Furthermore, a total of 6688 cases have been carefully examined through the use of CCTV footage, resulting in notable enhancements in crime detection and the safety of the public.23

Nevertheless, leaders of the opposition argue that law enforcement is too corrupt and overwhelmed to utilize the footage effectively for identifying offenders. They fear that police may deploy cameras equipped with facial recognition technology to specifically target protesters during aggressive crackdowns.

While there is some evidence of increased police responsiveness in urban areas, the system suffers from infrastructure gaps, delayed footage access, and inadequate

[21] ibid
[22] ibid
[23] ibid

maintenance .Moreover, the use of Chinese technology has raised geopolitical and cyber security questions.

Critics also argue that the Safe City project lacks independent oversight, public accountability, and data protection safeguards.it risks becoming a tool for authoritarian control rather than citizen safety.

3.2.2 DIGITAL SURVEILLANCE (SOCIAL MEDIA)

In order to identify and look into crimes that are computer-generated or electronically generated—that is, crimes perpetrated through online platforms. The Uganda Police formed an Electronic Counter Measure Unit (ECMU). The department in charge of enforcing the Computer Misuse Act is the ECMU.24

Civil society organizations believe that this unit is primarily targeting them and that it operates outside of the law.25

With 44 million people living there, Uganda possessed 25 million cell phones. subscribers at the start of 2018. The new rules are being used against people and organizations perceived as being anti-establishment, despite the nation having ratified a number of international treaties that guarantee freedom of expression.

Unwanted witness is a Ugandan civil society organization advocating for digital rights. Its report “State of security for HRDs in a digital era “states that 97% of journalists

[24] https://www.dandc.eu/en/article/what-ugandan-authorities-are-doing-limit-impact-online-opposition-voices accessed on 1st March,2025
[25] ibid

and human rights defenders claim that they face digital threats and are subjected to online surveillance.26 Seventy nine percent of them said they had no technical expertise to deal with the digital challenges and surveillance.27

In 2014, the Uganda Communications Commission (UCC) established a media-monitoring center, equipped with digital logger-surveillance equipment which records and analyzes public radio, television and print –media messages.28

Given the great influence social media has on the younger generation; the government is keen to monitor social media. Wilson Muruuli Mukasa, the former minister for security, said publicly that the government established the social media monitoring center "to sort out people who tarnish the government's reputation" meaning, getting rid of them.29

On 18th February 2016, during the presidential election, the UCC ordered telecom companies to block all social media. Facebook, WhatsApp and Twitter were thus unavailable when voting results were being transmitted from rural constituencies to the Electoral Commission in Kampala.30

The opposition claimed that they were kept from transmitting the correct results. The intervention, they say, enabled the government to rig the election.31

[26] ibid
[27] ibid
[28] ibid
[29] ibid
[30] ibid
[31] ibid

In June 2018, a social media tax was introduced, and anyone who wanted to access social media in Uganda must pay a tax of 200 Ugandan shillings equivalent to 5 US cents. This tax was aimed to limit the reach of people to social media.32

The Uganda Media Centre, the media regulatory authority appointed by the president, announced on 27th June that a team of state security officers and IT experts had been set up to scan profiles on Facebook and other social media networks in order to find posts critical of the government and the nation.33

Defending the special units' creation to an audience of citizen journalists at a news conference, Uganda Media Centre executive director Ofwono Opondo said: "We have realized that social media users are bitter and depressed people who are always complaining on their pages about the government and everything in the country, but they rarely get responses from the targeted ministries."34

"Increasing surveillance in order to better track down any criticism of the government is in itself a violation of freedom of information, " said Elodie Vialle, the head of RSFs Journalism and Technology Bureau. This measure is all the more worrying in a country that is in the habit of silencing critical journalists."35

As Uganda inches closer to the 2026 general elections, state pressure on digital expression is intensifying. A wave of arrests, warnings, and regulatory threats is targeting online critics particularly users of Tik Tok, X (formerly Twitter), and

[32] ibid
[33] https://rsf.org/en/uganda-creates-unit-spy-social-networks accessed on 2nd May 2025
[34] ibid
[35] ibid

YouTube raising concerns over the shrinking space for free expression and political dissent in the digital sphere.36

In January 2022, novelist and activist Kakwenza was charged with offensive communication under the same law for allegedly insulting President Museveni and his son on twitter. He was tortured while in detention, fled into exile in February 2022, after he was released on bail.37

Alongside prosecutions and regulatory threats, the Ugandan government is ramping up surveillance of digital platforms.38 The planned importation of AI – powered equipment to monitor social media activity, as recently disclosed by the UCC, is raising red flags among digital rights advocates.39 The technology is reportedly intended to filter out so –called "harmful content", including hate speech, disinformation, and incitement.40 However, without transparent oversight and public safeguards, such measures risk becoming tools of censorship rather than protection.41

The environment undermines Uganda's commitments under national and international human rights law. Freedom of expression, access to information, and the right to privacy are not privileges to be granted or revoked, they are fundamental rights that should be protected, especially during elections.42

[36] https://cipesa.org/2025/04/uganda-steps-up-pressure-on-social-media-crtitics-ahead-of-2026-polls/ accessed on 2nd May ,2025

[37] ibid
[38] ibid
[39] ibid
[40] ibid
[41] ibid
[42] ibid

3.2.3 DIGITAL NUMBER PLATES

The government of Uganda through the ministries of Works and Transport and Security officially launched the digital car number plate's project.43

Speaking at the launch in Kampala Minister Gen. Katumba Wamala said the primary benefit of rolling out Safety and control of motor-vehicles –related criminality. The ITMS project will deter theft of motor vehicles and vehicle-related criminality through enhanced traceability, tracking and real time feedback from the Police Command Centre.44

It will discourage reckless driving due to monitoring through the CCTV Camera network enhancing enforcement.45

Uganda's rollout of the new "digital" number plates is facing sharp criticism amid reports that stolen vehicles remain untraceable, raising serious questions about the system's effectiveness and the capacity of the Russian contractor implementing it.46

Motorcycle owners, especially those in the public sector, have voiced alarm over the inability to track stolen bikes equipped with the new plates, contradicting claims of enhanced security.47

[43] https://portal.itms.ug/blog/itms-in-media-1/uganda-rolls-out-digital-car-number-plates-projects-2 accessed on 2nd May,2025
[44] Ibid
[45] ibid
[46] https://pmldaily.com/news/2025/02/ugandas-digital-number-plates-face-scrutiny-over-tracking-failures-contractor-capacity.html accessed on 2nd May,2025
[47] ibid

Furthermore, concerns have been raised about the digital nature of the plates themselves. Experts argue that the system lacks real time tracking capabilities, unlike more advanced systems used in other countries.[48]

The controversy has also reignited concerns about the cost of the plates and potential privacy implications.[49]

While the government has a legitimate desire to improve the security of its people and transport management, recent events as discussed where the same government has used the acquired technologies to monitor its citizens and undermine digital rights, it is critical that any future attempt to enhance its surveillance apparatus is anchored in law with clear oversight mechanisms.[50]

This is because the deployment of surveillance technologies such as ITMS, Fin Fisher, and Huawei's CCTV present a veritable avenue for economic and political exploitation by collecting extensive data on people's behavior, location, activities and interests online and offline. This makes the risk of violation of privacy apparent, rendering citizens helpless because they essentially have no control over how the data will be used, even when they are aware that data is being collected.[51]

It is therefore important that the government reduce its reliance on foreign manufactured surveillance technologies, particularly from countries whose human

[48] ibid
[49] ibid
[50] https://cipessa.org/2024/08/rollout-of-digital-numbber-plates-poses-privacy-concerns-in-Uganda accessed on 2nd May,2025
[51] ibid

rights record is wanting, as these have tended to use these tools to suppress civic spaces.52

3.2.4 BIOMETRIC DATA

On 19th April,2017,Unwanted Witness Uganda learnt that over 7 million telecom subscribers had participated in SIM Card verification exercise since the 7 day ultimatum issued by Uganda Communications Commission (UCC)53

The organizing exercise, which is not fully guided by law, is meant to accomplish a hatched plan by the establishment to intercept and openly conduct surveillance on Ugandans.54

Uganda has mandated SIM Card registration linked to the National Identity Number (NIN) as part of the broader surveillance strategy. This allows for identity verification and real –time tracking of phone users. For example in 2017, the UCC deactivated all sim cards not registered with valid NINs as this move was framed as a national security necessity.

Verifying National ID data with SIM Card registration only justifies the government's surveillance traits and besides the country does not have storage which highly exposes citizens' data to abuse by both state and non-state actors.55

[52] ibid
[53] https://www.unwantedwitness.org/sharing-citizens-biometric-data-from-national-id-with-telecom-companies-is-intended-to-seal-a-plot-for-mass-surveillance/ accessed on 2nd May 2025
[54] ibid
[55] Ibid

According to the 2014/15 budget paper, the government earmarked UGX 205 billion to procure a phone tapping machine on grounds that the existing tapping equipment only tracked telephone communications between callers and recipients but could not record their voices.56

The billion shillings surveillance equipment supplied by the Israeli firm, enables the operatives to listen to phone conversations anywhere in the country, detects location of a caller and receiver and has the capacity to burst email accounts that are under surveillance.57

Uganda's National Identification Registration Authority (NIRA) collects biometric data for every citizen during ID registration, creating a centralized biometric database. It has been effective in eliminating duplicate identities and improving identification for government services.

The lack of data protection and secure storage mechanisms poses major privacy and cyber security risks.

3.3 Legal Frameworks regulating Surveillance in Uganda (the role of legal frameworks in governing Surveillance)

Legal frameworks play a crucial role in defining the boundaries between legitimate state surveillance and the protection of fundamental human rights. In democratic societies, surveillance must operate under a regime of legality, necessity, proportionality, and accountability. This ensures that while the state can safeguard

[56] ibid
[57] ibid

national security and public order, it does not infringe upon the civil liberties of its citizens without lawful justification.

In Uganda however, the evolution of legal frameworks regulating surveillance has struggled to keep pace with technological advancement and growing state appetite for control. The Ugandan state has invested heavily in surveillance infrastructure- including biometric systems, CCTV networks, digital communication intercepts, and data harvesting tools, yet the legal and regulatory structures meant to govern these practices are often vague, outdated, weakly enforced, or susceptible to abuse.

This section critically examines the primary legal instruments governing surveillance in Uganda, assessing their scope, effectiveness and limitations.

3.3.1 The Constitution of the Republic of Uganda, 1995

The Constitution of the Republic of Uganda, 1995 is the fundamental legal document that guarantees and regulates fundamental rights and freedoms. Any surveillance activity in Uganda must align with the Constitutional principles, particularly those found in Chapter Four (Protection and Promotion of Fundamental and Other Human Rights and Freedoms)

Article 27[58] provides that no person shall be subjected to unlawful search of the person, home or other property of that person or unlawful entry by others on the premises of that person.

[58] The Constitution of the Republic of Uganda

Article 27(2) (b) 59states that no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

Article 43 (1) 60also provides for limitations of rights and freedoms in the public interest but prohibits actions that are beyond what is acceptable and demonstrably justifiable in a democratic society.

The constitution recognizes privacy as a constitutional right implying that all surveillance must be legally sanctioned and proportionate and it also provides a basis of judicial review and legal redress in cases of unlawful surveillance.

However in terms of enforceability of the above laws, there is hindrance and delays in the judicial system and also reluctance to challenge state security organs in Uganda as most of the security organs tend to interfere with the independence of the judicial officers when exercising their powers.

During the 2021 elections, security agencies conducted digital surveillance on opposition candidates without publicly known legal warrants. While such actions were arguably unconstitutional under Article 2761 the lack of an effective judicial recourse meant that those rights were practically unenforceable.

Mass digital surveillance violates the right to privacy guaranteed by the 1995 Constitution62 and the International Covenant on Civil and Political Rights63 as it arbitrarily and unlawfully interferes with individuals' privacy. This is so much so

[59] ibid
[60] ibid
[61] ibid
[62] ibid
[63] Article 17 of the ICCPR

because mass digital surveillance is not authorized by law64 and covers an unlimited scope of the target's private life.65 Sotomayor J in her concurring opinion in the United States v Jones66 observed the following about surveillance and the right to privacy:

In this case, the government installed a Global Positioning System (GPS) tracking device on respondent Antoine Jones Jeep without a valid warrant and without Jones consent, then used that device to monitor the Jeeps movements over the course of four weeks. The government usurped Jones property for the purpose of conducting surveillance on him, hereby invading privacy interests long afforded, and undoubtedly entitled for Fourth Amendment Protection.67

What the Ugandan government's proposed mass digital surveillance intends to do is in material respect, similar to what the United States Government did in the above case, albeit on a larger scale and for an infinite period. If the Government goes ahead with its plans and implements the same, it will violate the right to privacy of the Ugandans, as guaranteed by Article 27.68

For mass digital surveillance to be acceptable and demonstrably in a free and democratic society, in light of the 1995 Constitution,69 it must satisfy the tripartite

[64] United States of America v Jones 565 US.400(2012)
[65] In Szabo and Vissy v Hungary App no 37138/2014 (ECtHR,12 January 2016)
[66] 565 U.S.400(2012)
[67] ibid
[68] The Constitution of the Republic of Uganda 1995
[69] Article 43(2)(c) of the Constitution of the Republic of Uganda

test of being legal, necessary and proportionate70 which have been ignored by the government of Uganda when implementing digital mass surveillance.

3.3.2 Data Protection and Privacy Act, 2019

In order to properly fulfill a public duty by a public body, for national security, or to prevent, detect, investigate, prosecute, or punish an offense or violation of the law, the Data Protection and Privacy Act of 2019 permits the collection of personal data without the consent of the data subject.71

The proposed widespread surveillance is justified by the government as being necessary for national security. The question of what types of surveillance are covered by the national security exception is thus brought up.72 The ability of a nation to defend itself against aggression or attacks is the essence of national security.73

The government's chosen form of targeted surveillance may involve digital surveillance through the use of global positioning systems, tracking devices mounted on cars, mobile phones with chips, tapping into phone cells, email conversations, and other methods, or physical surveillance by security personnel.It is mortifying to say, that section 774should not be interpreted separately from other parts of the same Act

[70] Charles Onyango Obbo v AG [2004] UGSC 1
[71] S.7(2)(b) Data Protection and Privacy Act,2019
[72] Nasser Nkonge ," No to Big Brother: The legality and implications of mass digital surveillance in Uganda" https://iuea.ac.ug
[73] www.collinsdictionary.com/dictionary/english/nationalsecurity accessed on 4th May,2025
[74] Data Protection and Privacy Act 2019

since it is a fundamental principle of statutory interpretation that the entire statute must be interpreted in its entirety.75

Regardless of any national security concerns, the same law prohibits data collection practices that violate the right to privacy.76 Even for national security reasons, the Act forbids mass digital surveillance since it is obviously a violation of the right to privacy.

The Act also details the principles of data collection, emphasizing the need for fair and lawful methods of gathering and processing personal data that is relevant and not excessive or unnecessary. It specifies that personal data should be retained only for the duration permitted by law or as long as it is needed. Additionally, it promotes transparency and the involvement of data subjects in the collection, processing, use, and retention of their personal data.

In a nation lacking data protection legislation to govern the retention, use, and storage of data, coupled with documented instances of abuse and misuse, it is difficult to trust the effectiveness of the system. A statement from Unwanted Witness-Uganda in December 2015 revealed that MTN Uganda was sharing subscriber information with the ruling National Resistance Movement party.77

On July 15, 2020, Unwanted Witness Uganda published a report accusing Safe Boda—a motorcycle transport service that operates in Uganda, Kenya, and Nigeria—of

[75] Uganda Revenue Authority v Kajura [2017] UGSC 63
[76] Section 10 ,Data Protection and Privacy Act 2019
[77] Unwanted Witness(Unlawful SIM Card Validation Exercise Is a Threat to Anonymity) https://www.unwantedwitness.org accessed on 4th May,2025

disclosing their clients' personal information to third parties without the necessary consent and awareness mandated by Section 7.78.

As a result, the Ugandan government is required to adhere to the data protection principles outlined in the Data Protection and Privacy Act 2019. The government's proposed mass digital surveillance violates all of the aforementioned data protection principles, making its implementation illegal.79Ironically, the same government that is required to make sure that data protection principles are followed also has no intention of doing so.

3.3.3 Regulation of Interception of Communications Act 2010

The RICA 2010 declares that no one may intercept communications until a warrant has been obtained.80A designated judge must receive an application from a party wishing to intercept any communication.81 And after reviewing the evidence, the judge can only issue a warrant if he or she is certain that the subject of the request has done or is likely to commit a crime.82

A designated judge is defined under section 1 83as a judge appointed by the Chief Justice under that section indicates that no request for a warrant can be submitted or authorized as permitted by the Act rendering all forms of digital surveillance unlawful, even when they are justified by the Act.

[78] The Data Protection and Privacy Act 2019
[79] Section 3(2) of the Data Protection and Privacy Act 2019
[80] Section 2 of the RICA
[81] Section 4 of the RICA
[82] Section 5 of the RICA
[83] The Regulation of Interception Of Communications Act ,2010

The RICA was implemented in 2010 and has faced criticism from Human rights organizations, both domestic and foreign for granting extensive authority to the government to monitor and intercept confidential communications.84

In line with section 9 of the RICA, telecommunications service providers must make sure that SIM card registration is completed by subscribers by providing detailed personal information. The Act also obligates telecom companies to install appropriate equipment that enables the interception of communications, imposing a penalty of five years of imprisonment for those who fail to comply. Section 3 establishes a Monitoring Center and requires mobile phone service providers to transmit intercepted communications to this center.85

In December 2010, Amnesty International criticized RICA for having a vague and overly broad framework for intercepting communications, which could lead to unwarranted surveillance of individuals and professionals like journalists, human rights advocates, and political dissidents who are involved in lawful activities while exercising their fundamental human rights, including freedom of expression and association.86

[84] Unwanted Witness(Unlawful SIM Card Validation Exercise Is a Threat to Anonymity) https://www.unwantedwitness.org accessed on 4th May,2025

[85] ibid
[86] ibid

3.3.4 The Computer Misuse Act 2011

The Computer Misuse Act is designed to safeguard the security of electronic transactions and information systems. According to sections 3 and 587The Act advances the regulation of access to data stored on computers by establishing protections and banning unauthorized access. Additionally, it outlines situations where access and alterations might be considered unauthorized, as specified in sections 8 and 1288respectively. According to the Act, offences related to computer misuse encompass unauthorized access (section 13) and unauthorized alteration of data (section 14)89, unauthorized access or interception of computer services (section 15)90 etc.

These parts indicate that although privacy is guaranteed, it can be revoked with proper authorization. The legislation further prohibits electronic fraud as outlined in section19.

The Act includes penalties for offences related to computers in section 20. Additionally, it establishes laws against cyber harassment (section 24), offensive communication (section 25), and cyber stalking (section 26).91

The legislation includes stipulations for preservation orders concerning data in situations of vulnerability or loss, as outlined in section 9.92Additionally, according to sections 9 and 11, investigators can request orders to conduct investigations and

[87] The Computer Misuse Act ,2011
[88] ibid
[89] ibid
[90] ibid
[91] ibid
[92] ibid

obtain data to assist in criminal inquiries. This legislation also allows for search and seizure based on orders issued by a Magistrate.

Importantly, this legislation has been utilized in the past to silence those who oppose the government, as shown by the arrest and legal action taken against social media critic Dr. Stella Nyanzi, who faced charges of cyber harassment and offensive communication under this law.93

Other individuals who have faced the consequences of the same legislation include former presidential candidate Henry Tumukunde, who was apprehended for purported treasonous remarks made during radio and television interviews; the Bizonto comedy group, who were detained for allegedly posting offensive and sectarian content; and author Kakwenza Rukirabashaija, who was arrested, held, and prosecuted for making offensive statements about the president and his son.94

In 2018, a group of seven journalists from various media organizations uncovered a corruption scandal at the Bank of Uganda and released images showcasing the dubious wealth of certain bank directors. The journalists were called in by the police under the Computer Misuse Act to provide their accounts. Eventually, the police lost interest in the matter since none of the implicated directors pursued any accusations against the journalists, leading to the case being dismissed.95

[93] State of internet Freedom in Africa 2018(Privacy and Personal Data Protection) https://cipesa.org accessed on 4th May 2025
[94] A Section of Uganda's Computer Misuse Act Outlawed! But, The Greater Part of the Law Remains Thorny https://cipesa.org accessed on 4th May 2025
[95] State of internet Freedom in Africa 2018(Privacy and Personal Data Protection) https://cipesa.org accessed on 4th May 2025

Edrine Wanyama, who serves as the Legal Officer at CIPESA, contends that the legislation poses a risk to digital rights and the digital civic space, not meeting the benchmarks set by international standards. Therefore, it is crucial to contest the law in a court of law.96

Although the law has many regressive aspects, Wanyama points out that there are some positive elements that, if used appropriately, might enhance certain facets of the digital civic space.97

3.3.5 Anti –Terrorism Act 2001

In recent years, Uganda has faced issues related to insecurity and overall instability, highlighted by public protests against President Museveni's administration. Acts of terrorism, whether genuine or staged, not only result in casualties and damage to property but also create fear among citizens and intensify insecurity in this East African nation.98

The government has quickly enacted laws to combat (alleged) terrorism in response to the 2001 attacks in the US, the bombings in Kampala in 2010, and the attacks that occurred in October and November 2021.99

The Ugandan government exploits the anti-terrorism legislation to go after its adversaries and suppress discussions on crucial matters impacting the nation. The

[96] Clare Muhindo (New Computer Misuse law threatens freedom of expression, activists say) https://acme-ug.org accessed on 4th May 2025
[97] ibid
[98] Florence Namasinga Selnes (Anti-terrorism regulation and the media in Uganda) https://verfassungsblog.de/os4-uganda accessed on 4th May 2025
[99] ibid

application of anti-terrorism regulations to silence opposing opinions signifies an increasing intolerance towards criticism of President Museveni's government. Authorities utilize anti-terror laws whenever it is convenient to restrict personal freedoms of expression and the press.100

Numerous times, the military has conducted raids on media organizations, rummaging through their premises and seizing documents and computers to find evidence that could compromise specific journalists and their employers.

The arrest of Doreen Biira in November 2016 for allegedly supporting terrorism highlights how the government employs legal measures to stifle journalists. Biira was detained for documenting and distributing footage of military violence in Western Uganda, during confrontations that resulted in more than 70 fatalities. The reporter faced charges of aiding terrorism, which is a criminal offense that could lead to a 7-year prison sentence if convicted.101

This sparked a backlash against the anti-terrorism legislation and led human rights advocates and journalist groups to urge the government to dismiss the terrorism charges against Biira.102

Clauses in the anti-terrorism legislation concerning communication interception and surveillance significantly impact how journalists engage with their sources, as well as

[100] ibid
[101] ibid
[102] ibid

their capacity to reach out freely to sources that authorities may categorize as terrorists.103

Unwanted Witness's examination of Uganda's most oppressive cyber legislation places the counter-terrorism law among the top three. This law has been criticized for violating international norms regarding freedom of expression and privacy rights.104

Since 2006, Uganda's anti-terrorism legislation has been utilized; Dr. Kizza Besigye, a consistent opponent of President Museveni, was detained and brought before the court on allegations of terrorism, rape, and treason. The prosecutor for the state was unable to present evidence for these accusations, which many political analysts perceived as driven by political motives given that the charges arose ahead of the general elections.105

[103] ibid
[104](Impact of the Anti-Terrorism Act Implementation to the Enjoyment of the right to Privacy) https://www.unwantedwitness.org accessed on 4th May 2025
[105] ibid

4.0 CHAPTER FOUR

4.1 MASS SURVEILLANCE AND CIVIL LIBERTIES

In the era of technology, the ability of governments to oversee and regulate the dissemination of information has grown exponentially, posing unprecedented obstacles to safeguarding fundamental human rights. Mass surveillance, the widespread, indiscriminate collection and analysis of personal data by government agencies has emerged as a particularly contentious issue in many jurisdictions. It raises serious concerns about the erosion of constitutionally guaranteed rights such as privacy, freedom of expression, freedom of assembly, and due process.

In Uganda the deployment of mass surveillance mechanisms has increased notably over the past decade, often justified on grounds of national security, crime prevention, and counter terrorism. These efforts, while arguably legitimate in purpose, have frequently occurred in legal and institutional vacuums that lack robust oversight, transparency, and accountability. The use of closed circuit television (CCTV) systems under the “safe city” initiative, mandatory biometric registration through the National Identification and Registration Authority (NIRA), and the monitoring of digital communications under laws like the Regulation of Interceptions Communications Act, 2010 illustrate a growing surveillance apparatus that operates with limited checks.

This chapter interrogates the impact of mass surveillance on individual privacy rights and civil liberties in Uganda with reference to constitutional guarantees, statutory instruments, and regional and international human rights standards. Through a critical analysis of state surveillance practices and legal frameworks, it seeks to determine whether Uganda's current surveillance regime aligns with democratic principles and the rule of law. By drawing on case studies, court rulings, and human rights reports, the chapter highlights the consequences of unchecked surveillance on Uganda's democratic space and offers policy recommendations for reform.

Mass surveillance refers to the collection, processing, production, examination, utilization, retention, or storage of data concerning many individuals, regardless of whether they are believed to be engaged in any unlawful activities.106

In legal terms, the issue with mass surveillance is that it is not strictly necessary or proportionate in a democratic society. There are frequently less intrusive options available. Moreover, even when these alternatives are lacking, we wonder if a democratic society can endure under perpetual surveillance.107

By continuously observing individuals, mass surveillance creates the possibility for unrestrained governmental authority and domination over citizens. Mass surveillance is based on the belief that any gathered information might be valuable to confront a potential danger, which conflicts with the core ideals and tenets of democratic

[106] Nasser Nkonge ," No to Big Brother: The legality and implications of mass digital surveillance in Uganda" https://iuea.ac.ug accessed on 6th May 2025
[107] ibid

societies that aim to restrict the knowledge a government has about its populace to control its power.108

Mass surveillance undermines the separation of powers since the executive branch can perform its actions without adequate oversight from the legislative and judicial branches. The powers related to mass surveillance lack proper independent approval, as authorization is given en masse rather than for each specific instance of wrongdoing. This fosters a climate of fear and mistrust that contradicts democratic ideals and principles, leading the state to view all individuals as guilty until they can prove otherwise.109

Constant monitoring fosters a sense of mistrust and fear, leading individuals who are not involved in any misconduct to alter their behavior, including how they act, speak, and interact—this phenomenon is often referred to as the chilling effect of mass surveillance. Consequently, it restricts the rightful use of our freedoms. It jeopardizes society's capacity to innovate and develop.110

Due to the vast quantities of data gathered and examined through mass surveillance, this approach also facilitates automated decision-making: obscure algorithms, often referred to as "black boxes," generate conclusions that are difficult to clarify owing to the complexity and confidentiality associated with the operation of these systems,

[108] ibid
[109] https://privacyinternational.org/learn/mass-surveillance accessed on 6th May 2025
[110] ibid

especially within a security framework. This additionally undermines the capacity to properly monitor mass surveillance activities.111

Governments are increasingly allocating resources towards surveillance, artificial intelligence, and machine learning technologies with the goal of integrating these tools into their operations and decision-making processes (Human Rights, Big Data and Technology Project 2018). This trend is particularly noticeable in the intelligence and law enforcement areas, where several governments have established extensive surveillance and analytical capabilities, including near-universal collection of communications data (La Quadrature du Net and Ordre des barreaux franc 112The implementation of facial recognition technology within networks of surveillance cameras (Amnesty International 2022; Ryan-Mosley 2022) and a range of predictive policing instruments (Deeks 2018; Oswald et al. 2018) signifies a fundamental shift in the dynamics between the State and individuals under its authority. These surveillance and analytical tools enable the State to observe the finer details of people's everyday activities, create patterns of behavior, pinpoint 'unusual' or 'suspicious' actions, and make personalized decisions based on this information.113

Given the presence of such sophisticated surveillance tools, it raises the question of whether people will alter their typical behavior to prevent unwanted conclusions from being made about them. Are they likely to avoid legitimate, albeit occasionally contentious, actions like exploring diverse or 'radical' concepts, associating with

[111] ibid
[112] Chilling Effects of Surveillance and Human Rights ;Insights from Qualitative Research in Uganda and Zimbabwe https://academic.oup.com accessed on 6th May 2025
[113] ibid

specific individuals, protesting, or engaging in political activities due to concerns over possible repercussions?[114]

Extensive digital monitoring frequently causes individuals to engage in self-censorship to evade scrutiny, which infringes upon the freedom of expression protected by the 1995 Constitution.[115] A prominent theme that surfaced from the research was self-censorship driven by surveillance. Considering the significance attached to the open exchange of ideas and the free growth of an individual's personality, this is undoubtedly contrary to the aim and purpose of the right to freedom of expression.[116]

Self-censorship was noted in relation to social media activity. An interviewee from Uganda expressed, "Before I share something, I consider: 'What am I about to share? What consequences could arise? ... Is it worth the risk of going back to prison?'In certain instances, acts of self-censorship seem to be motivated not just by personal gain, but also by a desire to shield others: 'I'm concerned about surveillance because my friends and family might be identifiable and either harmed or turned against me' (Participant 15). Naturally, individuals will inevitably seek ways to circumvent self-censorship and experiment with the limits of what constitutes 'acceptable' versus 'unacceptable' speech.[117] An interviewee from Uganda, for instance, stated that while they maintained their public presence, they toned down their manner of expression: The surveillance and arrests have caused me to be less radical. I do not

[114] ibid
[115] Article 29 of the Constitution of The Republic of Uganda 1995
[116] ibid
[117] ibid

express my views as strongly as I could because if I appear on television, the surveillance extends beyond me; it also affects the television station owner. The media owners are apprehensive, and they encouraged me to tone it down… I used to convey the truth directly, but now I have to communicate through metaphors.118

Although these alternative methods are commendable and demonstrate a courageous effort to confront authoritarian governments, the reality that individuals must either self-censor or create these workarounds highlights a serious infringement on the right to freedom of expression, which clearly affects the functioning of democracy.119

As stated earlier, an essential part of the chilling effect is the apprehension about the potential outcomes that might arise if certain actions are noticed.120. A Ugandan participant remarked that individuals are hesitant to express certain opinions during meetings, and some avoid engaging in specific discussions because they are uncertain about their safety.121

There is a significant amount of fear. Individuals observe the harsh treatment of activists currently and have chosen to remain silent for their own safety… Many are not prepared to jeopardize their own security and that of their loved ones, preferring to conform and avoid participating in those conversations.122 The threat of being watched has driven individuals to comply.123

[118] ibid
[119] ibid
[120] ibid
[121] ibid
[122] ibid
[123] ibid

This highlights another aspect of the chilling effect, which seems to go beyond an individual's direct expression, as previously mentioned in relation to self-censorship, to also influence the individuals that one interacts with or is thought to be connected to. As stated by an interview participant from Uganda: 'I avoid connecting with politically involved individuals on social media because I do not want to be identified with any specific group.'124

The entitlement to gather freely125the International Covenant on Civil and Political Rights enshrines the right to peaceful assembly. Restrictions on the exercise of this right may only be applied in accordance with the law and must be essential in a democratic society for reasons related to national security or public safety, maintaining public order, safeguarding public health or morals, or protecting the rights and freedoms of others. This right is also guaranteed by the constitution of Uganda.126

The freedom of assembly ensures individuals can come together peacefully. While public protests are often the most recognized examples of this right, it also includes gatherings of all kinds, whether held indoors or outdoors, and regardless of whether they are public or private.127

In a similar vein, it has been observed that disparaging remarks from a government representative can lead to intimidation, creating a chilling effect that discourages

[124] ibid
[125] Article 21 of the International Covenant on Civil and Political Rights
[126] Article 29 of the Constitution of The Republic of Uganda1995
[127] Chilling Effects of Surveillance and Human Rights ;Insights from Qualitative Research in Uganda and Zimbabwe https://academic.oup.com accessed on 6th May 2025

individuals from engaging in the activities of an association.128This aligns with the earlier observation regarding how a State's reaction to a specific action can create a chilling effect, resulting in reluctance to interact with certain individuals or participate in particular activities.129The right to gather peacefully is not an unconditional right, and may be restricted under specific circumstances. Nevertheless, due to its importance for the functioning of democracy, the range of any restrictions must be limited: "only persuasive and compelling justifications can justify limitations."130

Confidence, an essential element in the formation and preservation of relationships, is crucial for the practice of the right to freedom of assembly.131 In this context, it is important to highlight that a significant theme arising from the research is how the presence of surveillance, or the anxiety that comes with it, damages trust and personal connections. Notably, it seems that the unpredictability linked to surveillance, which is a core aspect of the chilling effect, fosters a cycle of fear and distrust.132 The potential existence of informers surfaced as a significant contributing factor in this situation, with the challenge of verifying whether an individual is an informer or not being a complicating element. Comparable impacts have been observed in different contexts.133 Ali134For instance, it was discovered that the

[128] ibid
[129] ibid
[130] ibid
[131] ibid
[132] ibid
[133] ibid
[134] Arshad Imtaz Ali is an author of an article " Citizens under Suspicion: Research with Community under surveillance."

existence of informers resulted in a breaking down of trust between communities. This caused significant adverse impacts on political engagement within the affected community by eliminating environments deemed secure for freely sharing opinions, organizing efforts, and establishing political identities.135

This concern about informants within an activist group or community was echoed by another participant: 'there are unofficial agents who are not officially employed as intelligence gatherers, but they have connections with individuals in intelligence.'136Typically, these individuals are friends, fellow activists, and colleagues of those who are being targeted (Participant 3).137The resulting feelings of paranoia and distrust were clearly mentioned: I've heard accounts of other comrades being watched, which made me quite anxious.138I began noticing shadows all around me, even when I was out enjoying drinks with friends; I would leave without saying farewell because it felt as though I was always being observed.139

The effect of the decline in trust and the fragmentation of inter-community trust on the capacity to organize effectively were mentioned by several interviewees. For example, one respondent from Uganda expressed it succinctly: 'There is a rupture in trust with some team members' (Participant 28). Another remarked: for human rights organizations and social movements, once the group has been compromised, it

https://www.researchgate.net/publication/295076458_Citizens_under_Suspicion_Responsive_Research_with_Community_under_Surveillance

[135] Chilling Effects of Surveillance and Human Rights ;Insights from Qualitative Research in Uganda and Zimbabwe https://academic.oup.com accessed on 6th May 2025

[136] ibid

[137] ibid

[138] ibid

[139] ibid

undermines trust and cohesion among colleagues, making it extremely challenging to coordinate actions even when the intentions are genuine and sincere.140 Throughout the years, the State's capacity to monitor and infiltrate organizations has adversely affected activism and the personal lives of those involved, particularly leaders in organizing efforts. It has hindered all our planned activities as activists due to a lack of trust.141

These elements undoubtedly hinder the capacity to organize. For example, needing a 'chain of trust' prior to mobilization will adversely impact a group's potential to attract a large audience, restricting involvement to only a small number of individuals.142 This challenge of organizing on a broader scale was highlighted by several interview participants.143

The effects of surveillance on a person's capacity to organize and develop political groups are significant.144 This research indicates that a surveillance-related chilling effect may fundamentally impair individuals' ability to organize and mount an effective political opposition, undermining both the right to freedom of assembly, and the functioning of democratic society.145

The reluctance of other people to engage with individuals who they believe may be subject to surveillance is a theme which emerged clearly from the research, particularly in Uganda. This factor has a straightforwardly negative impact on the

[140] ibid
[141] ibid
[142] ibid
[143] ibid
[144] ibid
[145] ibid

right to freedom of assembly, as it restricts open engagement. This was expressed by one interviewee: Most of our community or engagements have been curtailed because the people you want to work with are suspicious.146 They think the government [agents] is following them and they are afraid of negative impacts.147 For example during protests such as the Free Bobi Wine protests in 2020, authorities used surveillance and informers to identify and arrest demonstrators. The fear of being monitored discouraged many of them from participating, effectively limiting their constitutional right to assemble peacefully.

Also civil society organizations CSOs have reported increased surveillance and harassment. The NGO Act requires NGOs to disclose financial and operational information, and in some cases, intelligence agencies have infiltrated or monitored meetings, particularly those of human rights defenders and election observers.

Mass digital surveillance has a chilling effect on the right to freedom of movement guaranteed by the 1995 Constitution148, the African Charter on Human and Peoples Rights,149 and the International Covenant on Civil and Political Rights150, as it prohibits individuals from going about their daily routines and movements due to fear of being watched by authorities.

The right to freedom of movement presupposes liberty and freedom to move wherever and whenever one wishes. Mass digital surveillance takes away this as often

[146] ibid
[147] ibid
[148] Article 2 of the Constitution of the Republic of Uganda 1995
[149] Article 10
[150] Article 22

individuals may fear making certain movements to various destinations for fear of being associated with those destinations or for fear that their movements will not go well with the authorities. Members of the opposition parties, critics of government, and gender or sexual minorities will not be able to freely move about the country due to the proposed surveillance given the track record of security agencies towards them.151

Mass digital surveillance enables the acquisition of vast information about the members of the public, which, if in the wrong hands, can lead to blackmail and extortion of members of the public, especially if it is embarrassing, portrays immorality, or individuals' secrets.152

Sotomayor J in the United States v. Jones 153 described the nature of information that can be acquired in the following terms: Disclosed in GPS data will be trips the indisputably private nature of which takes little imagination to conjure trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.154

Mass digital surveillance enables state authorities to sort the public into categories of people,155depending on a given criterion, and in this particular case, it will be based on their movements. The intended government mass digital surveillance will enable

[151] ibid
[152] Nasser Nkonge ," No to Big Brother: The legality and implications of mass digital surveillance in Uganda" https://iuea.ac.ug accessed on 6th May 2025
[153] United States v Jones 565 U.S. 400 (2012).
[154] ibid
[155] Neil M. Richards, "The Dangers of Surveillance", (2013), 126, Harvard Law Review, p. 1956

state authorities to mark the general public's movement patterns and regular visits, which will be a tool for profiling the members of the public. This can be a disadvantage for many people, especially those belonging to minority groups.156

Because it allows state authorities to deliberately target a specific person or group of persons they suspect of engaging in illegal activity without a valid reason, mass digital surveillance contributes to the presumption of guilt.157

The 1995 Constitution's right to privacy and the International Covenant on Civil and Political Rights are both violated by widespread digital surveillance158because it infringes on people's privacy in an arbitrary and illegal manner. The reason for this is that the legislation does not permit widespread digital surveillance.159It encompasses an infinite amount of the target's personal life.160 In her concurring opinion in the case of United States v. Jones, Sotomayor J, 161noted the following regarding privacy rights and surveillance: Without obtaining a proper warrant or obtaining Antoine Jones' agreement, the government implanted a Global Positioning System (GPS) tracking device on his Jeep and utilized it to track Jones' travels for four weeks. Jones' private rights, which are unquestionably protected by the Fourth Amendment, were violated when the government took his property in order to spy on

[156]Nasser Nkonge ," No to Big Brother: The legality and implications of mass digital surveillance in Uganda" https://iuea.ac.ug accessed on 6th May 2025

[157]United States v Jones 565 U.S. 400 (2012)
[158] Article 17 of the ICCPR
[159]United States of America v Jones 565 U.S. 400(2012)
[160] Szabo and Vissy v Hungary App no 37138/2014 (ECtHR, 12 January 2016)
[161] United States v Jones 565 U.S. 400 (2012)

him.162Though on a greater scale and for an indefinite amount of time, the Ugandan governments intended mass digital surveillance is materially identical to what the US government did in the aforementioned instance. Ugandans' right to privacy, as protected by Article 27 of the 1995 Constitution, will be violated if the government moves forward with its intentions and carries them out.

The expansion of mass surveillance in Uganda has revealed a profound tension between state interests in security and safeguarding essential human liberties and rights. While the government asserts that surveillance technologies are vital tools for maintaining public order, deterring crime, and combating terrorism, the manner in which these tools are being deployed often lacks the constitutional and legal safeguards necessary to protect individual privacy and civil liberties.

Ultimately the chapter concludes that mass surveillance in Uganda is not merely a technical or security issue, it is a deeply political and legal question that strikes at the heart of constitutionalism and democratic governance. To restore balance, Uganda must undertake urgent legal reforms, establish independent oversight mechanisms, and foster a transparent and accountable culture in the use of surveillance technologies. Only then can the state fulfill its obligation to safeguard both state security and the rights and freedoms of its citizens in equal measure.

[162] ibid

5.0 CHAPTER FIVE

5.1 BALANCING NATIONAL SECURITY AND PRIVACY IN UGANDA

Uganda can balance privacy and national security in mass surveillance by implementing strong legal frameworks, fostering transparency, and ensuring accountability. This includes enacting robust data protection laws, establishing clear policies on surveillance, and providing mechanisms for redress when privacy is infringed upon.

Police in the community are changing. Since technology is developing so quickly, law enforcement organizations are implementing new digital tools to improve community trust and public safety. But this change also presents new difficulties, particularly in striking a balance between the need for efficient policing and privacy concerns.163

The way police engage with the communities they serve is changing as a result of digital tools like body-worn cameras, social media monitoring, and predictive analytics. These technologies have the potential to boost efficiency, increase transparency, and offer insightful information that helps with decision-making. Real-time data, for example, can assist law enforcement in locating crime hotspots more rapidly, allocating resources efficiently, and reacting to situations more quickly.164

[163] https://zencity.io/how-to-balance-privacy-and-public-safety-in-the-digital-age/#:~:text=One%20of%20the%20keys%20to,usage%2C%20retention%2C%20and%20access. Accessed on 6th May 2025
[164] ibid

Nevertheless, there are several disadvantages to integrating these tools. For instance, the growing usage of surveillance technologies creates questions regarding data security, individual privacy, and misuse potential.165

It is understandable that the public is concerned about privacy. Automated license plate scanners, facial recognition software, and surveillance cameras can make people feel like they are being watched all the time. Trust may be damaged by this impression, particularly in areas where ties between the police and the public have historically been tense.166

Furthermore, there is reason to be concerned about data breaches and illegal access to private data. Personal information may be at risk from cyberattacks if the data gathered by digital tools is not handled appropriately. Clear policies, openness, and strong security measures are necessary to address these problems and safeguard both individual privacy rights and public safety.167

Transparency is a crucial component in striking a balance between public safety and privacy. Law enforcement organizations must be transparent about the technologies they employ, the methods they use to gather data, and the privacy protections they have in place. This entails creating and disseminating explicit guidelines for the use, storage, and access to data.168

Participation from the community is essential to this process. By engaging locals in conversations about emerging technologies, law enforcement can allay fears up front

[165] ibid
[166] ibid
[167] ibid
[168] ibid

and foster confidence. Regular updates regarding technology use, community advisory boards, and public forums can all aid in bridging the divide between the public and the police.169

Uganda currently lacks a consolidated and privacy focused surveillance law. While laws like the Regulation of Interception of Communications Act (RICA) 2010 and the Computer Misuse Act 2011 permit surveillance, they lack strong privacy safeguards to balance security and privacy.

The outdated laws should be reformed for example RICA should be amended to include judicial oversight before and when intercepting communications. This would prevent abuse by security agencies.

There should be an enactment of a data protection law with enforcement powers. Even though Uganda has the Data Protection and Privacy Act 2019, its enforcement is weak. Strengthening the Personal Data Protection Office (PDPO) would ensure that data collected via surveillance is lawfully processed and stored.

Security agencies like ISO, CMI, ESO, and police should not operate without checks. An independent parliamentary committee on surveillance can approve and review surveillance warrants, investigate abuses and hold actors accountable and ensure surveillance programs are proportionate to threats. To ensure accountability, the Investigatory Powers Tribunal in the UK, for instance, considers accusations of illegal surveillance by security agencies.

[169] ibid

Public awareness campaigns should teach Ugandans about their data rights under the law, how to report surveillance abuse and the importance of privacy in a democratic society. This empowers citizens to demand accountability and use digital tools responsibly. For example in Estonia digital literacy programs help citizens understand E-governance systems and how data is managed, improving trust.

Collaboration with Civil Society organizations like Unwanted Witness Uganda should be included in policy-making to ensure human rights are not sidelined. Similarly, telecom companies should be required to publish data on government surveillance requests.

A digital rights group called Unwanted Witness promotes the safe, open, and inclusive use of technology in support of good governance and the realization of human rights. Mukasa pointed out that the Interception of Communications Act of 2010 and Uganda's Data Protection and Privacy Act of 2019 both have a number of flaws.170

In an effort to reduce urban crime, the Ugandan government has started deploying CCTV cameras throughout the nation since January 2019. Following this, a 10-year contract was signed in June 2021 with Joint Stock Company Global Security, a Russian business that carries out the smart monitoring project in automobiles.171

Dr. Dianah Ahumuza Ateenyi stated that while national security is important, Ugandans' right to privacy must be balanced with it. "National security is living on technology," she remarked. It takes the shape of the nation's CCTV cameras and the

[170] https://observer.ug/news/loopholes-in-privacy-laws-a-threat-to-national-security-warn-experts/ accessed on 6th May,2025
[171] ibid

computerized auto trackers that will soon be mounted in our vehicles. How can we achieve a balance between privacy and individual liberties? How do we balance the two?172"The government is making huge investments in new surveillance technologies with the law that expands their surveillance powers. There's a need for more safeguards and accountability. We are increasingly observing the privatization of public responsibilities through public-private surveillance partnerships without any human rights safeguards. There is a need for more scrutiny to ensure that human rights are not quietly abused, especially when the systems deployed are used for the mass processing of personal data. The data protection law gives leeway for surveillance for purposes of national security".

Section 7 of the Data Protection and Privacy Act of 2019 highlights national security among the necessary scenarios under which personal data can be collected. Section 13 subsection 3(b) of the same law notes, among other loopholes, that a data subject might not be informed when their data is being collected from a third party if the action is related to national security.173

Dr. Dianah Ahumuza Ateenyi observed that because young people make up the majority of Uganda's population, the competitions would give young people from various law schools in the nation a chance to demonstrate their knowledge of the country's privacy laws, identify any flaws in the legal system, and suggest fixes for the gaps.174

[172] ibid
[173] ibid
[174] ibid

Speaking at the same event, Dr. Dianah Ahumuza Ateenyi, who oversees Clinical Legal Education (CLE) at Makerere University's Public Interest Law Clinic (PILAC), reaffirmed the necessity of strengthening Uganda's privacy regulations to guarantee the security of user data.

the ones relevant Ahumuza claimed that the commercial sector was falling behind in protecting Ugandans' data, using the 2022 privacy scorecard created by Unwanted Witness.175

According to the scorecard, which examined data handling practices in Kenya and Uganda, businesses in both nations are not particularly interested in protecting personal information from unauthorized access, deletion, change, disclosure, or destruction.176

It was also determined that, throughout the year under review, no corporation in either country had released a transparency report that included important metrics and details about data governance and enforcement practices.177

Uganda should adopt international norms for human rights and align its surveillance policies with instruments like the International Covenant on Civil and Political Rights (ICCPR) which guarantees privacy under Article 17 and the African Charter on Human and Peoples Rights protecting personal liberty and dignity.

Parliament is mandated to make laws pertaining to any matter for the systematic functioning, and effective administration of Uganda. Additionally, it is obligated to

[175] ibid
[176] ibid
[177] ibid

safeguard the integrity of this Constitution and advance the principles of democratic governance within Uganda.178 To its efficient discharge of its functions, it has a number of committees179and to the National ID include: The Committee on Equal Opportunities; the Committee on Human Rights; the Committee on Information, Communication Technology and National Guidance; the Committee on Legal and Parliamentary Affairs; the Committee on Gender, Labor and Social Development; the Committee on Finance, Planning and Economic Development; and Budget Committee. Parliament should amend Section 65180 of the Act to provide a more precise and well-defined list of permissible purposes for which data in the register can be used. While the inclusion of national security and law enforcement purposes is crucial, the current phrasing of "any other purpose" is overly broad and could potentially lead to the misuse of personal data and revise the data collection requirements in Schedule 3 to limit the collection of sensitive personal information to what is strictly necessary for identification purposes. By minimizing data collection, NIRA can reduce the burden of managing and securing vast amounts of data and uphold individuals' privacy rights.181.

[178] Article 79(1) & (3) of the Constitution of the Republic of Uganda, 1995, as amended.
[179] Article 90 of the Constitution of the Republic of Uganda, 1995 as amended
[180] Registration of the Persons Act, 2015
[181] https://www.unwantedwitness.org/wp-content/uploads/2024/06/UW-position-paper-07.06.2024-Full.pdf accessed on 6th May 2025.

6.0 CHAPTER SIX

6.1 SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

6.1.1 Introduction

This chapter presents the key findings arising from the analysis of mass surveillance practices in Uganda in relation to the protection of personal privacy and national security imperatives. Drawing from primary and secondary sources, including statutory analysis, policy review and academic discourse, the chapter outlines core conclusions and proposes actionable recommendations to address the tension between state surveillance and individual rights in Uganda. The chapter ultimately aims to contribute toward the establishment of a democratic, lawful, and rights –sensitive surveillance regime.

6.1.2 Key Findings

Weak legal safeguards in Uganda's Surveillance Framework

The current legal framework governing surveillance in Uganda, especially the Regulation of Interception of Communications Act (2010) and the Computer Misuse Act (2011) lack clear comprehensive safeguards for the right to privacy. These laws permit state actors to conduct surveillance with minimal judicial oversight, creating potential for abuse. There is no centralized, independent supervisory authority overseeing the issuance and implementation of surveillance measures.

Disproportionate and non-transparent surveillance practices

Evidence suggests that security agencies operate in a culture of secrecy, often carrying out surveillance without informing the public or affected individuals. This undermines the principle of proportionality, which requires that surveillance be necessary, targeted, and limited in scope. State agencies like Internal Security Organization (ISO) and the Chieftaincy of Military Intelligence (CMI) reportedly conduct unwarranted monitoring, particularly during elections or political protests.

Limited Enforcement of Data Protection Office (DDPO) lacks adequate funding, staffing, and independence to act as an effective watchdog. There are few known enforcement actions or penalties for unauthorized data collection or breaches, particularly involving government entities.

Public Awareness and Civic Participation Remain Low

A significant portion of the Ugandan population remains unaware of their rights regarding data privacy and surveillance. Moreover, civil society engagement in surveillance policy making is limited. Surveys by organizations such as Unwanted Witness indicate that many citizens do not understand the scope of surveillance or how to challenge violations.

Civil society actors are often excluded from discussions on national security laws and digital policy development.

Tension between National Security and Human Rights

The Ugandan government frequently invokes national security to justify surveillance, often at the expense of constitutionally guaranteed rights such as freedom of expression 182 and the right to privacy183 .

Security justifications are often used to monitor opposition members, activists and journalists, indicating a politicized use of surveillance tools.

6.1.3 Recommendations

Reform and Harmonize Surveillance laws

There is an urgent need to review and amend existing surveillance legislation to align it with international human rights standards such as the ICCPR and the African Charter on Human and Peoples Rights.

Judicial authorization as a mandatory requirement before any surveillance measure to be implemented.

Surveillance should be limited to predefined serious security threats

Explicit safeguards against misuse should be included and provide remedies for victims of unlawful surveillance.

Strengthen Oversight and Accountability Mechanisms

Independent oversight is critical for balancing state power with individual rights. The government should establish a dedicated Surveillance Oversight Authority, separate from the executive, to oversee state surveillance activities.

[182] Article 29 of the Constitution of The Republic Of Uganda 1995
[183] Article 27 of the Constitution of The Republic Of Uganda 1995

Parliament should be empowered to conduct regular reviews of surveillance programs and publish oversight reports

Empower the Personal Data Protection Office.

The PDPO should be adequately resourced and empowered to act independently in reviewing surveillance data collection.

It should also mandate all security and government institutions to conduct Privacy Impact Assessments before implementing new surveillance systems.

Promote Public Awareness and Civic Participation

Citizen engagement is essential to ensuring that surveillance practices respect rights. Government should launch national campaigns to educate the public on data privacy and legal protections.

Civil society organizations such as Unwanted Witness should be included in consultations on new surveillance policies and technology procurement.

Implement Technical Safeguards and Limit Data Retention

Privacy respecting technologies should be incorporated and data minimization principles into surveillance systems and also enforcement of encryption standards for stored surveillance data.

6.1.4 Conclusion

Uganda's current approach to mass surveillance places undue emphasis on security while insufficiently protecting personal privacy. Without reform, this imbalance

threatens democratic governance and civil liberties. However, with legal, institutional, and public policy adjustments, Uganda can strike a sustainable balance that upholds national security while safeguarding the dignity and rights of its citizens. The recommendations provided in this chapter are intended to guide stakeholders, government, civil society, and international partners toward the realization of a just, transparent, and accountable surveillance regime in Uganda.

7.0 BIBLIOGRAPHY

7.1 STATUTES

The Constitution of the Republic of Uganda 1995

The Regulation of Interception of Communications Act, 2010

The Computer Misuse Act 2011

Electronic Transactions Act 2011

Electronic Signatures Act 2011

The Anti –Terrorism Act, 2002

Registration of the Persons Act, 2015

7.2 ONLINE JOURNALS

For God and My President: State Surveillance In Uganda> https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

The Dangers of Surveillance - Harvard Law Review >https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

No to Big Brother: The Legality and Implications of Mass Digital Surveillance InUganda>https://iuea.ac.ug/facultyoflaw/sitepad-data/uploads/2025/02/Nasser-Konde-No-to-Big-Brother-The-Legality-and-Implications-of-Mass-Digital-Surveillance-in-Uganda.pdf

Scrap new surveillance system, HRW tells Uganda https://www.theeastafrican.co.ke/tea/news/east-africa/scrap-new-surveillance-system-hrw-tells-uganda-4433356

Where Your Car License Plate Is a Spy, Daily Brief November 14, 2023 https://www.hrw.org/video-photos/audio/2023/11/14/where-your-car-license-plate-spy-daily-brief-november-14-2023

Have Uganda's Digital ID Cards Become a Tool for Mass Surveillance?https://techlabari.com/have-ugandas-digital-id-cards-become-a-tool-for-mass-surveillance/

A GPS Tracker on Every "Boda Boda": A Tale of Mass Surveillance in Ugandahttps://chrgj.org/2021-10-13-boda-boda-mass-surveillance-uganda/

Covid-19 surveillance in Kenya and Uganda is reducing people's rights.https://www.article19.org/covid-19-reduced-peoples-rights-in-kenya-and-uganda/

https://www.google.com/search?client=firefox-b-d&q=kizza+besigye+case+today

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

Loopholes in privacy laws a threat to national security, warn experts https://observer.ug/news/loopholes-in-privacy-laws-a-threat-to-national-security-warn-experts/

How to Balance Privacy and Public Safety in the Digital Age https://zencity.io/how-to-balance-privacy-and-public-safety-in-the-digital-age/#:~:text=One%20of%20the%20keys%20to,usage%2C%20retention%2C%20and%20access

Mass Surveillance https://privacyinternational.org/learn/mass-surveillance

Anti-terrorism regulation and the media in Uganda https://verfassungsblog.de/os4-uganda/

New computer misuse law threatens freedom of expression, activists sayhttps://acme-ug.org/2022/10/17/new-computer-misuse-law-threatens-freedom-of-expression-activists-say/

StateofInternetFreedomhttps://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2018-Resized.pdf

A Section of Uganda's Computer Misuse Act Outlawed! But, the Greater Part of the law remains thorny https ://cipesa.org/2023/01/a-section-of-ugandas-computer-misuse-act-outlawed-but-the-greater-part-of-the-law-remains-thorny/

CHOGM spy cameras now mere scarecrow? https://www.independent.co.ug/chogm-spy-cameras-now-mere-scarecrow/

Government has started installing CCTV cameras in different parts of Kampala.>https://twitter.com/ntvuganda/status/1036696599504801792

The Government Starts Installing CCTV Cameras In Major Urban Centers! https://newslexpoint.com/government-starts-cctv-camera/

President Museveni Orders Installation of Security Cameras https://ugandaradionetwork.net/story/president-museveni-directs-installation-of-security-cameras

Huawei infiltration in Uganda https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda Uganda's cctv system records 95 efficiency phase three to expand surveillance https://www.dailywestnile.info/news-now/uganda-s-cctv-system-records-95-efficiency-phase-three-to-expand-surveillance

Uganda's cash-strapped cops spend $126 million on CCTV from Huawei https://www.reuters.com/article/technology/ugandas-cash-strapped-cops-spend-126-million-on-cctv-from-huawei-idUSKCN1V50QL/

What Ugandan authorities are doing limit impact online opposition voices https://www.dandc.eu/en/article/what-ugandan-authorities-are-doing-limit-impact-online-opposition-voices accessed on 1st March,2025

Uganda creates unit spy social network https://rsf.org/en/uganda-creates-unit-spy-social-network

Uganda steps up pressure on social media critics ahead of 2026 polls https://cipesa.org/2025/04/uganda-steps-up-pressure-on-social-media-crtitics-ahead-of-2026-polls/

Uganda rolls out digital car number plates projects https://portal.itms.ug/blog/itms-in-media-1/uganda-rolls-out-digital-car-number-plates-projects-2

Uganda's digital number plates face scrutiny over tracking failures contractor capacity https://pmldaily.com/news/2025/02/ugandas-digital-number-plates-face-scrutiny-over-tracking-failures-contractor-capacity.html

Sharing citizen's biometric data from national id with telecom companies is intended to deal a plot for mass surveillance https://www.unwantedwitness.org/sharing-citizens-biometric-data-from-national-id-with-telecom-companies-is-intended-to-seal-a-plot-for-mass-surveillance/

Rollout of digital number latest poses privacy concerns in Uganda https://cipessa.org/2024/08/rollout-of-digital-numbber-plates-poses-privacy-concerns-in-Uganda

Collin's Dictionary http://www.collinsdictionary.com/dictionary/english/nationalsecurity

Unlawful sim card validation exercise is a threat to anonymity and privacy https://www.unwantedwitness.org/unlawful-sim-card-validation-exercise-is-a-threat-to-anonymity-and-privacy/

SafeBoda involved in personal data sharing with third parties https://www.unwantedwitness.org/revealed-safeboda-involved-in-personal-data-sharing-with-third-parties-unwanted-witness-report/

Impact of the anti-terrorism act implementation to the enjoyment of the right to privacy https://www.unwantedwitness.org/uw-policy-brief-impact-of-the-anti-terrorism-act-implementation-to-the-enjoyment-of-the-right-to-privacy/

Citizens under suspicion responsive research with community under suspicion responsive research with community under surveillance https://www.researchgate.net/publication/295076458_Citizens_under_Suspicion_Responsive_Research_with_Community_under_Surveillance

7.3 CASE LAW

United States of America v Jones 565 US.400 (2012)

Szabo and Vissy v Hungary App no 37138/2014

Charles Onyango Obbo v AG [2004] UGSC 1