A FRAMEWORK FOR MITIGATING SPYWARE-ENABLED SURVEILLANCE RISKS

CASE STUDY: UGANDA

Ainedembe Denis[1], Joseph Brian M. Kasozi[2]

[1,2]Faculty of Science, Uganda Martyrs University, Kampala, Uganda.

[1]ainedembe.denis@stud.umu.ac.ug

[2]bkasozi@umu.ac.ug

MAY, 2026

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACHPR	African Commission on Human and Peoples' Rights
ANOVA	Analysis of Variance
API	Application Programming Interface
AU	African Union
CCTV	Closed-Circuit Television
CI	Contextual Integrity
CIPESA	Collaboration on International ICT Policy in East and Southern Africa
CMI	Chieftaincy of Military Intelligence
COVID-19	Coronavirus Disease 2019
CSF	Cybersecurity Framework
DPPA	Data Protection and Privacy Act (2019)
E2EE	End-to-End Encryption
EAC	East African Community
FWaaS	Firewall as a Service
GPS	Global Positioning System
GSMA	Global System for Mobile Communications Association
ICT	Information and Communication Technology
IoC	Indicators of Compromise
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITMS	Intelligent Transport Monitoring System
ITU	International Telecommunication Union
MDM	Mobile Device Management
MVT	Mobile Verification Toolkit
NIST	National Institute of Standards and Technology
NITA-U	National Information Technology Authority - Uganda
NSO	NSO Group (Commercial spyware vendor)

ODPC	Office of the Data Protection Commissioner (Kenya)
OHCHR	Office of the High Commissioner for Human Rights (United Nations)
OTT	Over-The-Top (referring to the social media tax)
PbD	Privacy by Design
RAT	Remote Access Trojan
RCS	Remote Control System (Spyware)
RFID	Radio-Frequency Identification
RICA	Regulation of Interception of Communications Act (2010)
SES	Spyware-Enabled Surveillance
SIM	Subscriber Identity Module
SMEs	Small and Medium Enterprises
SPSS	Statistical Package for the Social Sciences
SS7	Signaling System No. 7
STS	Socio-Technical Systems
TAG	Threat Analysis Group (Google)
TFGBV	Technology-Facilitated Gender-Based Violence
UCC	Uganda Communications Commission
UI	User Interface
UMRA	Uganda Microfinance Regulatory Authority
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UPF	Uganda Police Force
UX	User Experience
VPN	Virtual Private Network
WOUGNET	Women of Uganda Network

LIST OF SYMBOLS

χ^2	Chi-square (Statistical test for association)
ρ	Spearman's Rank Correlation Coefficient (Rho)
r	Pearson Product-Moment Correlation Coefficient
H	Kruskal-Wallis H Statistic (Non-parametric ANOVA equivalent)
F	F-statistic (Used in ANOVA for comparing group means)
p	Probability Value (Significance level)
df	Degrees of Freedom
SD	Standard Deviation (Measure of data dispersion)
N / n	Total Sample Size / Sub-sample Size
M	Arithmetic Mean (Average)
$\approx$	Approximately equal to
<	Less than
>	Greater than
* / **	Significance at the 0.05 level / 0.01 level

ABSTRACT

This study investigated spyware-enabled digital surveillance within mobile ecosystems, proposing a generalizable socio-technical framework for risk mitigation and utilizing Uganda as a primary case study for validation. The research explored surveillance practices and actors, assessed impacts on privacy, trust, and power, and analyzed how user practices and policy environments shape exposure. Guided by Socio-Technical Systems (STS) Theory, supplemented by the Contextual Integrity framework and Privacy by Design principles, the study adopted an Interpretivist Philosophy and a Mixed-methods design. Data were collected from 320 survey respondents and 10 key informants in Uganda, supplemented by a Modified Delphi validation with 8 experts.

Findings revealed that spyware-enabled surveillance is pervasive across institutional, commercial, and interpersonal contexts, with 71.6% of respondents indicating awareness or suspicion of covert monitoring. The study established that surveillance significantly erodes trust in digital platforms (mean trust score 2.69/5) and triggers widespread self-censorship, with over 70% of users adapting their behavior due to privacy concerns. Results identified a critical implementation gap: while 62.2% of users lacked awareness of legal protections, over 50% had never received digital safety training, leaving them vulnerable to sophisticated mercenary spyware and interpersonal "stalkerware." Weak enforcement of the Data Protection and Privacy Act (2019) and limited institutional forensic capacity were identified as primary structural barriers.

Based on these findings, the study developed a framework, which integrates user empowerment, organizational governance, technical infrastructure, and legislative reform. The study concludes that mitigation requires a shift from individual responsibility to multi-stakeholder accountability. It recommends state-provisioned protective tooling, decentralized digital literacy, and the establishment of independent forensic rapid-response labs to enhance digital resilience, offering a model applicable to similar environments.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Mobile devices are now the primary gateway to the digital economy, with the global device ecosystem supporting over 9.2 billion active connections in 2025 (International Telecommunication Union, 2025). While the African continent averages a penetration of 92 subscriptions per 100 inhabitants (International Telecommunication Union, 2025), specific markets like Uganda have seen explosive growth (Mirembe et al., 2022). National sector statistics reveal a surge from approximately 37 million active mobile subscriptions in 2023 to over 45.7 million by 2024, with smartphone connections rising to approximately 19 million (Uganda Communications Commission 2023, Uganda Communications Commission 2024). While this rapid expansion has driven financial inclusion and civic participation, it has simultaneously exposed users to sophisticated digital risks, including "spyware-enabled surveillance". Such surveillance allows for the covert monitoring of devices to extract communications, location data, and intimate user activity without consent, transforming mobile technologies from tools of empowerment into potential instruments of invisible control (Chatterjee et al., 2018, Anglano, 2025, Deibert, 2022). The urgency of addressing these risks is reflected on the global stage; as a member representing Africa on the ITU Council, Uganda has actively advocated for international standards to build resilient and inclusive digital ecosystems (Uganda Communications Commission, 2026).

Globally, the proliferation of advanced spyware and surveillance technologies indicates that digital monitoring is no longer confined to exceptional national security contexts but is increasingly embedded within everyday digital infrastructures. The rise of the "Surveillance Industrial Complex" and the deployment of tools such as Pegasus and Predator illustrate how high-capability spyware can be utilized by both state and non-state actors to enable persistent monitoring across private and professional spheres with minimal transparency (Deibert, 2022, Katibah, 2023, Spens, 2024). Technical research confirms that modern spyware exploits complex software vulnerabilities, excessive application permissions, and social engineering to maintain stealth, creating a "detection gap" that renders traditional antivirus tools largely ineffective (Anglano, 2025, Chatterjee et al., 2018).

In Uganda, the risks associated with this technological evolution are particularly pronounced. Reports from investigative journalists and digital rights organizations highlight growing concerns regarding unexplained privacy intrusions and "digital intimidation," suggesting that spyware-enabled surveillance has moved into the realm of everyday digital life (Privacy International, 2015, Unwanted Witness, 2025, Musoke, 2025). Although Uganda has adopted formal legal instruments such as the Data Protection and Privacy Act (2019) and the National Cybersecurity Strategy (2022-2026), existing evidence suggests that institutional and regulatory protections have struggled to keep pace with rapid digitalization and the sophisticated nature of commercial surveillance capabilities (Uganda Ministry of ICT, 2023, Mirembe et al., 2022).

Recent scholarship increasingly frames this challenge as a socio-technical risk arising from the interaction of technological design, user practices, organizational routines, and governance environments. From this perspective, surveillance risks cannot be mitigated through technical controls alone but require integrated frameworks that align technological safeguards with institutional accountability and human factors (Sittig and Singh, 2016; Stefani et al., 2025; Tekeli, 2021). Alongside privacy concerns, scholars emphasize "digital resilience" as a critical outcome; referring to the capacity of individuals and systems to recognize, resist, and recover from surveillance harm (Budak et al., 2020). However, existing literature often frames resilience as an individual technical skill, paying limited attention to how broader socio-technical factors such as trust in digital systems and institutional power relations shape the ability to cope with spyware in Global South settings (Vissenberg et al., 2022; Ibrahim et al., 2025). Consequently, there is an urgent need for empirically grounded research that integrates these diverse perspectives into a unified framework for mitigating spyware-enabled surveillance risks in Uganda.

This study adopts a socio-technical perspective and designs a framework that brings together technical risk factors, user practices, and relevant governance considerations to mitigate spyware-enabled digital surveillance risks, utilizing Uganda as a case study for validation.

1.2 Statement of the Problem

Across Uganda, mobile devices played a central role in everyday communication, income-generating activities, professional work, and social relationships, and for many users they serve as the primary means of accessing digital services and participating online (Uganda Communications Commission 2024, Feldstein, 2019). While this deep integration had expanded opportunities for

connectivity and inclusion, it has also exposed users to new and often poorly understood forms of digital threats. As mobile devices increasingly mediated everyday interactions, they had become keys tools for covert monitoring and data extraction (Deibert, 2022).

A significant source of these risks is the growing use of spyware and digital surveillance technologies. Unlike visible cybersecurity threats, spyware operates covertly, enabling persistent monitoring of communications, location, and device activity without users' knowledge and consent (Chatterjee et al., 2018, Anglano, 2025). Although technical and security-focused research has documented spyware capabilities and detection challenges, this literature is largely based on Western contexts and provides limited insight into how surveillance is experienced within different socio-cultural and institutional environments (Deibert, 2022).

In Uganda, existing evidence on digital surveillance practices largely comes from investigative journalism, advocacy and reports focusing on state surveillance, civic space, and human rights (Privacy International, 2015, Unwanted Witness, 2025, Roberts and Mare, 2025)

While these sources provided valuable contextual insights, they rarely integrated technical characteristics of spyware with user practices, institutional roles, and governance mechanisms that shape everyday exposure and response to surveillance (Mirembe et al., 2022). As a result, there was limited empirical understanding of how spyware-enabled digital surveillance affects privacy, trust in digital systems, power relations, and digital resilience in everyday mobile technology use.

Overall, existing approaches to surveillance practices often examine technical, policy, and ethical concerns in isolation, resulting in limited evidence to guide effective mitigation strategies. As a result, there was insufficient understanding of how spyware-enabled surveillance affects privacy, trust, power relations, and digital resilience in everyday mobile technology use. This study addressed this gap by designing a socio-technical framework to support the mitigation of spyware-enabled digital surveillance risks, validated in the context of Uganda.

1.3 Purpose of the Study

The purpose of this study was to examine spyware-enabled digital surveillance associated with mobile device use, utilizing Uganda as a case study, and to design a socio-technical framework for mitigating related risks to privacy, trust, power relations, and digital resilience.

1.4 Objectives of the Study

1.4.1 Overall Objective

To design a socio-technical framework for mitigating spyware-enabled digital surveillance risks associated with mobile device use.

1.4.2 Specific Objectives

i. To examine spyware-enabled digital surveillance practices and related actors within Uganda's mobile digital ecosystem
ii. To explore how spyware-enabled digital surveillance affects users' privacy, trust, power and control in everyday digital behaviors.
iii. To analyze how user practices and existing policies, regulations, and organizational practices shape exposure to and responses to spyware-enabled digital surveillance.
iv. To design a socio-technical framework for mitigating spyware-enabled digital surveillance risks associated with mobile device use.

1.5 Research Questions

v. What forms of mobile-device spyware and digital surveillance are present within the Ugandan digital ecosystem?
vi. How does spyware-enabled digital surveillance affect users' privacy, trust, and sense of control in everyday mobile device use.
vii. How do users' everyday practices, together with existing policies, regulations, and organizational practices, shape exposure to and responses to spyware-enabled digital surveillance?
viii. How can insights from user experiences, surveillance practices, and existing approaches inform the design of a framework to mitigate spyware-enabled digital surveillance risks in Uganda?

1.6 Scope of the Study

The study was conducted in Uganda, with a focus on major urban and peri-urban centres across the four regions of the country, where mobile technology use was most concentrated. The study focused on spyware-enabled digital surveillance associated with mobile device use and examines its implications for users' privacy, trust, power relations, and digital resilience.

The study adopted a socio-technical perspective, considering both technological mechanisms and everyday user experiences, as well as relevant policies and organizational practices that shape surveillance risks and responses.

With regard to time scope, the study drawn primarily on literature published between 2015 and 2025 to capture recent developments in spyware technologies, digital surveillance practices, and regulatory responses. The research itself was expected to be conducted over a period of six months, covering proposal refinement, ethical approval, participant recruitment, data collection, analysis, and framework design.

1.7 Significance of the Study

Academic Contribution: The study contributed empirical evidence to socio-technical and information systems scholarship on gendered digital surveillance, utilizing Uganda as a case study. It helped in filling the research gap concerning regional, intersectional, socio-technical studies, and expands on privacy, trust, power, and resilience literature.

Policy and Institutional Relevance: The findings inform ongoing debates on digital rights, cybersecurity, and gender-sensitive approaches to surveillance, with specific relevance to policy environments like Uganda. By highlighting how surveillance practices are experienced in everyday contexts, the study assists policymakers and regulatory institutions in identifying gaps in existing frameworks and considering measures that better protect vulnerable groups while promoting accountability.

Practical and Social Impact: The study was also of value to civil society organisations, digital rights advocates, and community groups by providing empirically grounded insights that can support digital awareness initiatives and discussions around trust, safety, and resilience in surveillance-shaped environments.

Beyond theoretical contributions, the study produces a practical research output in the form of the Uganda Surveillance Watch Dashboard; a digital artefact that operationalizes the proposed framework by aggregating real-time threat intelligence and providing a public reference point for surveillance awareness.

1.8 Justification of the Study

This study was motivated by the limited body of primary research examining gendered digital surveillance from a socio-technical perspective, with Uganda as the primary case study. Although existing scholarship has documented growing concerns around surveillance, privacy erosion, and declining trust in digital systems, much of this work remains at a general or institutional level. There is comparatively little research that explores how these dynamics are experienced in everyday digital life, or how they intersect with gendered power relations and people's capacities to adapt and respond.

By focusing on lived experiences and placing spyware and surveillance within broader social, institutional, and technological contexts, this study addresses these gaps. In doing so, it contributes empirically grounded insights that are relevant not only to academic debates on surveillance and socio-technical systems, but also to policy discussions in similar contexts.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter provides a review of literature relevant to spyware and digital surveillance, focusing on their socio-technical implications for privacy, trust, power, and digital resilience. Mobile devices, once primarily associated with connectivity and socio-economic empowerment, now increasingly function as sites through which monitoring and control can be exercised across institutional and interpersonal contexts.

The literature reviewed in this chapter includes academic research, technical security studies, and policy reports. This interdisciplinary approach reflects the socio-technical nature of spyware, which is examined through the interaction of technical mechanisms, user practices, and institutional arrangements. The chapter synthesizes global, regional, and Uganda-specific studies to identify areas of convergence and existing gaps that inform the development of the proposed mitigation framework.

2.1 Theoretical Review

The theoretical review is anchored in three interrelated pillars that collectively provide the analytical lens for this study; Socio-Technical Systems (STS) Theory, the Contextual Integrity (CI) framework, and the principles of Privacy by Design (PbD).

2.1.1 Socio-Technical Systems Theory

Socio-Technical Systems Theory, developed through the foundational work of Trist and Bamforth (1951), challenges technological determinism by arguing that technologies and human actors cannot be treated as separate entities. Instead, the theory conceptualizes technical systems, user practices, organizational arrangements, and governance environments as interdependent elements of an integrated system (Trist and Bamforth, 1951, Emery and Trist, 1960). From this perspective, the effectiveness and consequences of any technology including spyware emerge not from the software alone, but from its interaction with broader social and institutional contexts.

Applied to digital surveillance, socio-technical perspectives have informed scholarship on how integrated frameworks can address risks that arise at the intersection of technical design and human behavior (Sittig and Singh, 2016, Stefani et al., 2025, Tekeli, 2021). This critique is particularly apposite in the Ugandan context, where surveillance practices have developed unevenly alongside

state digitalization strategies, often without corresponding investments in regulatory oversight or user-level protection (Mirembe et al., 2022). Within this lens, spyware is not understood as an isolated misuse of technology, but as a systemic outcome shaped by power asymmetries and governance constraints (Holden and Harsh, 2024).

2.1.2 Contextual Integrity Framework

To deepen the understanding of how spyware-enabled surveillance impacts privacy, this study utilizes the Contextual Integrity (CI) framework developed by (Nissenbaum, 2004). CI posits that privacy is not merely a right to secrecy, but a requirement for "context-relative informational norms." It suggests that privacy is violated when information intended for one context (e.g., personal messaging or mobile banking) is inappropriately diverted to another (e.g., state monitoring or commercial data scraping).

By adopting CI, the study moves beyond a binary "private vs. public" distinction and instead analyzes how spyware disrupts the "normative expectations" of Ugandan users. This framework provides the theoretical basis for Layer 4 (Legal & Policy) and Layer 5 (Civil Society) of the proposed mitigation strategy, as it highlights the need to restore integrity to informational flows within the mobile ecosystem (Nissenbaum, 2010).

2.1.3 Privacy by Design Principles

While STS and CI provide the diagnostic lens, Privacy by Design (PbD) provides the prescriptive pillar for mitigation. Pioneered by (Cavoukian, 2012), (PbD) advocates for the proactive integration of privacy protections into the very architecture of technical systems and organizational processes. It is defined by seven foundational principles, including "Privacy as the Default" and being "Proactive, not Reactive."

This study utilizes PbD to shift the focus from "blaming the user" for security failures toward a model of "systemic accountability." PbD provides the theoretical justification for the framework's emphasis on state-provisioned protective and mandatory point-of-sale digital onboarding (Layer 1). Ultimately, PbD ensures that digital resilience in Uganda is built into the foundational infrastructure of the mobile digital ecosystem rather than being a secondary addition.

2.2 Conceptual Review

2.2.1 Conceptualization of Core Constructs

The conceptual framework developed for this study is organized around five interrelated constructs: spyware, digital surveillance, privacy, trust, power, and digital resilience. These constructs were selected on the basis that they collectively capture the socio-technical dimensions of covert monitoring and its consequences for users, as established through the theoretical and empirical literature reviewed in this chapter. Each construct is defined below in relation to digital surveillance and the specific Ugandan context of this study.

Spyware refers to covert software designed to monitor, record, and extract data from digital devices without the informed consent of the user. Technical research identifies spyware as capable of accessing communications, location data, keystrokes, microphones, and cameras, often through the exploitation of software vulnerabilities, permission abuse, or social engineering techniques (Chatterjee et al., 2018, Anglano, 2025). Unlike overt monitoring systems, spyware is characterized by its persistence, invisibility, and capacity for continuous data extraction, making it a particularly intrusive form of surveillance technology.

Digital surveillance refers to the ways in which digital technologies are used to collect and process personal data in order to observe, anticipate, or influence behaviour (Lyon, 2018, Deibert, 2022). Rather than being limited to isolated technical systems, surveillance is increasingly understood as embedded within broader social and institutional settings. Contemporary scholarship therefore treats digital surveillance as a socio-technical practice, shaped not only by technological infrastructures, but also by legal frameworks, organizational arrangements, and prevailing social norms that influence how surveillance is implemented and experienced (Stevens et al., 2023).

Privacy is increasingly theorized as a relational and political condition rather than solely an individual right to data protection (Keen, 2022). Surveillance scholarship highlights that privacy violations generate broader social harms, including chilling effects on communication, participation, and trust (Lyon, 2018). Feminist perspectives further stressed that privacy is unevenly distributed, with violations disproportionately affecting individuals situated within asymmetric power relations, particularly in intimate and domestic contexts (Imam et al., 2025).

Trust is a multi-dimensional construct encompassing interpersonal trust, institutional trust, and trust in digital platforms and infrastructures (Lu and Yi, 2023). Research consistently demonstrates

that pervasive surveillance erodes trust by introducing uncertainty, encouraging self-censorship, and altering behavior (Ryan and Tynen, 2020). These effects are not uniform; gendered power relations shape whose trust is undermined and how surveillance reshapes social and institutional relationships.

Power is central to surveillance analysis. (Dahl, 1957) defines power relationally as the ability of one actor to influence the behavior of another in ways that would not otherwise occur. Applied to surveillance, this perspective directs attention to how control was exercised through access to data, technological design, institutional authority, and social positioning. Applied to spyware and digital surveillance in this study, power was understood as the uneven capacity of actors to influence others across economic, political, social, organizational, and intimate domains.

Digital resilience refers to the capacity of individuals and communities to recognize digital threats, adapt their practices, recover from harm, and navigate digitally mediated environments over time (Budak et al., 2020, Sun et al., 2022). Global South scholarship reframes resilience as relational and constrained, emphasizing collective coping strategies and negotiated engagement within systems of inequality (Ibrahim et al., 2025). This framing avoids individualizing responsibility and highlights how resilience is shaped by gendered power relations and socio-technical conditions.

2.2.2 Conceptual Framework

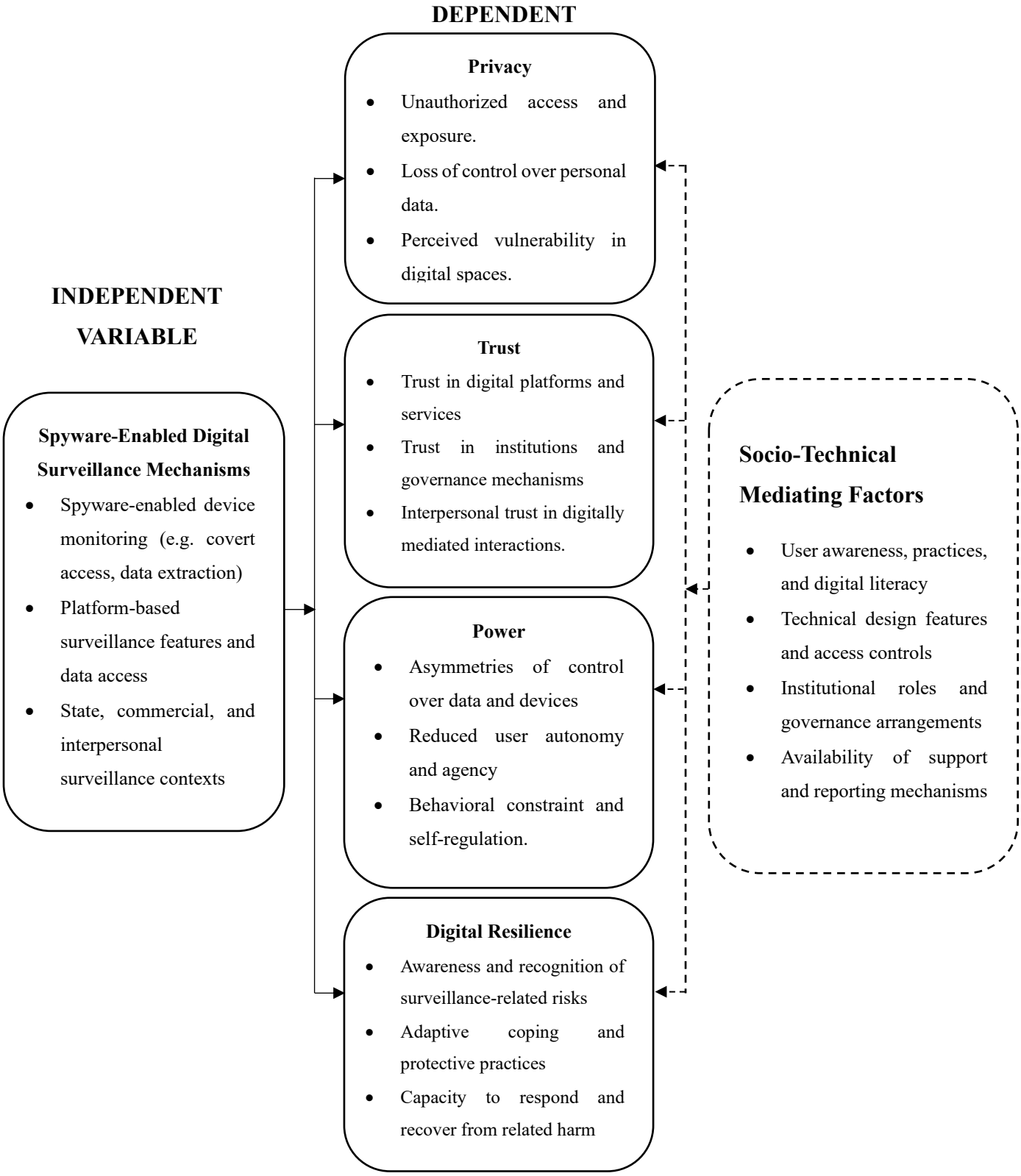

Figure 1: Conceptual Framework

Source: Adapted from socio-technical systems theory and surveillance studies literature

2.2.3 Narrative Explanation of the Conceptual Framework

The conceptual framework proposed that spyware-enabled digital surveillance mechanisms influence users' privacy, trust, power relations, and digital resilience through interconnected and mutually reinforcing processes rather than through simple, linear cause-effect relationships. Surveillance mechanisms including spyware-enabled device monitoring, platform-based data access, and surveillance enacted across state, commercial, and interpersonal contexts create conditions under which personal data was accessed without authorization, user autonomy may be constrained, and everyday digital interactions become subject to heightened monitoring.

Within the framework, the dependent variables that are; privacy, trust, and power are positioned as closely related outcome dimensions that interact dynamically. Intrusions into privacy such as covert data extraction or loss of control over personal information can undermine trust in digital platforms, institutions, and digitally mediated relationships. At the same time, diminished trust normalized surveillance practices or reduce users' willingness to challenge or resist monitoring, thereby reinforcing existing asymmetries of control and contributing to behavioral constraint and self-regulation (Stevens et al., 2023, Tabasum et al., 2025).

The framework further recognized that the effects of spyware-enabled surveillance are not uniform across users but are shaped by socio-technical mediating factors. These included users' awareness, practices, and levels of digital literacy; the design features and access controls embedded within digital technologies; institutional roles and governance arrangements; and the availability of support and reporting mechanisms. Together, these factors condition how surveillance mechanisms translate into lived experiences of privacy loss, trust erosion, and power imbalance, without acting as direct causal variables themselves.

Digital resilience is conceptualized both as an outcome of exposure to surveillance risks and as an adaptive process through which users respond to and manage such risks over time. Users develop awareness of surveillance practices, adopt protective or precautionary behaviors, modify their digital routines, or seek social and institutional support in response to perceived threats. However, the capacity to build and sustain digital resilience was uneven, shaped by access to resources, technical knowledge, and supportive socio-technical environments (Ibrahim et al., 2025).

Overall, the conceptual framework positioned privacy, trust, power, and digital resilience as interrelated dimensions of everyday digital life under conditions of spyware-enabled surveillance. The framework emphasized that the impacts of surveillance emerge from the interaction between technological mechanisms and socio-technical mediating factors, rather than being determined solely by technology itself. This perspective provided a structured basis for analyzing surveillance risks and for informing the development of a framework to address spyware-enabled digital surveillance risks in the Ugandan context.

2.3 Empirical Review

2.3.1 Digital Surveillance in the Contemporary Socio-Technical Context

Digital surveillance has evolved from targeted interception into an ambient, automated, and often invisible process embedded within everyday digital infrastructures. Feldstein's comparative analysis of AI-enabled surveillance provides one of the most comprehensive global mappings of this shift, documenting the deployment of smart city platforms, facial recognition systems, and predictive policing technologies in at least 75 of 176 countries worldwide (Feldstein, 2019). Notably, this diffusion cut across regime types, with both democracies and authoritarian states adopting similar surveillance capabilities. (Feldstein, 2019) argued that the determining factor in whether such technologies are abused is not regime classification per say, but the quality of governance, oversight, and accountability mechanisms.

This argument resonates with broader surveillance scholarship, which increasingly frames monitoring as a structural feature of contemporary digital societies rather than an exceptional state practice (Lyon, 2018). Surveillance is no longer confined to specific investigations but is embedded within platforms, infrastructures, and devices that mediate everyday communication, financial transactions, and social interaction (Andrejevic, 2014). The ubiquity of mobile devices, in particular, has intensified surveillance capacity by concentrating vast amounts of personal data communications, location, biometrics, and social networks into always-connected, sensor-rich objects carried at all times (OHCHR, 2022). Spyware and Surveillance technology, from this perspective, was produced not only by technical capability but by organizational routines, policy choices, and cultural normalization (Harkin et al., 2020).

From a socio-technical perspective, surveillance was therefore not merely a function of technical capability but of how technologies are designed, procured, regulated, and socially normalized (Emery and Trist, 1960, Harkin et al., 2020). This perspective was particularly relevant in the Ugandan context, where the rapid spread of digital technologies had not always been matched by equivalent growth in institutional capacity, clear regulatory guidance, or widespread public understanding of digital risks. As a result, surveillance practices often emerged in ways that are partially regulated and unevenly understood by users.

2.3.2 Spyware as an Extreme Form of Digital Surveillance

Within the wider landscape of digital surveillance, spyware is widely regarded as one of the most intrusive forms of monitoring. Unlike more visible or regulated surveillance practices, spyware typically operates covertly, remains active over extended periods, and provides extensive access to personal devices. Both academic research and technical investigations indicated that spyware can bypass conventional consent processes, exploit so-called “zero-click” vulnerabilities, and allow operators to access devices without the knowledge of the use (Chatterjee et al., 2018, Deibert, 2022, Pierazzi et al., 2020). Once deployed, spyware such as Pegasus or FinFisher extracted messages, emails, photos, and videos; monitor encrypted applications; track real-time location; and activate microphones and cameras, effectively turning personal devices into continuous surveillance instruments (Deibert, 2022). These capabilities fundamentally challenged liberal assumptions about user agency and informed consent in digital environments.

For analytical precision, this study distinguishes between three tiers of mobile spyware that differ in sophistication, detectability, and typical deployment context. The first tier comprises commodity stalkerware: commercially available, low-sophistication applications that are generally detectable by standard anti-malware tools and are primarily deployed in interpersonal surveillance contexts, including domestic abuse, coercive control, and intimate partner monitoring (Chatterjee et al., 2018, Anglano, 2025). The second tier covers open-source Remote Access Trojans (RATs), such as AhMyth and AndroRAT. Originally developed as legitimate remote administration tools and academic projects respectively, these have been widely weaponized by cybercriminals across East Africa to extract SMS messages (including one-time passwords), intercept calls, track location, and enable unauthorized microphone and camera access (Anglano, 2025)

Their medium-sophistication profile means they are increasingly evading detection through obfuscation techniques and distribution via trojanized applications. The third and most severe tier encompasses state-grade mercenary spyware, such as by NSO Group's Pegasus and Intellexa's Predator. These tools exploit zero-click vulnerabilities requiring no user interaction, operate at the kernel level of the device's operating system, and remain virtually undetectable by any commercially available security software (Deibert, 2022, OHCHR, 2022, Amnesty International, 2023). Mitigation strategies, detection methods, and policy responses differ substantially across these three tiers, and this classification informs the differentiated prescriptions.

The technical sophistication of modern spyware has continued to evolve, with the threat landscape shifting from malware requiring user interaction to zero-click exploits that require no action from the target (Deibert, 2022). Against state-grade tools, traditional signature-based detection systems are largely ineffective, creating a persistent detection gap that technical countermeasures alone cannot close (Deibert, 2022, Anglano, 2025). A significant advancement in this space is the Amnesty International Security Lab's open-source Mobile Verification Toolkit (MVT), a command-line forensic tool that scans device artifacts against known Indicators of Compromise (IOCs) to identify traces of Pegasus and comparable mercenary spyware on both iOS and Android devices (Amnesty International Security Lab, 2021). MVT represents the current best-in-class approach available for independent civil society forensics and is a key tool recommended within the framework proposed in Chapter Five of this study. This broader detection failure reinforces the case for a socio-technical approach to mitigation that addresses not only technical defenses but also the institutional, legal, and user-level conditions that shape surveillance risk.

Authoritative policy documentation by the United Nations Office of the High Commissioner for Human Rights (OHCHR) provided large-scale empirical evidence of spyware proliferation. The OHCHR reported that at least 65 governments have acquired commercial spyware, supported by a global industry of more than 500 surveillance technology vendors. This policy report drew on forensic investigations, court records, and verified disclosures, confirming NSO Group alone targets between 12,000 and 13,000 individuals annually, and that Pegasus spyware alone has been linked to over 50,000 targeted phone numbers worldwide, including journalists, politicians, and human rights defenders (OHCHR, 2022). These findings challenged narratives that frame spyware

as a narrowly targeted or exceptional security tool, instead revealing its routine deployment within global surveillance practices.

Technical peer-reviewed research complements these findings by demonstrating that spyware was not limited to state-grade tools. (Chatterjee et al., 2018)'s large-scale measurement study of consumer spyware identified hundreds of Android applications capable of intimate surveillance, many of which were distributed through official app stores and marketed as benign tools for child safety or device recovery. These applications enabled covert tracking, message extraction, call recording, and remote device control. Alarmingly, less than 3% of such applications were detected by widely used anti-spyware tools, highlighting the limited effectiveness of user-level technical countermeasures (Chatterjee et al., 2018). Subsequent technical reviews verify these findings, showing that modern surveillance ware exhibits high stealth, extensive permissions abuse, and resilience against detection (Liu et al., 2023, Anglano, 2025). In some documented cases, surveillance-grade software has been found pre-installed on commercially sold Android devices, eliminating the need for active deployment against the target (Baran, 2025).

These studies revealed how practices commonly associated with state surveillance increasingly overlap with those found in consumer and commercially available spyware. As a result, the boundaries between what was legally sanctioned, unlawfully deployed, or socially normalized surveillance have become less distinct in everyday digital life. This situation raised important questions about policy approaches that emphasize individual responsibility for digital security while paying less attention to the institutional and commercial forces that shape surveillance environments.

2.3.3 The Spyware Industrial Complex and the Political Economy of Surveillance

The proliferation of spyware cannot be understood as the work of isolated actors or opportunistic criminals. It is instead the product of a structured, globalized industry which scholars have termed the as "spyware industrial complex" in which private vendors, security consultants, intelligence agencies, and venture capital networks form mutually reinforcing relationships that sustain and expand commercial surveillance as a market (Spens, 2024).. The scale of this ecosystem is mapped by resources such as the Surveillance Watch interactive tool, which documents the cross-border corporate affiliations and funding structures linking surveillance technology companies to state and institutional clients worldwide (SurveillanceWatch.io, 2025). The Atlantic Council's inventory

of commercial spyware markets similarly confirms that surveillance is no longer an ad hoc, state-managed activity but a structural feature of global digital infrastructure, one driven by competitive commercial incentives and enabled by weak international regulatory oversight (Atlantic-Council, 2023).

At the heart of this political economy is the commodification of personal data. Harkin et al. (2020) argue that mobile phone surveillance has become a commodity in its own right whereby personal data is extracted, packaged, and monetized by private firms operating within permissive regulatory environments that have failed to keep pace with commercial innovation (Harkin et al., 2020). Deibert (2022) extends this analysis through the systematic forensic work of the Citizen Lab, characterizing the spyware industry as functioning as "despotism-as-a-service", enabling governments with limited institutional safeguards to acquire the most sophisticated surveillance capabilities with minimal accountability, and at scale (Deibert, 2022). This framing is reinforced by evidence of weak international export controls, legally opaque procurement mechanisms, and an absence of effective redress for individuals whose communications have been unlawfully intercepted (OHCHR, 2022).

These dynamics are not confined to the Global North. Investigative studies of digital surveillance in East and Southern Africa reveal that the same procurement patterns, foreign vendor dependency, secretive tendering processes, and the temporal alignment of surveillance acquisitions with electoral periods operate with particular intensity in the region, where institutional oversight is weakest (Roberts and Mare, 2025, Unwanted Witness, 2025).

While such reports are policy- and advocacy-oriented rather than peer-reviewed, their methodological rigour grounded in forensic evidence, leaked procurement records, and verified disclosures provides the kind of contextually specific empirical insight that academic literature rarely achieves in under-researched regional settings. Together, these sources expose a surveillance economy that blurs the line between lawful security practice and institutionalized political control, underscoring the need for a socio-technical analytical lens that can account for the power relations embedded within these technological systems.

2.3.4 Digital Surveillance, Privacy and Human Rights

Traditionally, privacy had been understood as an individual's fundamental right to control the circulation of personal information, encompassing not only the ability to withhold such information but also the power to decide to whom and under what conditions it is shared (Westin, 1967) However, recent research indicated that this definition is increasingly inadequate in digital contexts, where invisible data flows, complex technological infrastructures, and asymmetries of knowledge between users and institutions make privacy more difficult to protect and experience (Lyon, 2018, Matzner, 2016). Spyware fundamentally undermines informational control by bypassing consent mechanisms entirely and exploiting vulnerabilities unknown even to device manufacturers.

(OHCHR, 2022) highlighted that spyware produces relational privacy harms by extending surveillance beyond direct targets to encompass entire social networks. This insight was echoed in technical analyses showing that compromised devices expose communications with third parties who have no knowledge of or ability to consent to surveillance (Deibert, 2022, Chatterjee et al., 2018). The United Nations Office of the High Commissioner for Human Rights (OHCHR, 2022) has characterized the deployment of commercial spyware against individuals as an assault on the 'very essence' of the right to privacy one that creates a chilling effect on civil society, free expression, and political participation that extends well beyond the directly targeted individual. This framing shifts privacy from an individual data protection concern to a structural human rights challenge, necessitating a mitigation response that is grounded not only in technical controls but in international human rights standards of necessity, proportionality, and accountability.

Research focused on Uganda highlights similar concerns. A national survey on digital human rights found significant gaps in awareness of digital privacy risks, with many participants unaware that smartphones could be monitored remotely without any visible signs (Mirembe et al., 2022). These findings suggest that legal recognition of privacy rights, such as those enshrined in Uganda's Constitution and the Data Protection and Privacy Act, has not translated into meaningful protection at the user level.

Historical investigative reports further confirmed that these risks have materialized, with FinFisher intrusion malware forensically linked to Ugandan security agencies between 2011 and 2013 (Privacy International, 2015). This evidence demonstrated that spyware use in Uganda was not

speculative but empirically established, reinforcing concerns about persistent privacy violations in the digital domain.

2.3.5 Surveillance, Trust, and Behavioral Change

In the field of Information Systems, trust plays a central role in shaping technology adoption, continued use, and user behavior. Eisend's meta-analysis demonstrates that behavioral reinforcement, social norms, and perceived control strongly influence digital behavior, often outweighing demographic factors (Eisend, 2019). Although not focused specifically on surveillance, these findings help explain why spyware-enabled monitoring can persist undetected: users tend to rely on habitual interaction with familiar platforms rather than maintaining continuous critical awareness of risk.

Surveillance erodes trust by introducing uncertainty regarding who has access to personal data, how that data is used, and for what purposes. Office of the High Commissioner for Human Rights (OHCHR) indicated that awareness of surveillance produces measurable chilling effects, with 25% of individuals modifying online behavior after learning about mass monitoring and between 34% and 61% engaging in self-censorship, or withdrawing from digital participation due to perceived monitoring (OHCHR, 2022). These findings align with sociological accounts of anticipatory compliance, where individuals regulate their behavior in response to the perceived monitoring.

Empirical studies from Uganda reflect similar dynamics. Survey-based research reports widespread self-censorship, low confidence in digital governance mechanisms, and limited trust in reporting or redress processes (Mirembe et al., 2022). Investigative reports further document how journalists and civil society actors anticipate digital monitoring during politically sensitive periods, reinforcing climates of suspicion and behavioral restraint (Privacy International, 2015, Unwanted Witness, 2025).

Importantly, trust erosion was not limited to state or institutional surveillance but also emerged within interpersonal and intimate digital contexts, where everyday technologies are repurposed for covert monitoring. Studies on technology-facilitated harm in Uganda document practices including WhatsApp Web session hijacking, remote location tracking, and unauthorized account access, which undermine interpersonal trust and reshape digital behavior within intimate relationships (Brown, 2024, Chisala-Tempelhoff and Kirya, 2024, AtomicMail, 2025).

Although these studies were primarily social-scientific, their findings were consistent with technical security research demonstrating the ease with which consumer spyware and platform features can be exploited for covert surveillance (Chatterjee et al., 2018, Liu et al., 2023). Together, this body of evidence highlights how spyware-enabled surveillance whether institutional or interpersonal changes trust relationships and encourages precautionary, avoidant, or self-censoring behavior in everyday digital life.

2.3.6 Systems Power as a Socio-Technical Capacity in Surveillance Systems

Surveillance and power had been extensively examined in the fields of surveillance studies, Information Systems, and political sociology, yet there was considerable variation in how power is conceptualized. A foundational and widely accepted definition was provided by (Dahl, 1957) who defines power relationally as the ability of one actor to influence the behavior of another in ways that would not otherwise occur. Importantly, Dahl's formulation is analytically neutral, focusing on observable influence rather than legitimacy, intent, or political authority. This relational understanding provides a useful baseline for analyzing power across diverse social, economic, and institutional contexts.

Building on this foundation, contemporary surveillance scholarship argues that digital technologies mediate power by reshaping how information was produced, accessed, and acted upon. (Lyon, 2018) and (Feldstein, 2019) demonstrate that modern surveillance operates less through direct coercion and more through informational asymmetries that enable anticipation, behavioral regulation, and strategic advantage. From this perspective, power was generated less through overt force and more through increased visibility and data-driven knowledge. This was evident in digital surveillance, where monitoring is integrated into everyday infrastructures such as mobile devices, online platforms, and databases (Harkin et al., 2020).

Socio-technical approaches further clarify this view by emphasizing that surveillance technologies do not exercise power on their own. As (Leese, 2021) argues, their influence emerges from socio-technical practices that combine technical capabilities with organizational routines, economic incentives, and human judgment. For instance, in predictive policing systems, power was exercised through how data outputs are interpreted and applied, rather than by automation alone. This perspective aligned with broader Information Systems research, which conceptualized power as

arising from interactions between technological artifacts and social systems (Emery and Trist, 1960, Harkin et al., 2020).

Empirical studies on spyware and other surveillance technologies reinforce this understanding. Both state-grade and consumer spyware create informational advantages by allowing covert access to communications, location data, and behavior patterns (Chatterjee et al., 2018, Deibert, 2022, OHCHR, 2022). Such capabilities shaped behavior through self-regulation and anticipatory compliance, even without direct enforcement (Volosevici and Isbasoiu, 2025). These effects are observed across institutional, organizational, economic, and interpersonal settings, including workplace monitoring, competitive intelligence, and intimate partner surveillance (Harkin et al., 2020, Brown, 2024).

Overall, the literature portrays power as a socio-technical capacity produced by informational advantages in surveillance systems. While some studies focused on political governance and state authority (Lyon, 2018, Feldstein, 2019), others highlight economic competition, organizational control, or interpersonal influence (Harkin et al., 2020, Chatterjee et al., 2018, Brown, 2024).

Building on these insights, this study adopted a neutral understanding of power: it was the capacity generated by spyware and surveillance systems to influence behavior, decision-making, and access to information across social, economic, organizational, and institutional domains, without assuming inherent misuse or political intent.

2.3.7 Digital Resilience and Its Limits

Digital resilience refers to the ability of individuals and communities to anticipate, withstand, and recover from digital harms. Policy discussions often stress digital literacy and awareness as key solutions. However, the evidence reviewed here suggested that relying solely on individual coping strategies is insufficient. In Uganda, for example, most people had never received formal training on digital rights or security, which limits their ability to anticipate or respond to spyware (Mirembe et al., 2022).

Technical research further demonstrates that resilience was constrained by systemic factors. Anti-spyware tools fail to detect most consumer surveillance applications, while state-grade spyware remains virtually undetectable (Chatterjee et al., 2018, Deibert, 2022). Uganda's National Cybersecurity Strategy prioritized economic security and cybercrime but largely omits spyware,

gendered surveillance, and accountability mechanisms, revealing a policy-practice gap that undermines meaningful resilience (Uganda Ministry of ICT, 2023).

In Uganda, the relational and constrained character of digital resilience is particularly pronounced. Research indicates that awareness of surveillance risks, where it exists, is unevenly distributed across occupational groups, with ICT professionals and civil society actors demonstrating considerably higher levels of risk awareness than everyday mobile device users, small business owners, and domestic workers (Mirembe et al., 2022). This uneven distribution of resilience capacity reinforces rather than disrupts existing social inequalities, underscoring the need for a mitigation framework that addresses not only individual digital awareness but also the institutional and technical conditions that enable or constrain protective action across diverse user populations.

2.3.8 Spyware-Enabled Surveillance in the Ugandan Context

Uganda's digital surveillance landscape is shaped by a distinctive convergence of historical political repression, rapid but unevenly governed digital expansion, and an active commercial spyware market factors that together create a risk environment of particular severity for mobile device users. Understanding this context is essential for grounding the global and regional literature reviewed in preceding sections within the specific socio-political and institutional conditions that frame this study.

Historical foundations and the emergence of state spyware.

The use of spyware by state actors in Uganda is not speculative but empirically established and forensically documented. Following the contested 2011 presidential elections, officials of Uganda's Chieftaincy of Military Intelligence (CMI) and the Uganda Police Force (UPF), acting on presidential orders, deployed FinFisher intrusion malware manufactured by the UK-based Gamma Group International in a covert surveillance operation codenamed Fungua Macho (Swahili: "Open Your Eyes") (Privacy International, 2015). At least 73 intelligence operatives participated in the operation, which targeted opposition leaders, journalists, and civil society actors. A leaked confidential intelligence brief prepared for Ugandan President explicitly stated that the operation's goal included the ability to "manage and control the media houses and opposition politicians which may involve blackmailing them" (Privacy International, 2015) **(Privacy-International, 2015, BBC, 2015).** The operation deployed full "Fintrusion suite"

capabilities, enabling covert remote access to communications, microphones, cameras, and passwords without the target's knowledge. This evidence situates Uganda among the earliest documented cases of state-grade commercial spyware deployment in Sub-Saharan Africa, establishing a pattern of using technical surveillance as a tool of political management that predates the global Pegasus controversies by nearly a decade.

This pattern was further corroborated by concurrent revelations. Leaked internal emails from the 2015 Hacking Team data breach revealed that Italian surveillance company Hacking Team and Israeli firm NICE Systems were simultaneously negotiating a separate, larger surveillance package for the Ugandan government, described internally as "sponsored by the topmost level of the country" (Unwanted Witness, 2025). The proposed system included Remote Control System (RCS) capabilities: zero-day exploits, email monitoring, keystroke recording, and camera and microphone access for any device in the country. In parallel, investigative reporting by BBC Newsnight confirmed that Gamma Group's FinFisher technology had been used to spy on opposition politicians, journalists, and LGBT activists, with the Ugandan government denying the operation's existence despite documentary evidence to the contrary (BBC, 2015). Together, these revelations established that Uganda's surveillance apparatus was not the work of a single agency or isolated incident, but reflected a deliberate, multi-vendor procurement strategy enabled by the absence of export controls on surveillance technology.

The electoral cycle and persistent targeting.

A defining characteristic of Uganda's surveillance landscape is its temporal correlation with electoral cycles. The 2011 Fungua Macho operation was triggered by post-election protests (Privacy International, 2015). In the 2016 and 2021 electoral periods, authorities imposed social media shutdowns, restricted access to platforms including Facebook and Twitter, and invoked the Computer Misuse Act to prosecute online critics and dissenting voices (Nassuuna and Kimbugwe, 2025). Uganda's Regulation of Interception of Communications Act 2010 (RICA) provides statutory authority for broad interception of communications for national security purposes, requiring telecommunications providers to install real-time electronic surveillance equipment and exposing them to severe penalties for non-compliance, a provision civil society organization have described as susceptible to broad interpretation and abuse (Lubowa, 2025, Madoi, 2026)

Section 5(u) of the Uganda Communications Act 2017 further empowered government to establish social media monitoring and interception centres, with documented procurement bids from technology companies based in China, Israel, Italy, Poland and the United Kingdom ahead of the 2016 elections (Madoi, 2026, Nassuuna and Kimbugwe, 2025).

The Anti-Terrorism Act 2002 further authorizes security officers to intercept communications without judicial oversight in terrorism-related investigations a provision civil society organization have described as susceptible to broad interpretation and abuse (Lubowa, 2025).

This pattern has continued into the contemporary period. In May 2025, prominent investigative journalist Canary Mugume of NBS Television received a mercenary spyware warning directly from Apple Inc. a notification typically reserved for state-level targeting and subsequently had his mobile phone physically seized in a targeted attack. Mugume explicitly noted the electoral dimension: "They last sent this report in 2021; there is a pattern electoral season" (Musoke, 2025). His case was documented in the Unwanted Witness (2025) regional report, Surveillance/Spyware: An Impediment to Civil Society, Human Rights Defenders and Journalists in East and Southern Africa, which found that Uganda's surveillance machinery had evolved into a complex system combining broad ambient monitoring with targeted spyware campaigns against journalists, human rights defenders, and opposition politicians. In April 2025, reports emerged that the Government of Uganda was procuring a new digital social media tracking tool, raising further concerns about institutionalized digital surveillance in the run-up to the 2026 general elections (Nassuuna and Kimbugwe, 2025).

The expanding infrastructure of surveillance.

Uganda's surveillance environment extends beyond mobile spyware to encompass a layered physical and digital infrastructure. Since 2013, mandatory SIM card registration under the Registration of Persons Act has linked all phone numbers to national identity documents, effectively eliminating communication anonymity (Lubowa, 2025). In 2018, a social media tax (OTT tax) was introduced, which critics characterized as a mechanism for curbing online dissent rather than broadening the tax base. In 2020, Huawei facial recognition cameras were deployed across Kampala under a "safe city" initiative but were reported to have been used to monitor protests (Ngamita, 2025). Most recently, Uganda's Intelligent Transport Monitoring System (ITMS) introduced digital number plates embedded with Radio-Frequency Identification (RFID)

chips and QR codes capable of tracking vehicle movements in real-time across the country. The system is operated by Joint Stock Company Global Security, a Russian contractor, and its command structure runs directly from the Office of the President through the Ministry of Security to the Uganda Police Force (Katusiime, 2025, Ngamita, 2025, Madoi, 2026). The ITMS intersects with Huawei's existing CCTV smart-city network to create what investigators have described as an "all-seeing infrastructure capable of tracking citizens' movements, associations, and activities with alarming precision" (Katusiime, 2025). These developments collectively represent a systematic and layered expansion of surveillance capacity across physical, digital, and telecommunications dimensions, with minimal public transparency, legislative oversight, or judicial accountability for the data collected.

The expansion of Uganda's surveillance infrastructure is not limited to urban or political contexts. Investigative reporting has documented the deployment of dual-use data-aggregation platforms in conservation governance, where wildlife tracking tools such as EarthRanger are used to monitor rangers, community members, and civil society actors in national park buffer zones, reflecting a diffusion of surveillance logic across governance domains (Oluka et al., 2026; Madoi, 2026).

Gendered and civil society dimensions.

Surveillance risks in Uganda are not uniform across population groups. Women, feminist activists, and civil society organizations face distinct and compounding vulnerabilities. Research presented at DataFest Africa 2024 documented how spyware deployed by both state and non-state actors has significantly impacted civic space by enabling surveillance of feminist activists, suppressing online campaigns against gender-based violence, and eroding trust within activist networks (Women of Uganda Network 2024). When activists suspect that their communications may be monitored, the resulting paranoia creates internal divisions and weakens collective action an effect particularly damaging in organizing environments that depend on interpersonal solidarity (Women of Uganda Network 2024). At the interpersonal level, consumer-grade surveillance tools have been documented in the context of intimate partner surveillance, coercive control, and technology-facilitated gender-based violence in Uganda, with practices including WhatsApp Web session hijacking, remote location tracking, and unauthorized account access (Brown, 2024, Chisala-Tempelhoff and Kirya, 2024). These dimensions of surveillance risk interpersonal, gendered, and

activist-targeted remain systematically under-researched in Uganda's existing literature, which has tended to focus on political and state surveillance of high-profile targets.

The regulatory and enforcement gap.

Uganda has developed formal legal instruments for privacy and data protection: Article 27 of the 1995 Constitution protects the right to privacy; the Data Protection and Privacy Act 2019 establishes data subject rights and processing obligations; and the Computer Misuse Act 2011 criminalizes unauthorized access. However, the gap between legal provision and practical protection is substantial. Mirembe et al. found significant gaps in awareness of digital privacy rights among Ugandan mobile device users, with many unaware that smartphones could be monitored remotely without visible signs (Mirembe et al., 2022). The Personal Data Protection Office established under the DPPA 2019 remains chronically understaffed and under-resourced, limiting its capacity to investigate or sanction violations. The Citizen Lab and Privacy International investigations referenced above were conducted precisely because Ugandan regulatory bodies lacked the forensic capacity or political independence to investigate state-sponsored surveillance. As noted, Uganda is legal framework "permits boundless surveillance of the communications of citizens," with statutory instruments providing broad interception powers while offering limited mechanisms for users to seek redress or verify whether their devices have been compromised.

Taken together, the Ugandan surveillance landscape is characterized by five interconnected features: a documented history of state-grade spyware deployment stretching from 2011 to the present; an electoral cycle that consistently correlates with intensified surveillance and platform suppression; a systematically expanding physical and digital surveillance infrastructure involving foreign contractors and technologies with minimal accountability; gendered and civil society dimensions that disproportionately affect women, activists, and human rights defenders; and a regulatory framework whose formal provisions are consistently outpaced by surveillance capabilities and undermined by weak enforcement. These features justify the present study's integrated, socio-technical approach, which treats Uganda's surveillance risk environment as produced not by technology alone, but by the interaction of technical systems, institutional choices, governance failures, and social power relations and which positions the development of a multi-layered mitigation framework as both empirically necessary and practically urgent.

2.4 Synthesis and Research Gaps

The reviewed literature demonstrated broad convergence on the technical capabilities and risks associated with spyware and digital surveillance. Studies focused on technical and security aspects, mostly conducted in Western and Global North contexts, provide detailed analyses of spyware architectures, attack methods, and the challenges of detection. These studies show that modern spyware is widespread, often operates covertly, and is difficult to detect with standard security tools (Chatterjee et al., 2018, Deibert, 2022). These studies offer strong evidence of how surveillance technologies operate, but they tend to prioritize system-level analysis over social context and lived experience.

Across Information Systems, surveillance studies, and human rights literature, there is consistent evidence that both actual and perceived surveillance erode user trust, encourage self-censorship, and reshape digital behavior (Lyon, 2018, Eisend, 2019, OHCHR, 2022). However, much of this evidence was derived from Western democracies or global comparative literature, limiting its contextual relevance for low and middle-income countries where digital infrastructures, governance arrangements, and social norms differ significantly.

In contrast, literature that spoke directly to Uganda and the broader East and Southern African region is dominated by investigative reports, policy analyses, and civil society documentation rather than peer-reviewed academic research. These sources provided critical empirical insights into state surveillance practices, procurement of monitoring technologies, and impacts on journalists and civil society actors (Roberts and Mare, 2025, Unwanted Witness, 2025).

While methodologically rigorous in their own terms, such reports are often sector-specific and rarely integrate technical, social, and gendered dimensions into a unified analytical framework.

Gender emerges as a recognized but underdeveloped theme in the literature. Feminist and socio-legal studies document the prevalence of technology-facilitated gender-based violence and highlight how digital monitoring is used to exert coercive control, especially against women (Chisala-Tempelhoff and Kirya, 2024, Brown, 2024). Nevertheless, there remained lack of empirically grounded, comparative research that systematically examines how men and women experience spyware and digital surveillance differently, or how gender shapes perceptions of risk, trust, and coping strategies beyond specific categories of harm.

Overall, the literature points to a gap in integrated, socio-technical, and context-sensitive research that brings together technical characteristics of spyware, gendered social dynamics, institutional arrangements, and user-level responses. In the Ugandan context in particular, existing research had tended to prioritize specific sectors such as journalism, civil society, or policy advocacy, while offering limited empirical insight into how spyware and digital surveillance are experienced across diverse user groups, including professionals, technocrats, and everyday mobile device users. There remained a lack of empirical studies that examine how these different actors interpret, navigate, and respond to surveillance within their everyday social and professional lives. This study addressed this gap by adopting a gender-responsive socio-technical approach that captures experiences across multiple user categories, with particular attention to privacy, trust, power, and digital resilience.

While recent scholarship has advanced methods for detecting spyware through machine learning techniques (Qabalin et al., 2022), and has begun documenting the transnational dimensions of the surveillance industry, integrated research that synthesizes these forensic realities into a localized, socio-technical mitigation framework for the Ugandan context remains absent

This study addresses that gap directly.

CHAPTER THREE: METHODOLOGY

3.0 Introduction

This chapter presented the methodology adopted for the study. It explained the philosophical orientation, research approach, methodological choice, research design, study population, sampling procedures, data collection methods, data analysis techniques, ethical considerations, and limitations of the study. The methodological decisions were guided by the study objectives and by the need to examine spyware-enabled digital surveillance as a socio-technical phenomenon that combines technical mechanisms, user practices, and governance conditions within Uganda's digital ecosystem.

3.1 Research Design

Research design according to (Khanday and Khanam, 2019), is a procedural plan that is adopted by a researcher to answer questions in a valid way. The research design is also known to define the type of analysis to be applied for the desired result to be obtained. It focuses on answering research questions in a reasonable way. defines research design as an outline, plan, or strategy that specifies the procedure to be used in seeking answers to research questions. It involves specifying things such as how the data will be collected and analyzed, what type of research will work for answering the research questions, while ensuring coherence and logical ways, between data collection and analysis (Leavy, 2022, Dannels, 2018).

This study adopted the Saunders et al. (2019) Research Onion as a guiding framework for structuring the research design (Saunders et al., 2019). The Saunders Research Onion is a layered approach that illustrates the different stages involved in the development of a research methodology (Saunders et al., 2019). While using the research onion, one must go from the outer most layers that is; Research Philosophy, Research Approaches, Research Strategies, time horizons and lastly to the inner most layer which is Data Collection Methods.

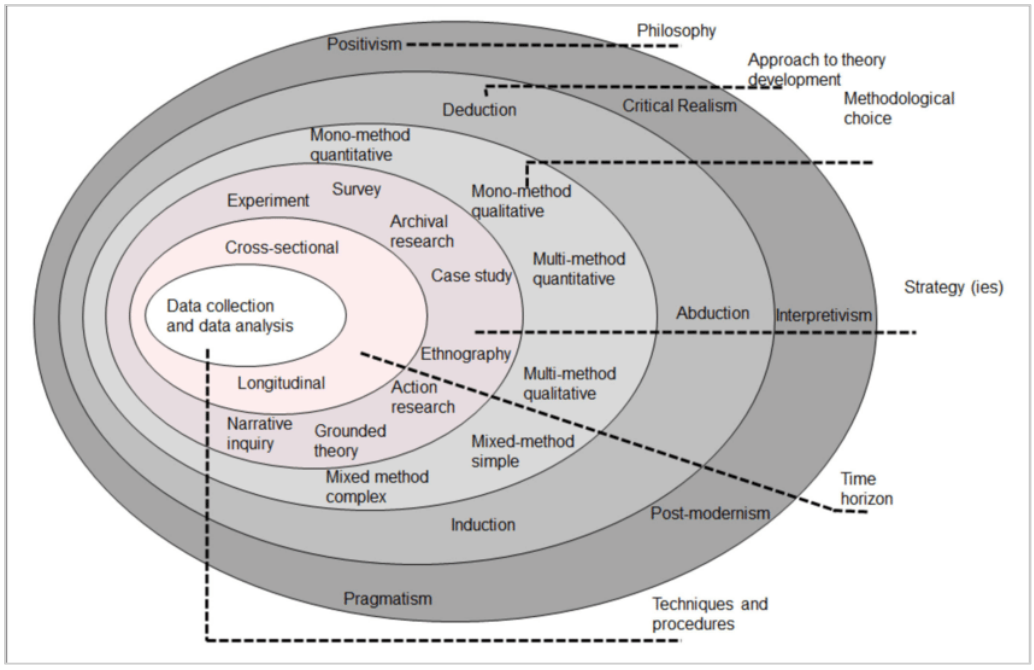

Figure 2: Research onion (Saunders et al., 2019)

Given the exploratory nature of spyware-enabled digital surveillance and the limited empirical evidence available in Uganda, the study was designed to prioritize depth of understanding rather than statistical generalization.

3.2 Research philosophy

Research philosophy concerned assumptions about the nature of reality and how knowledge about that reality can be generated (Saunders et al., 2019). This study was guided by an **interpretivist research philosophy**, which holds that social reality was socially constructed and that meaning emerges through human experience and interaction (Ryan, 2018, Schwandt, 1994, Orlikowski and Baroudi, 1991).

Interpretivism was appropriate for this study because spyware-enabled digital surveillance was not experienced uniformly or objectively. Its effects on privacy, trust, power, and digital resilience are shaped by how individuals perceive surveillance, interpret risk, and navigate everyday digital practices. An interpretivist stance allowed the study to explore these subjective meanings and contextual experiences rather than treating surveillance solely as a technical or measurable phenomenon (Ryan, 2018).

3.3 Research Approach

A research approach explained how theory and empirical data are related within a study (Woiceshyn and Daellenbach, 2018). This study adopted an inductive research approach, which involves developing insights and conceptual understanding from empirical data rather than testing predefined hypotheses.

The inductive approach was suitable because the study does not seek to validate an existing spyware-specific framework. Instead, it allowed patterns and themes to emerge from participants' experiences, survey responses, and documentary evidence. These insights were then synthesized to inform the development of a framework for addressing spyware-enabled digital surveillance risks (Azungah, 2018).

3.4 Research Method

According to Sheppard (2024), research methods refer to a systematic process of inquiry used to understand and examine aspects of the social world. This implies that research should follow a series of interconnected steps that work together to produce meaningful and reliable findings. Research methods can therefore be understood as the strategies, procedures, and techniques used to collect and analyze data in order to generate new knowledge or develop a deeper understanding of a particular issue. In many cases, the term research methodology is used to describe the broader scientific approach that guides the collection, analysis, and interpretation of either quantitative or qualitative data in response to research questions. Research methods are important because they help guide the study and keep the investigation focused on the most relevant aspects of the research problem (Sheppard, 2024).

In line with (Saunders et al., 2019), this study adopted a mixed-method (simple) methodological choice, combining qualitative interviews with a descriptive survey and document review, with integration occurring at the interpretation stage. This combination within a single study to provide a more comprehensive understanding of the research problem (Plonsky, 2017, Myers and Avison, 2002, Ghanad, 2023).

The mixed-methods approach were appropriate because spyware-enabled digital surveillance was both a technical and social phenomenon. Qualitative data were used to capture in-depth insights into users' experiences, perceptions, and responses to surveillance, while quantitative data provide

numerical indicators that help illustrate patterns of awareness, perceived risk, trust, and behavioral change.

The quantitative component of the study adopted a descriptive survey design. According to (Ghanad, 2023), descriptive survey research is useful in describing characteristics, attitudes, behaviours, and opinions within a target population through the collection of numerical data. Quantitative methods also enable the use of statistical analysis to identify patterns, relationships, and trends within the collected data. In this study, quantitative data provided measurable indicators related to levels of awareness, perceptions of surveillance risk, trust in digital systems, confidence in identifying spyware threats, and behavioural responses among users. The use of surveys also made it possible to gather data from a relatively larger group of participants, thereby improving the generalizability and reliability of findings.

The qualitative component of the study was used to obtain in-depth insights into participants' experiences, perceptions, and concerns regarding digital surveillance and spyware-related risks. Through interviews, respondents were able to explain how surveillance practices affect their sense of privacy, trust in digital platforms, and online behaviour. Qualitative methods were particularly important because they allow researchers to understand meanings, interpretations, and lived experiences associated with a phenomenon.

The study further incorporated document review and technical analysis to strengthen the interpretation of findings and provide institutional and technological context to the research problem. Documentary sources included policy documents, legal frameworks, organizational reports, technical papers, and peer-reviewed studies related to spyware, surveillance technologies, cybersecurity, and digital rights. These sources were important in contextualizing the findings within broader debates on digital surveillance, governance, and cybersecurity practices in Uganda and beyond.

Technical and documentary evidence also supported the understanding of spyware detection and analysis techniques. Previous studies such as (Qabalin et al., 2022) classify spyware detection approaches according to analysis techniques such as dynamic and static analysis, detection logic including signature-based, anomaly-based, and hybrid approaches, and deployment modes such as host-based, network-based, and hybrid-based detection systems. These studies further categorize spyware activities into baseline, installation-related, and operational phases. Integrating such

technical literature into the study helped bridge the gap between users' experiences and the underlying technological mechanisms that enable spyware surveillance.

This approach aligns with recommendations in Information Systems research that complex digital risks should not be examined using a single method, but instead require the integration of multiple forms of evidence (Sittig and Singh, 2016, Stefani et al., 2025).

3.5 Research Strategy

The study employed a combination of semi-structured interviews, a descriptive survey, and document review as its main research strategies. Semi-structured interviews enable flexible, in-depth exploration of participants lived experiences and interpretations of spyware-enabled surveillance (Oltmann, 2016). A descriptive survey complemented interview data by capturing numerical patterns related to awareness, perceived risks, trust in digital systems, and coping practices. Document review provided contextual and technical grounding by examining relevant policies, regulatory reports, cybersecurity assessments, and academic literature including technical spyware detection research used to stabilize shared vocabulary for discussing mitigation options without turning the thesis into a network-traffic classification study (Qabalin et al., 2022). These strategies support triangulation and enhance the credibility of the findings.

3.6 Study Population

The study population consists of 320 mobile device users and 10 key informants who are likely to have relevant experience or knowledge related to spyware-enabled digital surveillance in Uganda. These included journalists, civil society actors, digital rights advocates, ICT professionals, and everyday mobile phone users. These groups were selected because they interact with digital technologies in different ways and were exposed to varying surveillance risks within Uganda's digital environment.

3.7 Sampling Techniques and Sample Size

The study employed a mixed-methods sample composition reflecting the qualitative and quantitative components of the research. For the qualitative component, a smaller group of 10 participants was selected for in-depth interviews, with the final number guided by thematic saturation rather than a predetermined sample size (Guest et al., 2012). This approach ensured rich, context-specific insights into users' experiences of spyware-enabled digital surveillance.

For the quantitative component, a larger group of 320 respondents was included through a descriptive survey in order to capture indicative patterns related to awareness, perceived risk, trust, and coping practices across different user groups and was determined using Krejcie and Morgan Table. The survey sample was intended to provide breadth and contextual support for qualitative findings rather than statistical generalization or hypothesis testing.

3.8 Data Collection Methods, Instruments and Triangulation

3.8.1 Data Collection Methods and Tools

Semi-structured interviews were the primary qualitative data collection method. Two interview guides were used: one focusing on the participants lived experiences of spyware-enabled digital surveillance, and another focusing on perceptions, awareness, and professional or observational insights for participants without direct personal experience. The interview guides contained open-ended questions designed to explore experiences of surveillance, perceptions of privacy and trust, perceived influence and control, awareness of risks, and responses to suspected surveillance.

Interviews allowed flexibility, probing, and clarification, enabling participants to express their experiences and perspectives in their own words. With participants' consent, interviews was recorded using a digital recording device to ensure accurate capture of responses.

A short, structured survey was used to collect quantitative data. The survey consisted of closed-ended and Likert-scale questions focusing on awareness of spyware risks, perceived privacy threats, trust in digital platforms and institutions, perceived influence of surveillance, and changes in digital behaviors.

The survey was administered using both printed questionnaires and an online version created using Google Forms. This dual approach was intended to increase accessibility and participation among different groups of mobile device users. The survey was designed to generate descriptive statistics that complement and contextualize the qualitative interview findings.

Document review was used to analyze secondary data from regulatory bodies, policy documents, cybersecurity reports, digital rights publications, and relevant academic literature. This method supported triangulation and helped situate individual user experiences within broader socio-technical, institutional, and governance contexts related to spyware-enabled digital surveillance.

3.8.2 Conceptual technical vocabulary

To enable consistent and precise engagement with technical documentation during document review, this subsection establishes the analytical vocabulary used to describe spyware detection approaches throughout the study. These terms are adopted from the technical literature as neutral descriptors rather than as theoretical claims, and their use is limited to the methodological contexts described below.

Technical security literature commonly summarizes spyware detection models using three dimensions: analysis technique (dynamic vs. static), detection approach (anomaly-based, signature-based, or hybrid), and deployment approach (host-based, network-based, or hybrid-based)

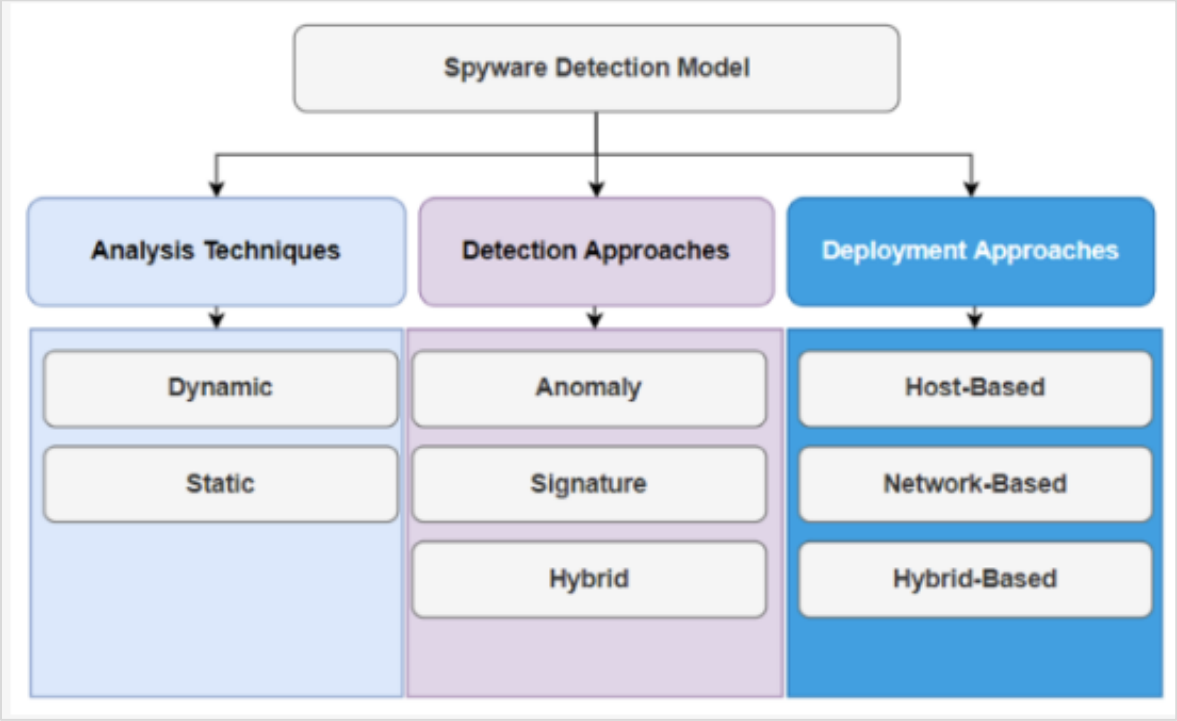

Figure 3: Spyware detection approaches (Qabalin et al., 2022)

Separately, benchmark work on commercial Android spyware has used a three-phase lifecycle distinction between benign baseline activity, installation-phase activity, and operational-phase activity when spyware functions are exercised more fully (Qabalin et al., 2022).

In this study, these constructs are used only as neutral analytical language when (a) summarizing technical documents in document review, (b) structuring discussion in findings and interpretation

where participants refer to timing or sequence (for example, “after installing an app,” “after someone had access,” “ongoing strange behaviour”), and (c) articulating mitigation implications in the proposed framework (for example, differences between controls relevant before full compromise vs. after suspected compromise). The study does not collect PCAP network traces, does not label participants’ devices using traffic classes, and does not train or validate machine-learning classifiers on external spyware traffic datasets.

3.8.3 Empirical Research Artefact: Uganda Surveillance Watch

To support data triangulation, the researcher developed a web-based dashboard (Uganda Surveillance Watch). This tool was designed to aggregate fragmented data from global sources (SurveillanceWatch.io, MITRE ATT&CK®, and Wikipedia) and overlay them with the primary findings of this study. The dashboard served as a “live” representation of the socio-technical ecosystem, allowing the researcher to visualize the intersection of technical vendor data with the reported experiences of Ugandan users.

3.9 Data Analysis

Data analysis in this study followed a mixed-methods approach, combining qualitative, quantitative, and documentary data to support the design of the proposed framework.

Qualitative data from semi-structured interviews and open-ended survey responses were analysed using thematic analysis. Interview recordings were first transcribed, after which the researcher became familiar with the data by repeatedly reading the transcripts and responses. Initial coding was carried out manually by assigning short labels to meaningful sections of data related to spyware experiences, privacy concerns, trust, power and control, and coping or protective practices. Microsoft Word was used for transcription and annotation, while Microsoft Excel will support the organisation of codes and emerging themes in tabular form. Where appropriate, qualitative data analysis software such as NVivo was used to assist with systematic comparison of codes and themes across data sources. Related codes was then grouped into broader themes, such as loss of privacy, erosion of trust, or adaptive user behaviours. Themes were reviewed and refined by comparing patterns across participants and data sources to ensure consistency and relevance.

Quantitative survey data was analysed using descriptive statistics and inferential statistics such as chi-square and correlational analysis, including frequencies and percentages, to identify patterns

related to user awareness of spyware, perceived risks, levels of trust in digital systems, and behavioural responses to surveillance using SPSS Version 27.0. Microsoft Excel was used to organise and analyse the survey data.

Documentary data, including policy reports, technical documents, and regulatory materials, was analysed using content analysis. Relevant documents was reviewed and manually coded using thematic tables to identify key policy positions, institutional roles, protective measures, and gaps related to spyware-enabled digital surveillance.

Findings from the qualitative, quantitative, and documentary analyses was integrated during interpretation. This combined analysis informed the design of a framework aimed at mitigating spyware-enabled digital surveillance risks associated with mobile device use in Uganda.

3. 10 Data Quality and Trustworthiness

The quality and trustworthiness of this study are ensured through several complementary strategies that support credible and well-grounded findings.

Triangulation was used by combining multiple sources of data, including qualitative interviews, survey responses, and document review. Comparing findings across these sources allows key patterns and insights to be confirmed, reducing reliance on any single method.

Consistency of themes was assessed during analysis by examining whether similar ideas and experiences emerge across different participants and data sources. Themes were refined through repeated comparison to ensure they accurately reflect participants' accounts of spyware-enabled digital surveillance

Expert review was used as a validation strategy for the study's findings and the developed framework. After the framework is designed, it was shared with knowledgeable practitioners and academics, such as ICT and cybersecurity experts, digital rights practitioners, and academic supervisors. Their feedback was used to assess the clarity, relevance, and practical usefulness of the framework and to inform further refinement.

Thick description was employed to provide rich and contextualized accounts of participants' experiences, supporting meaningful interpretation of the findings. The researcher also engaged in

reflexive practice by continuously reflecting on personal assumptions and positionality throughout data collection and analysis.

Audit trail was maintained through systematic documentation of key methodological decisions and analytical steps. This enhanced transparency and supports the dependability of the research process.

3.11 Ethical Considerations

Ethical approval was sought from relevant institutional authorities prior to data collection. Participants are informed about the purpose of the study, the voluntary nature of participation, and their right to withdraw at any time. Informed consent was obtained from all participants.

Given the sensitivity of spyware-enabled surveillance, particular care was taken to protect participants' confidentiality and anonymity. No personally identifiable information was recorded, and all data are stored securely and used solely for academic purposes.

3.12 Challenges or Limitations of the Study

The study was exploratory and context-specific, and its findings were not intended to be statistically generalizable to the entire Ugandan population. The sensitive nature of digital surveillance also limited participants' willingness to disclose certain experiences. These limitations were mitigated through triangulation of data sources, careful ethical practices, and transparent reporting of findings.

Additionally, the study does not empirically validate spyware using network packet capture, host-based malware reversing, or machine-learning classification of traffic datasets (Qabalin et al., 2022). Technical vocabulary drawn from that literature is therefore used for conceptual clarity and structured interpretation, not as evidence of confirmed compromise in specific devices.

3.13 Time Horizon and Study Timeline

This study adopted a cross-sectional time horizon, with data collected at a single point in time rather than across multiple phases or periods (Saunders et al., 2019). This approach was appropriate for the exploratory nature of the research, which sought to understand current experiences, perceptions, and practices related to spyware-enabled digital surveillance within Uganda's digital environment.

The study was conducted over a six-month period, during which all key activities, including literature review, ethical approval, participant recruitment, data collection, data analysis, and report writing was carried out systematically. This timeframe allowed sufficient opportunity for in-depth qualitative engagement, descriptive survey analysis, and integration of findings to inform the development of the proposed framework.

Conclusion

This research report presented a study that examined spyware-enabled digital surveillance risks associated with mobile device use in Uganda through a socio-technical perspective. Focusing on adult mobile device users across diverse professional, social, and civic contexts including journalists, civil society actors, professionals, technocrats, and everyday users. The study sought to capture how surveillance was experienced within Uganda's rapidly expanding digital ecosystem. By engaging participants with varied forms of mobile technology use, the research aims to develop a grounded understanding of how spyware-enabled surveillance affects privacy, trust, power relations, and digital resilience in everyday life.

The literature review highlighted important gaps in existing scholarship. While prior studies had documented the technical capabilities of spyware and broader digital surveillance infrastructures, much of this work remains fragmented across technical, policy, and ethical domains, with limited attention to how these risks are experienced by users in Global South contexts. In particular, there was a lack of context-specific frameworks that integrate technical vulnerabilities, user practices, and governance considerations to guide effective mitigation of spyware-enabled digital surveillance risks. This study responded to this gap by bringing these perspectives together within a unified socio-technical framework tailored to the Ugandan context.

Methodologically, the study adopted a mixed-methods, interpretivist approach that was well suited to exploring the complex and lived dimensions of digital surveillance. Through qualitative interviews, a descriptive survey, and continuous document review, the research generated rich, contextualized insights into user experiences while also capturing broader patterns of awareness, risk perception, and response. Attention to trustworthiness, ethical integrity, and methodological rigor guided the research process, ensuring that findings were credible, transparent, and responsibly produced.

Overall, the study was expected to contribute to academic debates on spyware and digital surveillance within the field of Information Systems by offering an empirically grounded socio-technical perspective. At a practical level, the findings were intended to inform policymakers, digital rights advocates, civil society actors, and technology users by supporting the development of more context-appropriate approaches to privacy protection, digital governance, and digital resilience in Uganda.

CHAPTER FOUR: DATA ANALYSIS, PRESENTATION, AND INTERPRETATION

4.1 Introduction

This chapter presents the study findings on spyware-enabled digital surveillance in Uganda's mobile digital ecosystem, based on a mixed-methods design involving 320 survey respondents, key informant interviews, and document review. The chapter addresses the study objectives by examining surveillance practices and actors, effects on privacy, trust, power, and control, and the ways user practices, institutional arrangements, and policy environments shape exposure and response.

Quantitative data from the structured survey were analyzed using descriptive and inferential statistics, including frequencies, percentages, cross-tabulations, chi-square tests, the Kruskal-Wallis H test, and correlation analysis. For multiple-response questions (Q5, Q10, Q14, and Q19), disaggregated response analysis was applied to capture the full pattern of participant selections. Qualitative interview data were analyzed using thematic analysis to identify recurrent meanings, experiences, and response patterns related to spyware risks.

Documentary sources, including policy, legal, regulatory, and technical materials, were analyzed using content analysis to identify institutional roles, governance measures, implementation gaps, and enforcement constraints.

Findings from these three evidence streams were integrated during interpretation to produce a contextually grounded understanding of spyware risks in Uganda. This integrated analysis informed the design and validation of the proposed socio-technical mitigation framework, which is presented later in the chapter and discussed further in Chapter Five.

4.2 Quantitative (Survey) Findings

4.2.1 Demographic and Background Characteristics of Respondents

Understanding the demographic composition of the study sample was essential for contextualizing all subsequent findings. The survey collected data on age, gender, occupational category, and device usage frequency, which together provided a socio-technical profile of mobile device users in Uganda.

Age and Gender Distribution

Figure 4 and Figure 5 below presents the age and gender distribution of the 320 respondents who participated in the study.

Table 1: Demographic Profile of Respondents (N=320)

Age group					
		Count	Percent	Valid Percent	Cumulative Percent
Valid	18–24	78	24.4	24.4	24.4
	25–34	152	47.5	47.5	71.9
	35–44	72	22.5	22.5	94.4
	45–54	12	3.8	3.8	98.1
	55 and above	6	1.9	1.9	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

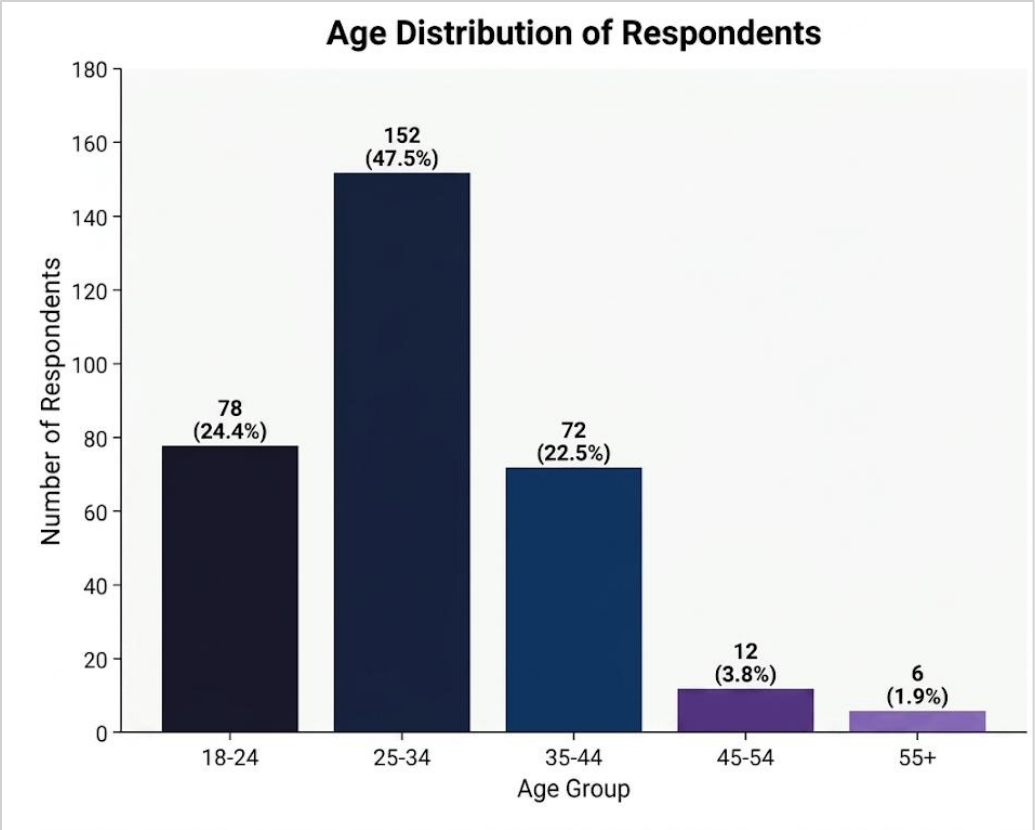

Figure 4: Age Distribution of Respondents

According to the age distribution, the majority of respondents (152, or 47.5%) were in the 25-34 age range, followed by those in the 18-24 age range (78, or 24.4%). 22.5% (72) of respondents were between the ages of 35 and 44, 3.8% (12) were between the ages of 45 and 54, and 1.9% (6) were beyond the age of 55. In Uganda, where internet penetration is still highest among young people, the comparatively low participation of older age groups (45 and above) was consistent with overall trends of digital adoption.

Table 2: Gender of Respondents

Gender of respondents					
		Count	Percent	Valid Percent	Cumulative Percent
Valid	Female	106	33.1	33.1	33.1
	Male	214	66.9	66.9	100.0

	Total	320	100.0	100.0	

Source: Primary Data, 2026

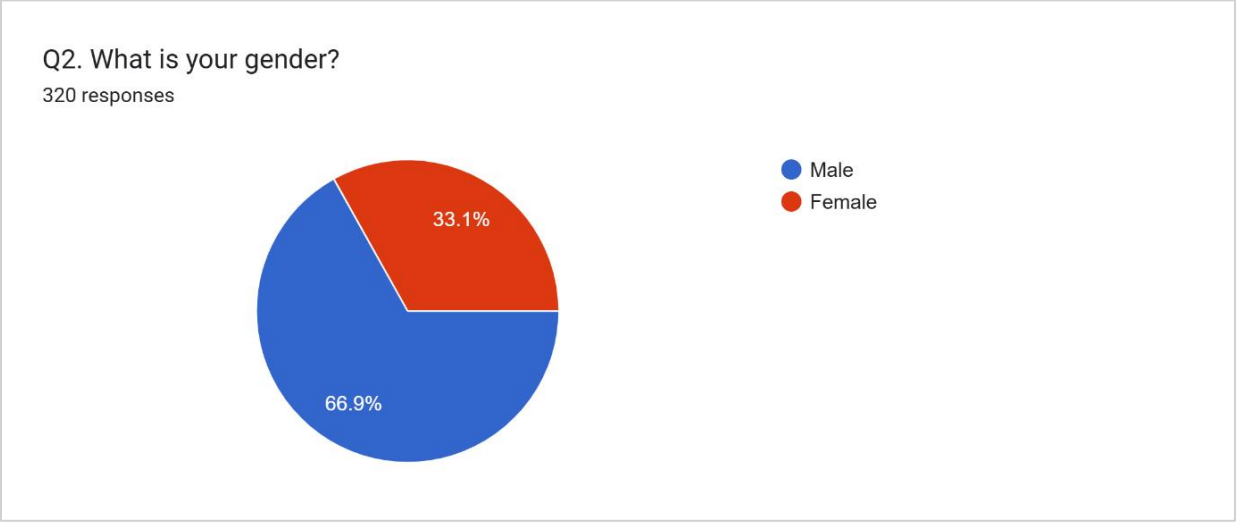

Figure 5: Gender of respondents

Regarding gender, 106 respondents (33.1%) identified as female and 214 respondents (66.9%) as male. A binary presentation in the questionnaire or a reflection of sociocultural norms in the Ugandan context are suggested by the fact that no respondents identified as non-binary or chose not to disclose. Although it also reflected documented patterns of mobile internet uptake in Uganda, where male users tend to outnumber female users, especially among ICT-engaged occupational groups, the gender imbalance was recognized as a potential limitation in the interpretation of gendered differences in surveillance experiences.

Occupational Distribution

Figure 6 illustrates the occupational background of respondents, which was important for understanding the digital exposure levels and security postures likely to characterize different user groups.

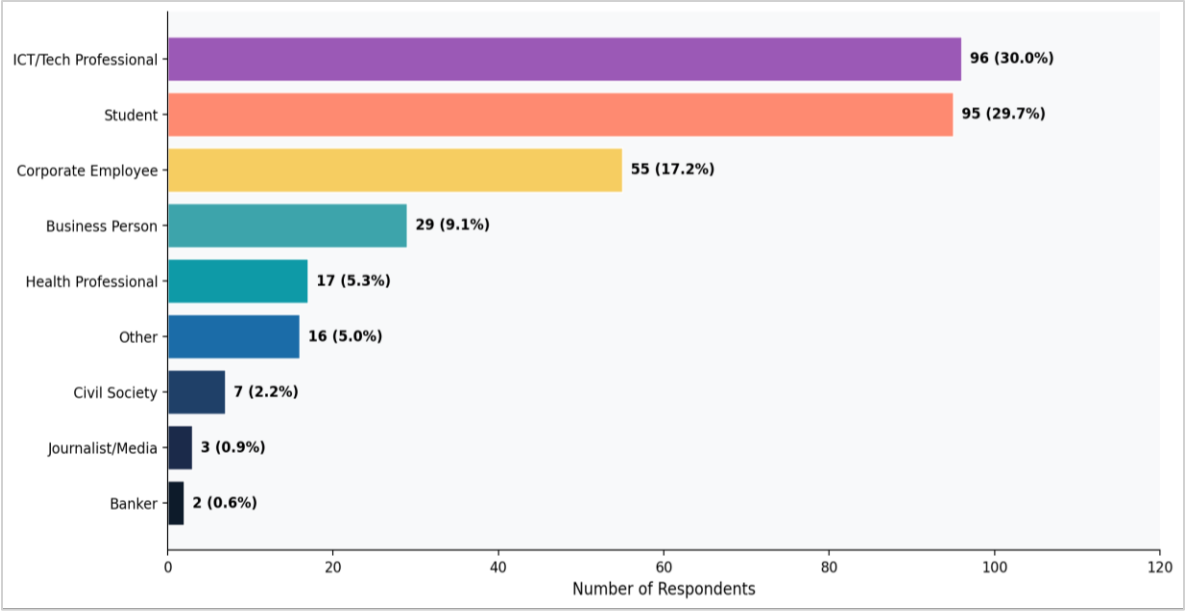

Figure 6: Occupational Distribution of Respondents (N=320)

At 30.0% (96 respondents), ICT and technology workers made up the largest occupational group. Students came in second at 29.7% (95 respondents). 17.2% (55) were corporate employees, 5.9% (19) were business owners and entrepreneurs, and 5.3% (17) were health professionals. The remaining respondents came from a range of industries, including banking, social work, media, civic society, and engineering. Each category had less than five respondents. For analytical purposes, these categories were grouped together under "Other". The purposeful and snowball sampling technique used, which targeted people with meaningful contact with mobile digital technologies, was consistent with the comparatively high representation of ICT professionals and students. Additionally, this professional profile indicated that most respondents were digitally literate, which had significant ramifications for how self-reported surveillance was interpreted.

4.2.3 Device Usage Frequency and Prior Spyware Awareness

Table 3 and Figure 7 presents data on how frequently respondents used their mobile devices for internet access and whether, prior to the survey, they were already aware that mobile devices could be used for surveillance.

Table 3: Device Usage Frequency and Prior Spyware Awareness

How often do you use your mobile devices (phone / tablet / Laptop) to access the internet?

		Count	Percent	Valid Percent	Cumulative Percent
Valid	A few times per week	2	0.6	0.6	0.6
	Daily	131	40.9	40.9	41.6
	Rarely	1	0.3	0.3	41.9
	Several times daily	186	58.1	58.1	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

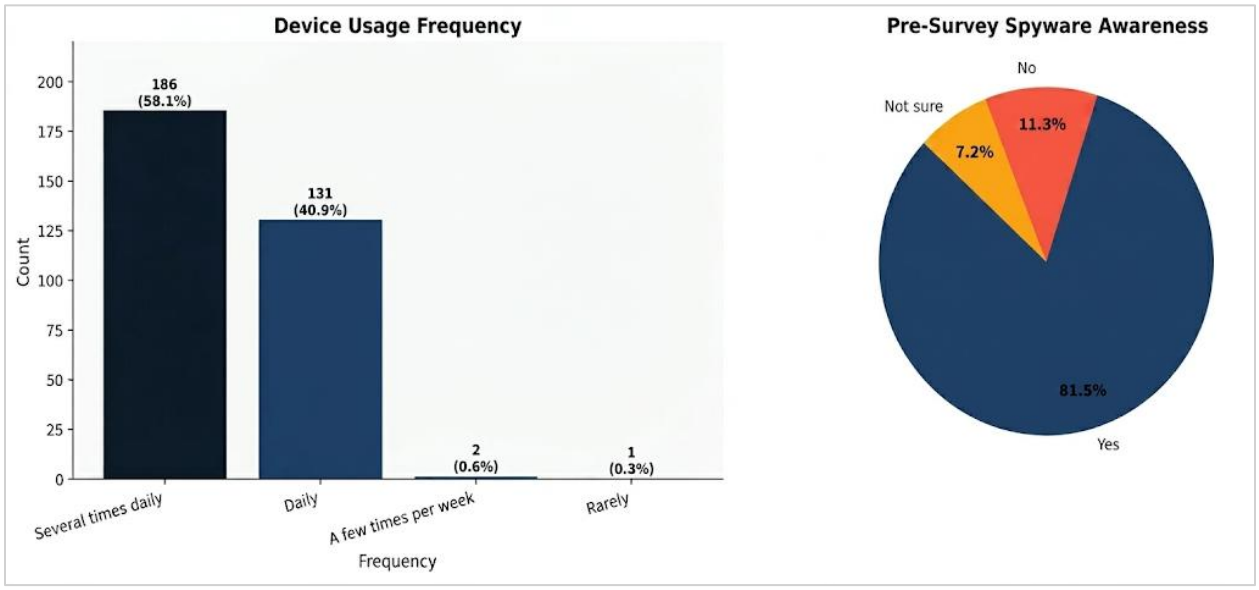

Figure 7: Device Use Frequency and Prior Spyware Awareness

The vast majority of respondents (186, or 58.1%) said they used their mobile devices to access the internet multiple times a day, and 131 (40.9%) said they did so every day. One respondent (0.3%) said they used their devices infrequently, while just two respondents (0.6%) said they used them a few times a week. This almost universal pattern of heavy daily mobile device use highlighted the increased significance of spyware risks in daily life and was consistent with Uganda's rapidly growing mobile broadband penetration, which reached roughly 39.2% of the population in 2024 (Uganda Communications Commission 2024).

Regarding awareness, 260 respondents (81.3%) said they were already aware that phones and other mobile devices may be used as surveillance tools. 36 respondents (11.3%) said they had no prior knowledge, while another 23 respondents (7.2%) were doubtful. Although the comparatively high percentage of ICT workers and students in the sample may have exaggerated this number in comparison to the larger Ugandan population, these results indicated a generally raised baseline knowledge of surveillance risk among the study group. The necessity for widespread public sensitization, especially among non-technical user groups, was nevertheless brought to light by the existence of a non-trivial knowledge gap (about 18.5% not completely aware).

4.2.4 Spyware and Surveillance Practices and Actors

The study examined the nature and prevalence of spyware-enabled digital surveillance practices within Uganda's mobile digital ecosystem, with specific attention to the actors involved, the types of surveillance suspected or experienced, and the technical indicators that users associated with such surveillance.

Prevalence of Surveillance Suspicion

Figure 8 presents respondents' self-reported experiences of suspected unauthorized monitoring, together with the indicators that led to such suspicions.

Table 4: Prevalence of Surveillance Suspicion

Have you ever suspected that your phone or laptop was monitored without your consent?					
		Count	Percent	Valid Percent	Cumulative Percent
Valid	No	91	28.4	28.4	28.4
	Not sure	40	12.5	12.5	40.9
	Yes	189	59.1	59.1	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

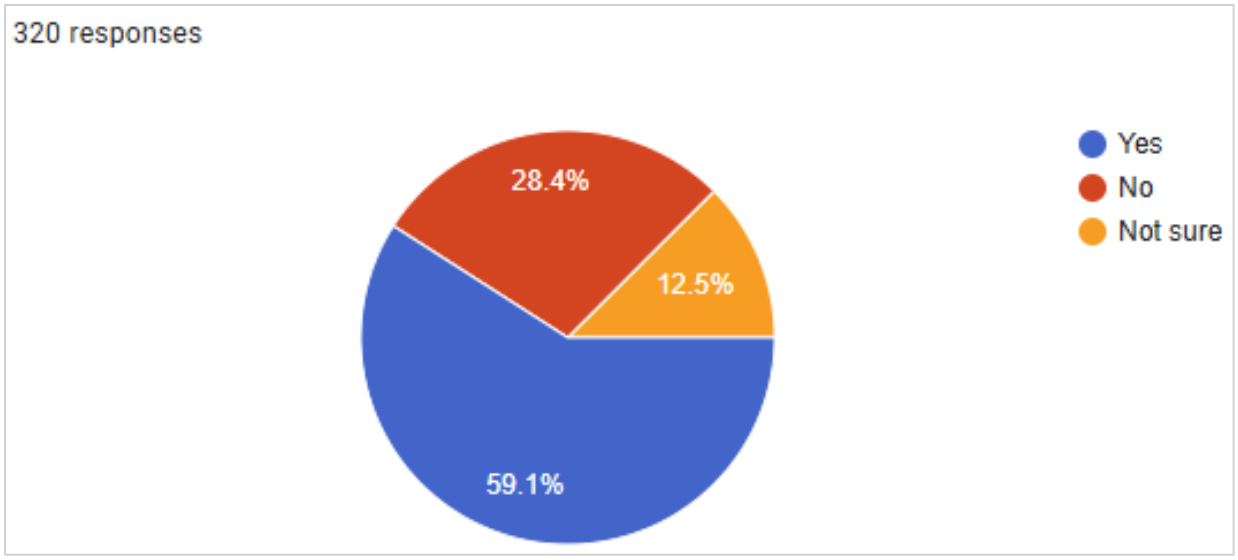

Figure 8: Surveillance Suspicion Prevalence and Indicators

A startling 59.1% of respondents (189) said they had at some point suspected that their laptop or phone was being watched without their permission. Just 28.4% (91) said they had never had such doubts, while another 12.5% (40) were doubtful. The percentage of respondents who had experienced some level of surveillance-related concern reached 71.6% when the "Yes" and "Not sure" replies were combined. This statistic highlighted how widespread surveillance anxiety is in Uganda's mobile digital ecosystem. This result was in line with more extensive regional data from Access Now's (2023) Digital Rights in Sub-Saharan Africa research, which revealed significant worries about monitoring among East African mobile device users in the wake of high-profile revelations of state actors' use of spyware.

Table 5: Surveillance suspected or experienced

If yes or unsure, what made you suspicious?					
		Count	Percent	Valid Percent	Cumulative Percent
Valid		49	15.3	15.3	15.3
	Information from media or other people	75	23.4	23.4	38.8
	Not sure	44	13.8	13.8	52.5

	Unauthorized access to messages, calls or accounts	57	17.8	17.8	70.3
	Unusual device behaviour	95	29.7	29.7	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

Indicators of Suspected surveillance

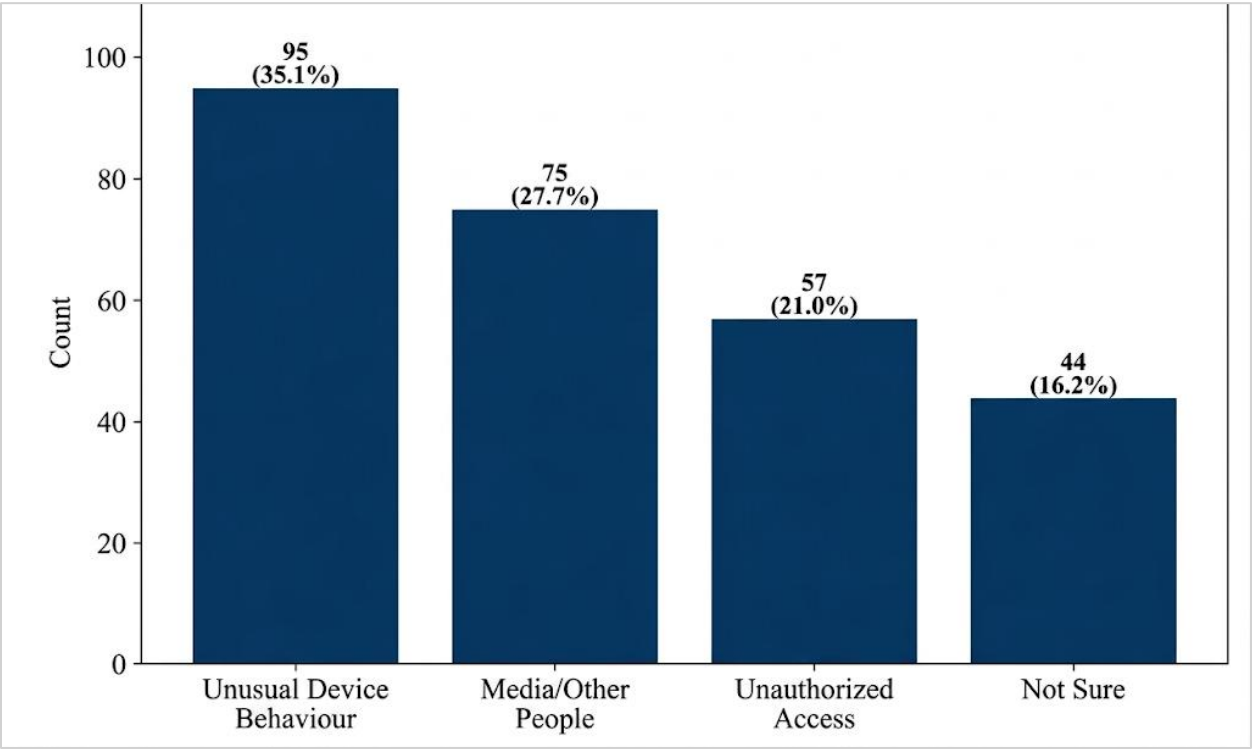

Figure 9: Surveillance suspected or experienced

The most common indicator of suspicion or doubt among people was device behavior that seems odd. 95 responses (or 35.4%) indicated strange behaviors on devices, such as battery drain, heat build-up, vacuuming of data, or activity in the background they could not explain. The second most commonly reported method for determining if someone was surveilling them was through media reports and conversations with other people (75 responses, or 27.9%), which says much about the impact media sources and social networks have on increasing a person's awareness of surveillance in Uganda. The third most commonly reported reason to believe that their account

was compromised was because someone had accessed their messages, phone calls or accounts without authorization (57 responses, or 21.2%). This indicates that a fair number of users have experienced clear evidence of lack of security with their accounts and this likely indicates that they are victims of credential-stealing spyware or SIM swap attacks. A further 44 respondents (16.4%) reported being unsure of what prompted their suspicions, pointing to the opacity and difficulty of detecting sophisticated spyware without technical tools.

4.2.5 Device Use Purposes and Exposure Pathways

Question 5 was a multiple-response item asking respondents to select all primary purposes for which they used their mobile devices. Given the multiple-response nature of this question, the frequencies exceeded the total sample size of 320. The disaggregated results are presented in Table 6 below.

Table 6: Primary Purposes of Mobile Device Use (Multiple Response, N=320)

Device Use Purpose	Frequency (n)	Percentage of Respondents (%)
Calls and Messaging	295	92.2
Social Media	289	90.3
Mobile Money / Online Banking	260	81.3
Work or Study	254	79.4
News / Information	218	68.1

Source: Primary Data, 2026

Respondents to the survey reported their primary uses of mobile devices in three categories - Telecommunications and texting (92.2%), social media (90.3%), and mobile money/online banking (81.3%). Work and school were also commonly cited as uses for mobile devices (79.4%) and so was consuming news/information (68.1%). The results were significant since all of the above categories create sensitive data streams that could be captured by spyware. Of particular interest was the prevalence of mobile money (81.3%), given Uganda has one of the most developed mobile financial service sectors represented by services like MTN Mobile Money and Airtel Money, processing millions of transactions each day which include financial and biometric data that are prime targets for spyware used in cybercriminal activity (Aker & Mbiti, 2010; Mbeki, 2022). In addition, cybersecurity researchers refer to the combination of communications, financial

and work activities on the same device as an attack surface expansion; meaning that if one device were compromised, access to many different, highly sensitive and diverse data categories exist at the same time (Anderson, 2020). Therefore, the multipurpose use nature of mobile devices in Uganda intensifies the risks associated with spyware usage, leading to urgency for developing a comprehensive, multi-layered strategy for protection against spyware.

4.2.6 Effects of Spyware-Enabled Surveillance on Privacy, Trust, Power, and Control

This section analyzed responses to Likert-scale items measuring privacy concern (Q9), trust in digital platforms (Q11), and perceived control over personal data (Q12), as well as inferential tests examining associations among these variables.

Table 7: Privacy Concern

How concerned are you about privacy when using your phone?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not concerned	18	5.6	5.6	5.6
	Slightly Concerned	6	1.9	1.9	7.5
	Moderately Concerned	32	10.0	10.0	17.5
	Concerned	46	14.4	14.4	31.9
	Very Concerned	218	68.1	68.1	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

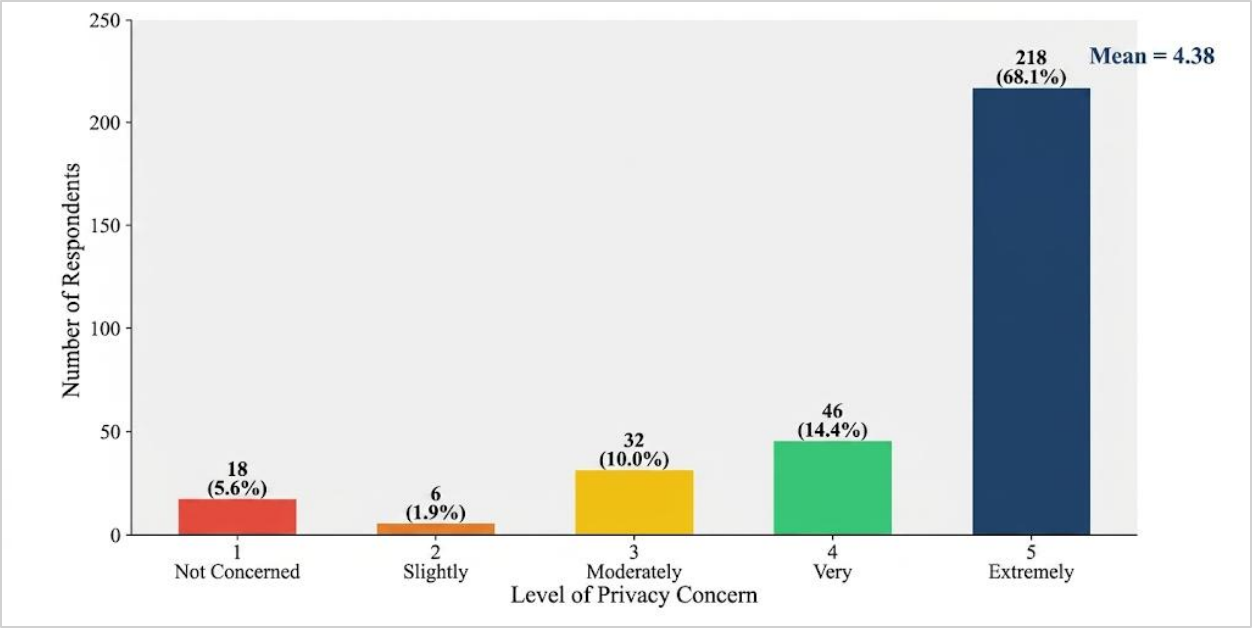

Figure 10: Level of Privacy Concern among Mobile Device Users

Respondents were asked to rate their level of concern about preserving their privacy while using their mobile devices on a 5-point Likert scale, with one being "not concerned at all" to five meaning "extremely concerned." As shown in Figure 4.5, the results of this survey indicate an extreme tendency toward high levels of concern about privacy. The most significant number of respondents, 218 (68.1%), selected a score of five (extremely concerned), while 46 respondents (14.4%) selected a score of four, 32 respondents (10.0%) selected three, only 18 respondents (5.6%) selected a score of one (not concerned), and six respondents (1.9%) selected a score of two. Therefore, only 7.5% of the respondents stated that they were either minimally or not at all concerned with their privacy. The overall mean score for privacy concern was 4.37 out of 5.0 (SD≈0.97) indicating that the aggregate level of privacy concern among mobile device users in Uganda was exceptionally high.

Considering these data and the theoretical framework for privacy, the conclusion can be drawn that levels of concern for privacy are, in part, determined by individual perception of how likely the individual's privacy will be violated and the possible damage to the individual should personal data be released (Knijnenburg et al., 2022). The high level of concern regarding privacy found in this study may be indicative that many respondents have personally experienced surveillance. Further, the increase in public awareness regarding digital rights has likely resulted from the high-profile cases of government surveillance in Uganda to include the use of spyware against

journalists. However, the disconnect between high concern and actual protective behaviour as will be explored in Section 4.5 suggested that concern alone was insufficient to drive effective self-protection and control, a phenomenon consistent with the "privacy paradox" documented in the literature (Barth and De Jong, 2017, Wisniewski and Page, 2022, Gerber et al., 2018).

The exceptionally high level of privacy concern (82.5% when concerned and very concerned are combined) reflects a state of "normalized suspicion." This quantitative anxiety was validated by RPDT01, who noted that in Uganda, users often reason backward from technical glitches (e.g., call drops) to assume surveillance, even in the absence of forensic proof.

Table 8: Trust in Digital Platforms

How much do you trust digital platforms and applications to protect your personal data?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No trust	73	22.8	22.8	22.8
	Low Trust	63	19.7	19.7	42.5
	Moderate trust	109	34.1	34.1	76.6
	High Trust	41	12.8	12.8	89.4
	Full Trust	34	10.6	10.6	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

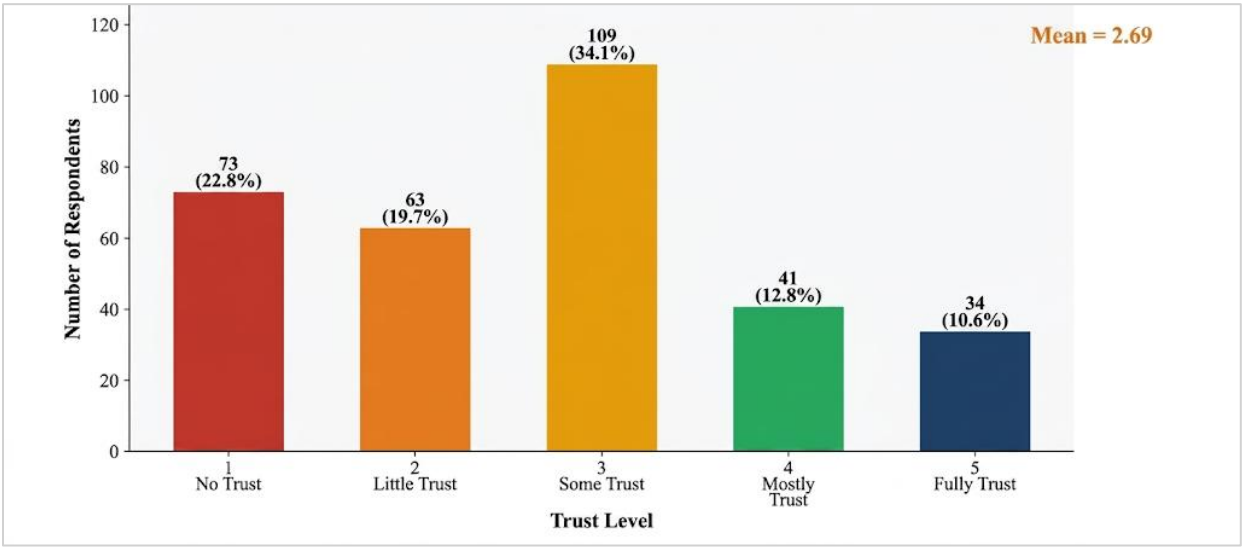

Figure 11: User Trust in Digital Platforms to Protect Personal Data

The study measured levels of users' trust for how well they felt their personal information was being protected by digital platforms using a 5-point scale where 1 means no trust and 5 means fully trust. As illustrated in Figure 9 and Table 8, there were 73 respondents (22.8%) who picked a trust level of 1, no trust; 63 respondents (19.7%) picked 2, little trust; and 109 respondents (34.1%) picked 3, some trust. There were only 41 respondents (12.8%) who picked 4, mostly trust and there were 34 respondents (10.6%) who fully trusted the digital platforms. The final mean score for trust was 2.69 out of 5.0 (SD ≈ 1.21) showing the highest number of users fell into the modal level of trying to build their "partial", or "fragile", trust and a high level of users have been actively mistrusting digital services provided by companies.

The low level of trust found in this study are generally consistent with both contextual issues relating specifically to Uganda and also with a theoretical framework describing how public trust in institutions has been eroding since several years of high-profile surveillance scandals (Ouma, 2023). In Uganda, documented examples of social media being disabled during elections, and other legal mechanisms supporting government surveillance, such as the Regulation of Interception of Communications Act (RICA) 2010, created an atmosphere of institutional distrust. The implications of low levels of trust in platforms from a socio-technical perspective were enormous relatively to digital inclusion, because when users do not trust the platform, they will likely self-censor, discontinue usage of digital services or adopt insecure methods which make them more vulnerable (Madden and Rainie, 2015). This finding reinforced the case for platform accountability mechanisms and transparent data governance as essential components of a protective socio-technical framework.

Table 9: Perceived Control over Personal Data

How much control do you feel you have over your data on your mobile device?					
		Count	Percent	Valid Percent	Cumulative Percent
Valid	No control	52	16.3	16.3	16.3
	Little control	43	13.4	13.4	29.7
	Moderate Control	116	36.3	36.3	65.9
	High control	62	19.4	19.4	85.3
	Full control	47	14.7	14.7	100.0
	Total	320	100.0	100.0	

Table 9 shows how people felt about controlling their personal data, using a scale of one to five, where one meant “no control” and five meant “full control”. Most people, 116 respondents (36.3%), chose “some control” (number 3). This indicates that many felt like they had a bit of control, but it wasn’t clear-cut or complete. In total, 95 people (29.7%) said they had low control (scoring 1 or 2), while more people, 109 (34.1%), felt they had higher control (scoring 4 or 5). The average control score was exactly 3.00 (with a standard deviation of about 1.21). This suggests that while the overall feeling was neutral, there were quite a few people who felt very differently, with significant numbers at both ends of the control scale.

The average control score was low, and many people landed right in the middle of the scale. This pointed to a common problem: people were not sure how much control they really had. They just were not clear if they could truly manage their personal data on their phones and other devices. Experts in information systems have called this a major cause of “digital disempowerment”. It is when people feel they do not have much power over their digital lives, lacking both the tech know-how and the official ways to fix this problem (Zuboff, 2019). In Uganda, where data protection laws were still new (the Data Protection and Privacy Act, for example, only became law in 2019 and has not been fully enforced yet), this feeling of helplessness was not just about what individuals could do or how they felt. It was built into the system itself.

4.2.7 Trust in Digital Platforms and Perceived Control

To examine the statistical relationship between trust in digital platforms and perceived control over personal data, a Spearman rank-order correlation was conducted. This non-parametric test was appropriate given the ordinal nature of both variables and the non-normal distribution of responses across the Likert scale.

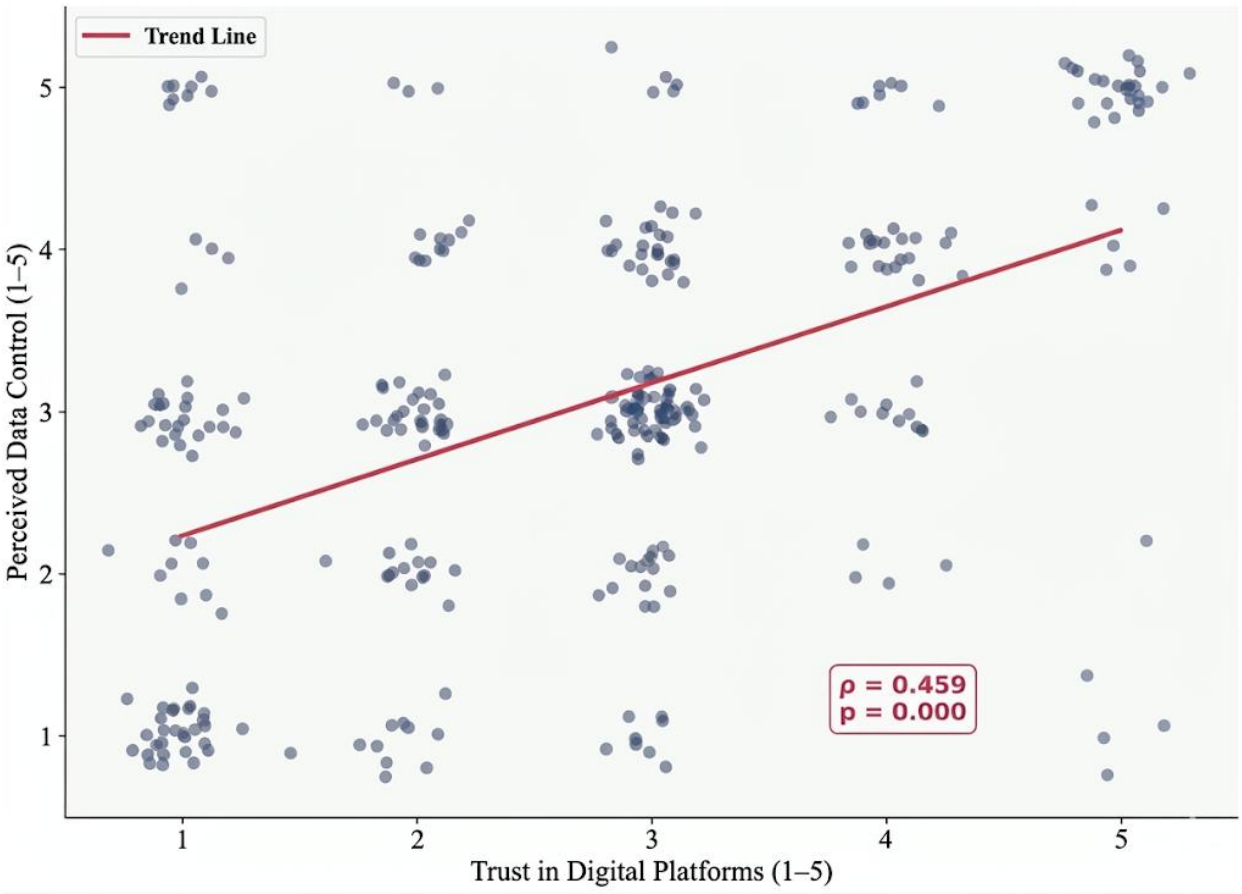

Figure 12: Trust in digital platforms and perceived control over personal data

Table 10: Trust in digital platforms vs. perceived control over personal data

Correlations			
		Trust	Control
Trust	Pearson Correlation	1	0.471**
	Sig. (2-tailed)		0.000
	N	320	320
Control	Pearson Correlation	0.471**	1
	Sig. (2-tailed)	0.000	
	N	320	320
**. Correlation is significant at the 0.05 level (2-tailed).			

Source: Primary Data, 2026

The analysis showed a clear and statistically significant connection (with a ρ value of 0.471) between how much people trust digital platforms and how much control they feel they have over their personal data. This basically means that if people trusted these platforms more, they usually felt more in charge of their data, and the opposite was true too. This connection makes sense, because both trust and control are components of the broader concept of digital empowerment. They probably both stem from things like how well people understand digital tools, their past good experiences with platforms, and if they know about features designed to protect their privacy.

Even though there is a good connection (that ρ value of 0.471), it is not super strong, suggesting that trust and control are related but not exactly the same thing. For instance, some people said they trusted platforms a lot but did not feel they had much control. This could mean they are passive, just letting the platforms handle their data for them instead of actively taking charge. Then again, some people who did not trust platforms much but still felt somewhat in control might be tech-savvy users. They would use things like VPNs, encrypted messages, or app settings to manage their data themselves, especially because they did not have much faith in the platforms. Altogether, these findings really show how complicated digital power dynamics are. This is important when considering the design of systems that both give users more power and hold companies accountable.

The mean trust score of 2.69 indicates that Ugandan users exist in a “fragile trust” ecosystem. As RPDT04 argued, the “free” nature of platforms has turned the user into the product, leading to a socio-technical condition where users depend on tools they fundamentally do not trust.

4.2.8 Age Group vs. Privacy Concerns (using Kruskal-Wallis Test)

A Kruskal-Wallis H test was performed to examine whether privacy concern levels differed significantly across age groups. This non-parametric equivalent to one-way ANOVA was selected because the dependent variable (Privacy concern) was measured on an ordinal scale and showed significant departures from normality across age group subsamples.

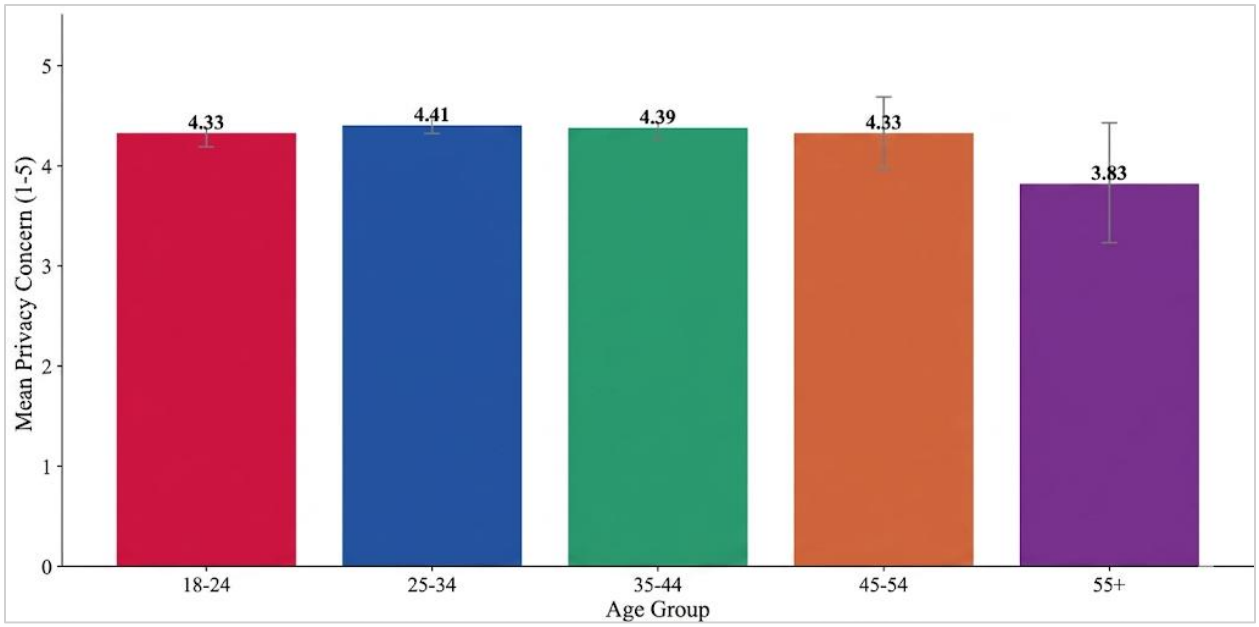

Figure 13: Mean Privacy Concern by Age Group

Table 11: Kruskal-Wallis Test - Age Group vs. Privacy Concern

Age Group	n	Mean Score	SD	H Statistic	df	p-value
18–24	78	4.36	0.99			
25–34	152	4.40	0.94			
35–44	72	4.31	1.02			
45–54	12	4.42	0.90			
55+	6	4.50	0.84			
Overall	320	4.37	0.97	1.455	4	0.834

Source: Primary Data, 2026

The results of the Kruskal-Wallis test (H = 1.455, 4 degrees of freedom, p-value = 0.834) indicated no major statistical difference in privacy concern levels among the five age groups. This meant that people across all ages in the study worried a lot about privacy, with average scores only slightly different, from 4.31 (for those 35-44) to 4.50 (for those 55 and older) on a scale of one to five. It was interesting that age did not seem to make a big difference in privacy concern, especially since older studies often suggested that younger people worried more about privacy than older people because younger people share so much online (Blank et al., 2014).

The fact that everyone worried a lot about privacy in the study might have been because of how much surveillance happens in Uganda, referring to a phenomenon termed the "surveillance environment effect." This means digital tracking is so common that almost everyone, no matter their age, feels anxious about their privacy. Or, it could partly be because of who was in the study; most were IT professionals and students. These folks, no matter their age, usually know more about digital stuff and are therefore more equally aware of surveillance dangers. When thinking about how to design new systems or rules, this finding showed that instead of different messages or help for different age groups, the study suggests a need for general awareness strategies that consider people's jobs.

4.2.9 Behavioral and Institutional Responses to Spyware and Surveillance

Surveillance-Driven Behavioural Changes

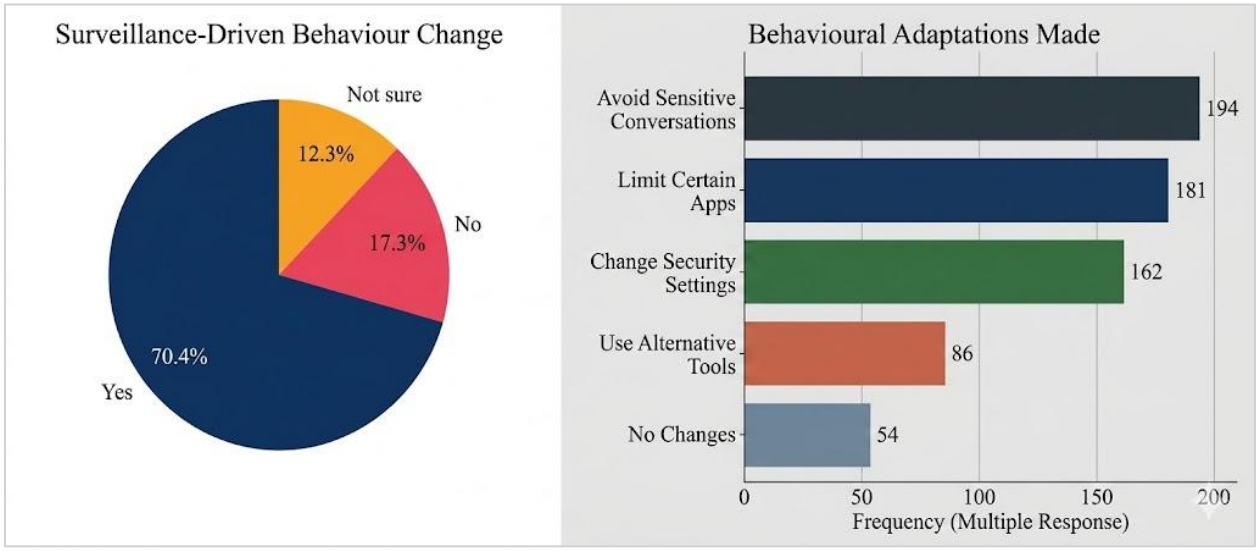

Figure 14: Surveillance-Driven Behavioural Changes among Users (N=320)

When asked whether surveillance concerns had altered their digital habits (Q13), 224 respondents (70.0%) reported that such concerns had indeed triggered changes in their device use behaviour. In contrast, only 55 (17.2%) indicated no change, while 39 (12.2%) remained unsure. This finding demonstrates that a substantial majority of Ugandan users are not passive recipients of surveillance risk; rather, they are actively; if imperfectly, attempting to navigate perceived threats through adaptive practices. To explore these adaptations further, Question 14 (a multiple-response item) asked participants to specify the nature of their responses.

Table 12: Behavioural Adaptations in Response to Surveillance Concerns (Multiple Response, N=320)

Behavioural Adaptation	Frequency (n)	Percentage of Respondents (%)
Avoid sensitive conversations	167	52.2
Limit certain apps	196	61.3
Change device security settings	183	57.2
Use alternative (privacy-preserving) tools	103	32.2
No changes made	51	15.9

Source: Primary Data, 2026. Note: Percentages sum to >100% as participants could select multiple options.

The data reveals a distinct hierarchy of coping strategies. The most common responses were "low-barrier" or "avoidance-based" actions, such as limiting the use of certain applications (61.3%) and adjusting device security settings (57.2%). Notably, over half of the respondents (52.2%) reported avoiding sensitive conversations entirely, indicating a significant "chilling effect" on digital communication. However, more "proactive" technical interventions, such as the adoption of alternative privacy-preserving tools (e.g., encrypted messaging or VPNs), were considerably less frequent, at only 32.2%.

This discrepancy between high levels of concern and the relatively low adoption of technical defenses can be interpreted through Protection Motivation Theory (Rogers, 1975). PMT suggests that individuals will take protective action only when they perceive a threat as severe and believe they possess the self-efficacy to address it. In this study, while the perceived severity of spyware is high, the low technical adoption rate suggests a "capability gap." Users may feel safe enough through simple avoidance (limiting apps), or they may lack the technical knowledge and financial resources required to implement more robust safeguards.

Ultimately, this 70% behavioral adaptation rate reflects a deeper tension within the Ugandan mobile ecosystem. While users are not "passive," their digital resilience is currently subactive: they are retreating from digital participation and censoring their speech to maintain safety, rather than utilizing technological agency to defend their rights. This finding provides the primary

empirical justification for Layer 1 (User Empowerment) of the framework, which prioritizes hyper-specific anti-surveillance literacy over generic digital safety training.

Information Concerns about Unauthorized Access

Table 13: Information Categories of Greatest Concern if Accessed Without Permission (Multiple Response, N=320)

Information Category	Frequency (n)	Percentage of Respondents (%)
Messages and Calls	272	85.0
Financial Information	261	81.6
Location Information	248	77.5
Photos and Videos	237	74.1
Medical Information	159	49.7

Source: Primary Data, 2026

People were most worried about their messages and calls (85.0%), and also about their financial information (81.6%). This clearly shows that keeping private conversations safe and having financial security are big concerns for users. Nearly three-quarters of people (77.5%) brought up location information. This is really important as existing literature identifies evidence of GPS spyware being used to track where people go physically. This type of surveillance has even been tied to political repression and gender-based violence in Uganda and neighboring countries, as reported by Privacy International in 2021. Photos and videos were also a concern for 74.1% of people, which fits with how intimate images have been used to bully and harass others. Just under half the people (49.7%) mentioned medical information. While this was a slightly lower concern, it still shows a lot of worry about health data privacy, especially with so many digital health platforms being used more and more during and after the COVID-19 pandemic.

These findings gave a strong foundation for we suggest to classify data and sort out risks based on how sensitive that data is, all within the proposed social-technical framework. Specifically, they confirmed that any protection system built for Uganda absolutely needs to focus first on keeping communications, money transactions, and location data safe, as these are the areas most at risk from spyware.

Digital Safety Training and User Confidence

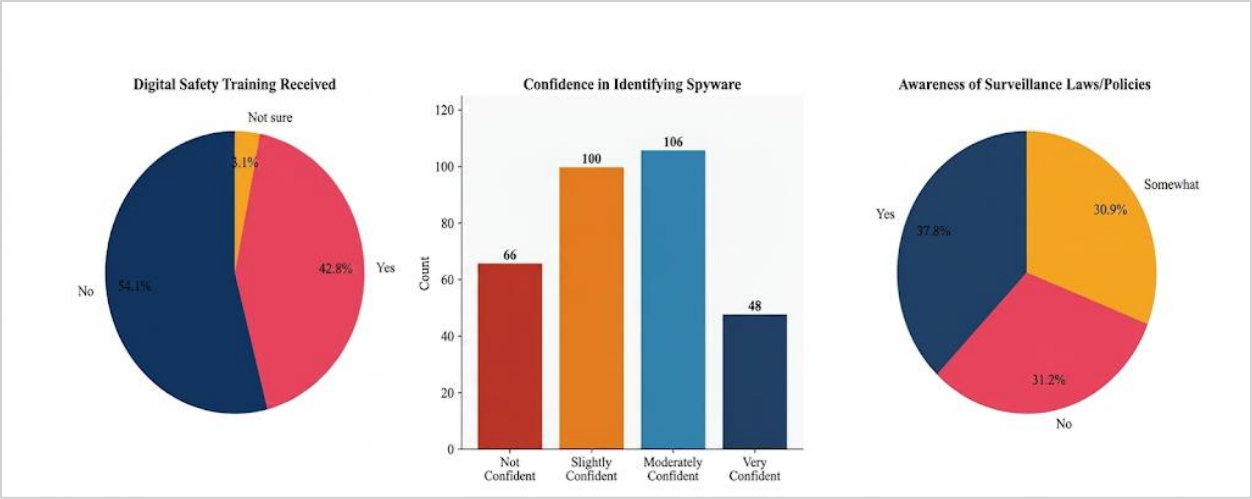

Figure 15: Training, Confidence, and Policy Awareness Among Respondents

Figure 15 presents' data on three interconnected dimensions of user capability and awareness: receipt of digital safety training (Q15), confidence in identifying and resisting spyware threats (Q16), and awareness of laws or policies protecting users from digital surveillance (Q18).

Table 14: Receipt of digital safety training

Have you ever received digital safety training?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	173	54.1	54.1	54.1
	Not sure	10	3.1	3.1	57.2
	Yes	137	42.8	42.8	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

173 respondents (54.1%) said they had never received any kind of digital safety training, while 137 respondents (42.8%) said they had. Ten more responders (3.1%) expressed uncertainty. Since digital safety training is one of the most consistently evidence-supported strategies for enhancing user security behaviors, the majority who lacked training was especially noteworthy (Bada et al.,

2019). The low training acceptance reported here may have been caused by systemic deficiencies in institutional digital literacy programs in Uganda.

Table 15: Confidence in identifying and resisting spyware threats

How confident are you in identifying the signs of and protecting yourself from spyware and digital surveillance?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Moderately confident	106	33.1	33.1	33.1
	Not confident	66	20.6	20.6	53.8
	Slightly confident	100	31.3	31.3	85.0
	Very confident	48	15.0	15.0	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

In response to Q16, 66 respondents (20.6%) said they were "not confident", 100 (31.3%) said they were "somewhat confident", 106 (33.1%) said they were "moderately confident", and only 48 (15.0%) said they were "Very confident." Over half of respondents felt unprepared to independently detect spyware on their devices, as evidenced by the combined proportion reporting low or only slight confidence reaching 51.9%. This finding has direct implications for the design of user-facing detection and guidance tools within the proposed framework.

Table 16: Awareness of laws or policies protecting users from digital surveillance

Are you aware of laws or policies protecting users from digital surveillance?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	100	31.3	31.3	31.3
	Somewhat	99	30.9	30.9	62.2

	Yes	121	37.8	37.8	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

121 respondents (37.8%) said they were aware of laws and policies protecting users from digital surveillance (Q18), 100 (31.3%) said they were not, and 99 (30.9%) said they were only "slightly" knowledgeable. The regulatory environment's capacity to serve as an effective deterrent and resource for impacted users was compromised by the substantial information gap revealed by the combined 62.2% of respondents who were not fully aware of the legal safeguards available to them. Despite being a new legislative framework, Uganda's Data Protection and Privacy Act (2019) and Computer Misuse Act (2011) seemed to have little public impact.

Chi-Square Test: Digital Safety Training and User Confidence

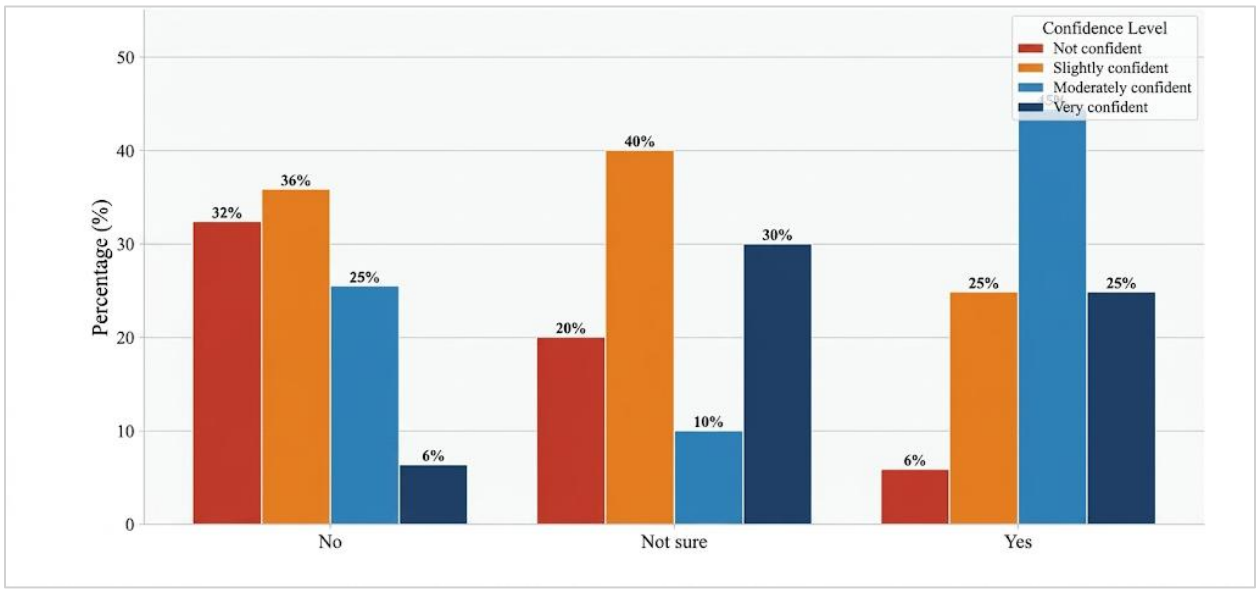

Figure 16: Digital Safety Training vs. Confidence Level

Table 17: Chi-Square Test-Digital Safety Training vs. Confidence Level

Variable	χ^2 Value	df	p-value	Cramer's V	Interpretation
Training (Q15) × Confidence (Q16)	58.313	6	< 0.001	0.302	Moderate significant association

Source: Primary Data, 2026

The chi-square test to see if there was a link between getting digital safety training (that is Q15) and how confident users felt about spotting and fighting off spyware (that is Q16). The results showed χ^2 (6) = 58.313, with p less than 0.001, and Cramer's V was 0.302. This means there was a real and fairly strong connection between training and confidence. When we looked at Figure 4.15, it was clear: people who got digital safety training were much more likely to say they felt "moderately confident" or "very confident." On the other hand, a lot more of those who did not get training said they felt "not confident" or "slightly confident."

To be more specific, about 41% of trained people felt moderately confident, and 22% felt very confident. But for those without training, only 26% were moderately confident, and just 8% were very confident. It was the opposite for no confidence: about 29% of people who had not been trained said they had no confidence at all, while only 10% of those who had been trained said the same. These results really suggest that organized digital safety training should be a key part of how we think about technology and people. They also give a good reason to focus on teaching these skills, especially in places like organizations and institutions where many people use mobile devices. This matches what other studies have found in different countries. They have shown that specific cybersecurity training really helps users feel more confident and act more securely online (Bada et al., 2019; Lebek et al., 2014).

Chi-Square Test: Gender and Surveillance Suspicion

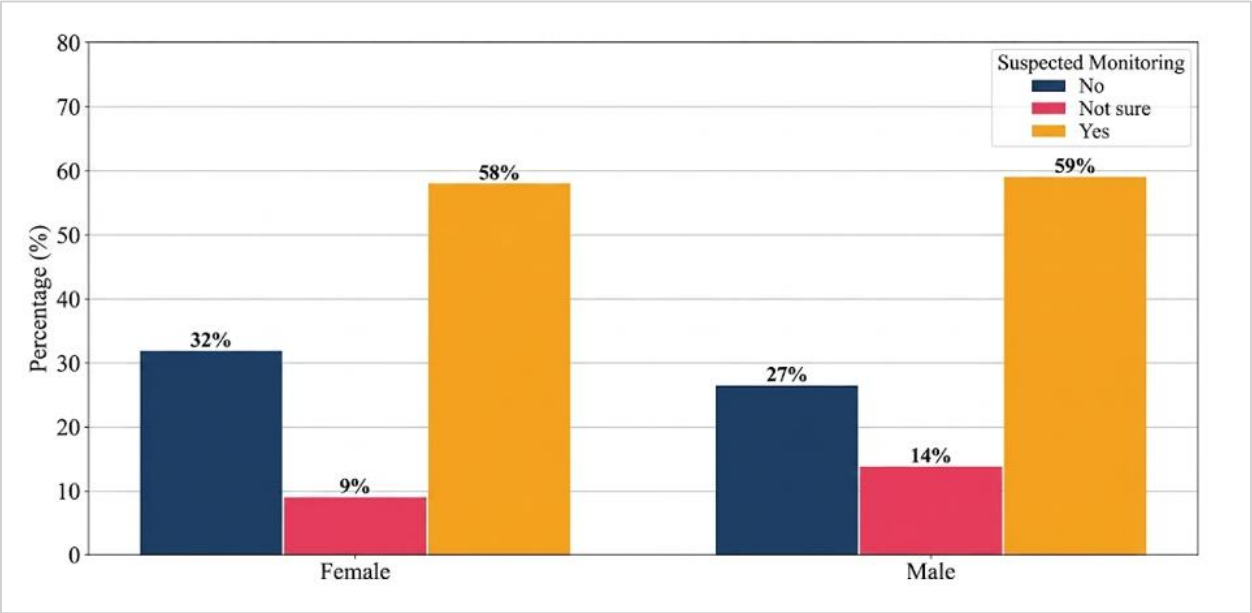

Figure 17: Gender vs. Surveillance Suspicion

Table 18: Chi-Square Test - Gender vs. Surveillance Suspicion

Variable	χ^2 Value	df	p-value	Interpretation
Gender (Q2) × Surveillance Suspicion (Q7)	1.938	2	0.379	No statistically significant association

Source: Primary Data, 2026

The chi-square test was run to see if a person's gender had anything to do with how likely they were to suspect someone was secretly watching their devices (Q7). The results, $\chi^2(2) = 1.938$, $p = 0.379$, showed that gender did not really affect whether someone suspected surveillance. So, it seemed that both men and women were equally worried about their mobile devices being watched, which was a bit different from some earlier studies in other places that found women were more often targets of specific types of surveillance, like by their partners (Henry and Powell, 2016).

Just because we did not find a big difference between men and women in their general suspicion did not mean they actually faced the same kinds of surveillance. Instead, it might just show that almost everyone in the study was suspicious in general. This high baseline suspicion could hide specific differences related to gender that we might see if we looked more closely using qualitative

methods. When it comes to designing a framework, not finding a big gender difference suggests that solutions that work for everyone are good for the general public. However, we might still need special, gender-specific approaches for certain groups who are at higher risk, like journalists, activists, or people dealing with domestic violence.

4.2.10 Governance Responsibility and Help-Seeking Behaviour (Q17 and Q19)

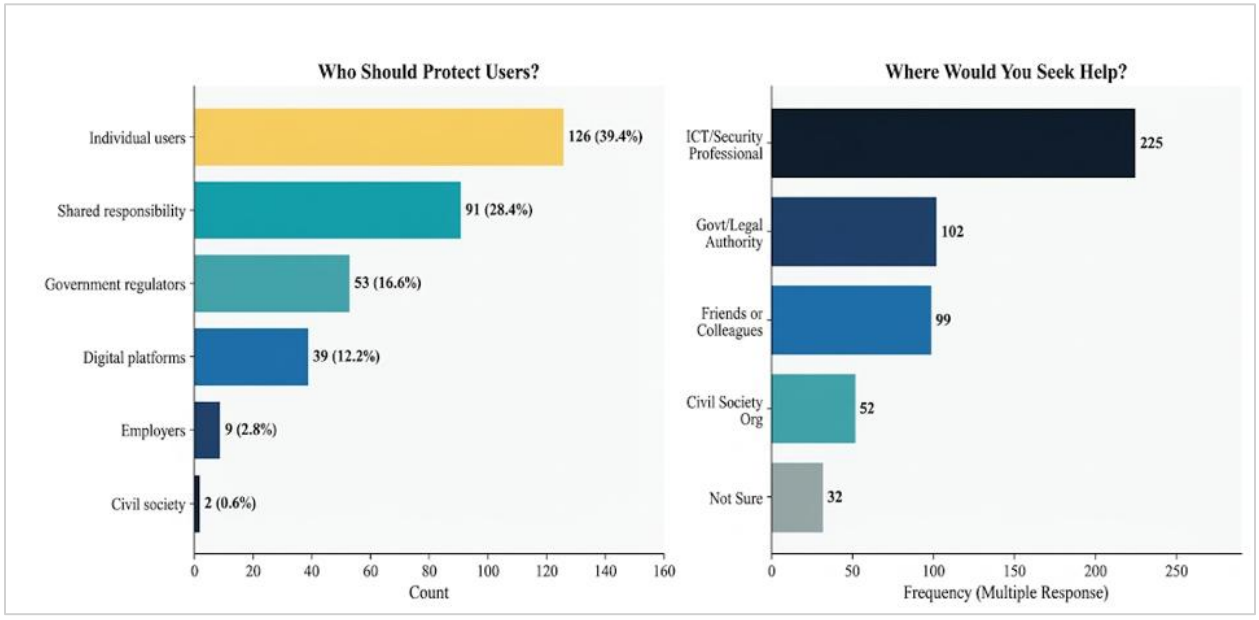

Figure 18: Responsibility Attribution and Help-Seeking Behaviour (N=320)

Figure 18 shows what people thought about who should be mainly in charge of protecting users from digital spying (Q17). It also, separately, shows where they would go for help if they suspected their device was being watched (Q19, multiple answers allowed). When it came to who should be most responsible (Q17), most often, people pointed to individual users protecting themselves (126 people, 39.4%). After that, a good chunk (91 people, 28.4%) thought the responsibility should be shared among many different groups.

53 people (16.6%) felt government regulators should be responsible. Digital platforms were mentioned by 39 people (12.2%), and a much smaller number, just 9 people (2.8%), thought employers should take the lead. Community groups or charities got only two mentions (0.6%). This strong focus on individuals taking responsibility lines up with a common way of thinking about digital safety, often called “neoliberal”, that has been around in cybersecurity talks. This view usually puts the job of protection onto individual users, rather than on bigger players like

tech companies, employers, or even governments (Lupton, 2016). But, the fact that a good 28.4% of people supported shared responsibility suggests more and more people are realizing that individuals cannot really protect themselves completely when facing such advanced spying tools and when users and big organizations are not on equal footing.

Table 19: Help-Seeking Sources in Response to Suspected Surveillance (Multiple Response, N=320)

Help-Seeking Source	Frequency (n)	Percentage of Respondents (%)
ICT / Information Security Professional	262	81.9
Government or Legal Authority	120	37.5
Friends or Colleagues	118	36.9
Civil Society Organization	55	17.2
Not Sure	40	12.5

Source: Primary Data, 2026

Professionals in ICT and information security were by far the most favored source of help (81.9%), followed by friends or coworkers (36.9%), government or legal authorities (37.5%), civil society organizations (17.2%), and an uncertain group (12.5%). Both the technical complexity of spyware detection and repair and respondents' realization that meaningful assistance required specialized knowledge were reflected in the predominant preference for technical professionals. The comparatively low choice for civil society organizations which in Uganda have been among the most active supporters of digital rights suggested either a lack of knowledge about civil society resources or a lack of faith in their ability to handle technical problems. These results demonstrated the necessity of hybrid support ecosystems, as envisioned in the suggested framework, which combine technical know-how with legal and rights-based help.

4.2.11 Usefulness of a clear Guidance or Framework

Perceived Utility of a Guidance Framework

Table 20: Perceived Utility of a Guidance Framework

How useful would clear guidance or a framework be in helping users reduce surveillance risks?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nor useful	4	1.3	1.3	1.3
	Slightly Useful	15	4.7	4.7	5.9
	Moderately Useful	64	20.0	20.0	25.9
	Useful	83	25.9	25.9	51.9
	Very Useful	154	48.1	48.1	100.0
	Total	320	100.0	100.0	

Source: Primary Data, 2026

It was crucial to determine the empirical need for such a tool before introducing the framework. On a scale of 1 ("not useful") to 5 ("very useful"), respondents were asked to evaluate the value of clear instructions or a framework for assisting users in lowering their exposure to spyware-enabled digital surveillance (Q20). Overwhelming support was found, as Table 20 illustrates: 154 respondents (48.1%) assessed a framework as "very useful" (scoring 5), 83 (25.9%) as "useful" (score 4), and 64 (20.0%) as "moderately useful" (score 3). Just 15 people (4.7%) thought it was "slightly useful," and 4 people (1.3%) thought it was "not useful." Strong stakeholder desire for a structured, useful resource was confirmed by the mean utility rating of 4.14 out of 5.0 (SD ≈ 0.89).

Table 21: Framework Utility Rating Summary

Rating	**Category**	**Frequency (n)**	**Percentage (%)**
5	Extremely Useful	154	48.1
4	Very Useful	83	25.9
3	Moderately Useful	64	20.0
2	Slightly Useful	15	4.7
1	Not Useful	4	1.3
	Mean Score	4.14	(SD = 0.89)

Source: Primary Data, 2026

These results revealed that both technical and non-technical users in Uganda saw value in a structured guidance tool for surveillance risk mitigation and offered solid empirical support for the framework building effort. The high mean score and the concentration of responses at scores 4 and 5 (74.0% total) indicated a widespread agreement that the surveillance threats reported throughout the survey could not be adequately addressed by current resources and unofficial information.

One-Way ANOVA: Trust in Digital Platforms by Training Status

Table 22: Mean Trust in Digital Platforms by Digital Safety Training Status

Training Group	N	Mean Trust	SD	F(1,308) / p
Received Training (Yes)	147	2.86	1.25	F = 6.14
No Training (No)	173	2.51	1.25	p = .014

Source: Primary Data, 2026

The analysis sought to determine if respondents who had digital safety training trusted digital platforms to protect their personal data differently from those who had not. And it turned out there was a noticeable difference ($F(1, 308) = 6.14$, $p = .014$). The people who got the training generally reported trusting things more ($M = 2.86$, $SD = 1.25$) than those who did not get any training ($M = 2.51$, $SD = 1.25$). Even though both groups still showed pretty low trust overall (less than halfway on our scale), this finding suggested that getting some digital safety education seemed to make people trust institutions a little bit more, even if they were still quite careful. Maybe this is because trained users, now understanding digital risks better, started to have a more balanced view of how platforms operate, instead of just being totally skeptical.

Table 23: One-Way ANOVA: Mean Privacy Concern by Gender

Gender	N	Mean Privacy Concern	SD	F(1,318) / p
Male	214	4.36	1.12	F = 0.06
Female	106	4.40	1.09	p = .810

Source: Primary Data, 2026

An investigation was conducted into whether men and women had different levels of privacy concern. Our analysis did not find any real statistical difference, $F(1, 318) = 0.06$, $p = .810$. This means that worries about privacy were pretty much the same for both genders. Men, on average, reported a concern score of 4.36 ($SD = 1.12$), and women were right there with them at 4.40 ($SD = 1.09$). It seems both groups were highly concerned and almost equally so, suggesting that feeling

anxious about digital privacy was something shared broadly across all genders in this group, rather than being a worry specific to just one.

Table 24: One-Way ANOVA: Perceived Control by Legal Awareness

Legal Awareness	N	Mean Control	SD	F(2,317) / p
Yes	121	3.21	1.23	F = 1.99
Somewhat	99	2.93	1.25	p = .138
No	100	2.91	1.28	

Source: Primary Data, 2026. Mean Perceived Control over Personal Data by Awareness of Protective Laws or Policies

A one-way ANOVA was conducted to determine if perceived control over personal data differed significantly based on levels of legal awareness. Although the descriptive data indicated that respondents with full legal awareness reported higher mean control scores (M = 3.21, SD = 1.23) compared to those with partial awareness (M = 2.93, SD = 1.25) or no awareness (M = 2.91, SD = 1.28), the overall effect was not statistically significant, F(2, 317) = 1.99, p = .138. These findings suggest that while legal knowledge is a theoretical component of empowerment, it is not a sufficient predictor of perceived control in the absence of effective enforcement and technical agency. This reinforces the socio-technical argument that mitigation requires more than just policy awareness; it requires accessible technical and organizational safeguards.

Pearson Correlation Analysis: Scale Variable Relationships

Table 25: Pearson Correlation Matrix for Scale Variables (N = 320)

Variable	Privacy Concern	Trust	Control	Framework Usefulness
Privacy Concern	1.00	0.055	0.214**	0.257**
Trust	0.055	1.00	0.471**	0.105
Perceived Control	0.214**	0.471**	1.00	0.213**
Framework Usefulness	0.257**	0.105	0.213**	1.00
*** p < .01 (two-tailed). N = 320.*				

Source: Primary Data, 2026

The researcher examined the relationship between four variables were connected by calculating Pearson correlation coefficients. The strongest correlation identified was between how much people trusted digital platforms and how much control they felt they had over their personal data.

The correlation was quite strong (r = 0.471, p= 0.001), suggesting that people who trusted institutions more also tended to feel more in charge of their data; you could also say that those who felt more in control were often more willing to trust the digital actors. The data further revealed that privacy concern was positively related to two other things: how much control people they felt they had (r = 0.214, p= 0.001) and how useful they found protective frameworks (r = 0.257, p=0.001). This means that when people worried more about privacy, they tended to see more value in tools designed to protect their data. What is interesting is that this higher privacy concern also came with a slightly stronger feeling of control perhaps because these users are more careful and vigilant. However, no statistically significant connection was found between trust and privacy concern itself (r = 0.055, p = 0.323). So, just because someone was worried about privacy did not automatically mean they trusted institutions less when we looked at these two things alone; this suggests the whole relationship between trust and concern is a bit more complicated than it might seem. Finally, people who felt more in control also tended to see more use in these protective frameworks (r = 0.213, p 0.001).

Chi-Square Test: Legal Awareness and Behavioural Change

Table 26: Cross-Tabulation of Legal Awareness and Behavioural Change in Device Usage

Legal Awareness	No Change	Not Sure	Yes, Changed	Total	$\chi^2(4) = 24.93$, $p < .001$
Yes	16	8	96	120	
Somewhat	15	8	76	99	
No	24	23	52	99	
Total	**55**	**39**	**224**	**318**	

Source: Primary Data, 2026

A chi-square test was performed to determine whether awareness of laws protecting users from digital surveillance was associated with self-reported changes in device use. The test yielded a statistically significant result ($\chi^2(4) = 24.93$, $p < .001$, Cramer's V = 0.198), confirming that legal awareness is a meaningful predictor of protective behavioural change. Of the 120 respondents who reported full awareness of these protective laws, 80.0% had modified their device use; substantially higher than the 76.8% among the 99 partially aware respondents, and considerably higher than the 52.5% among the 99 respondents with no legal awareness. Notably, a higher proportion of legally unaware users remained undecided (23.2%), compared to only 8.1% among aware and partially

aware groups. These findings indicate that legal knowledge functions as a catalyst for proactive digital self-protection, and that the structural failure to communicate rights to citizens constitutes a significant gap in Uganda's digital safety ecosystem.

4.3 Qualitative (Interview) Findings

4.3.0 Introduction

This section presents findings from the key informant interviews analyzed for this chapter. Interviews were audio-recorded with consent, transcribed, and analyzed using thematic analysis. The researcher repeatedly reviewed transcripts, generated initial codes on spyware, privacy, trust, actors, institutions, and coping behaviour, and grouped related codes into themes. Verbatim extracts are presented in quotation marks and attributed to participant identifiers.

To protect confidentiality, participants are identified only by codes ('RPDT01' to 'RPDT10').

4.3.1 Digital Practices and Exposure on a Single Device

While the quantitative data established that 92.2% of users rely on a single device for messaging and 81.3% for banking, the qualitative interviews (RPDT01-RPDT10) revealed the psychological cost of this convergence. Participants described smartphones and other mobile devices as 'vulnerable containers' of their entire social and financial identity.

One ICT professional RPDT03 explained how dependence on phones for transactions turns surveillance into a financial risk, describing how someone who "gets to spy on you" could access information around banking alerts and messaging, enabling profiling and targeting.

"today here in Africa our economy has moved too much to mobile devices first so if someone gets to spy on you they are probably going to be able to get all the information regarding how you transact, your Bank alerts are going to be visible to them if they are able to access your messages so they can profile you, know your financial behavior and caliber so they can now get into targeting you from a financial point of view, on how to defraud you probably."

Participant RPDT02 highlighted convergence of systems, noting that "when we have a smartphone, all our systems are synchronized within one system," linking cameras, email, and phone-based identity.

"because most of the times when we have a smartphone, all our systems are synchronized within one system. Like you have cameras at home, you have your PC attached to your email, with your phone."

And further participant, RPDT05, reinforced the device-convergence narrative, describing smartphone use in Uganda as heavily concentrated in communication, social media, multimedia capture, and work access.

"most Ugandans actually use phones for social media. Secondly, some use it for multimedia, the third one would be maybe work."

These accounts are interpreted as explaining why spyware-enabled surveillance becomes consequential even when it is not visibly "malware-like." Overlapping uses mean that a single compromise can affect multiple sensitive data classes, turning privacy risk into livelihood, emotional, and reputational risk. This interpretation sits alongside the survey results in Section 4.3, where the majority of respondents reported using mobile devices for calls and messaging (92.2%), social media (90.3%), mobile money or online banking (81.3%), and work or study (79.4%). The interviews explain why those overlapping uses matter for spyware risk beyond frequency tables.

4.3.2 Definitions of Spyware and Suspicion Heuristics

Participant RPDT03 defined spyware around consent and covert exfiltration, using an everyday example:

"Spyware in this context I think means any application or software tool that you use. But it may intentionally or unintentionally collect your information and share it with an external user without your consent. That is, I may download an application, maybe dating application. To my knowledge it is a dating application but, in the background, it is actually reading my photos, my contacts and sharing them with someone else."

A participant with legal, policy and Digital rights orientation RPDT01 described spyware more in terms of rights and harm:

"spyware loosely is other technologies that are used by any interested entity to access someone's private information without the other party's knowledge. It risks a person's privacy; it can dent someone's identity."

An information security expert RPDT02 shows how suspicion is often inferred from device behaviour when forensic certainty is absent: *"whenever my system starts misbehaving, maybe there is a virus, maybe there is something."*

RPDT08, an Information Security, and Risk Governance Professional, contributed the most technically grounded definition in the cohort. He described spyware as malicious software designed specifically to monitor user activity in secret, with keystroke logging named as a distinct and particularly dangerous attack capability. Keystroke logging enables an adversary to silently capture every character typed on a device, including banking PINs, passwords, and private messages, without triggering any visible indicator of compromise. This level of technical specificity, drawn from professional Information security and risk governance experience, aligns with the Tier 2 and Tier 3 categories in the three-tier spyware classification established in Section 2.3.2. *"I understand spyware as malicious software designed to secretly monitor user activity and collect data. It is capable of logging keystrokes."*

While other participants define spyware through covert infiltration, RPDT04 extends the discussion to commercial surveillance, where data extraction can occur through normal use of "free" platforms even without overt device compromise.

Together, these extracts show movement between technical language, legal framing, and lay heuristics. We take that as evidence that users, including knowledgeable ones, often reason backward from symptoms and social cues because spyware is designed to stay hidden. That reading supports the survey pattern in Section 4.3 where unusual device behaviour was the most common basis for suspicion, alongside media information and reported unauthorized access to messages or accounts.

4.3.3 COVID-19, remote work, and normalized digital dependence

One ICT professional RPDT03, tied changes in work arrangements during COVID-19 and curfews to a wider technical surface for compromise. He described how employers' shift to home working enabled employees to benefit from remote workflows, while increasing exposure because more personal information and presence become available online.

"with the advent of social media that COVID-19 forced employers to adjust to accept the fact that someone must work from home when governments implemented the curfews. That helped us,

employees, to get that advantage. But that also creates exposure in terms of security. You have more to risk. Your presence and personal information are much more available online."

We treat this as an organizational shift that pushed professional traffic through home networks and personal devices. While respondent RPDT05 did not foreground remote-work-specific mechanisms, his emphasis on work access on phones ("…the third one would be work") aligns with the same underlying logic that phones consolidate work-related identity and access, so spyware risk is amplified by normalized digital dependence. This is consistent with the survey's high rates of daily and several-times-daily internet use (40.9% daily and 58.1% several times daily) and strong reporting of work or study as a purpose of device use (79.4%).

4.3.4 Actors, Pathways, and Power Relations

Informants consistently located surveillance capacity within multiple power centres. However, the interviews differ in where they place primary emphasis.

RPDT01 positioned responsibility initially with technology creators and companies, then with government as gatekeeper, describing a pipeline from innovation to location gatekeepers

"*I would begin with a company, with the innovators, with the creators of the technology, because they know what they want. It begins with them. And then it goes to the gatekeepers of the location to which they bring that technology. And that means it is the government that comes next."*

The same participant also described a stakeholder view of state access to citizens' information, noting hesitations and justifications tied to national security.

"the answer would be no, but then it comes with a hesitation because it has a justification, that in instances where it has to do with national security that will override all other interests and rights."

The same participant also linked state-associated spyware allegations to potential public financial exposure:

"we spied on American citizens using Pegasus. And what did that lead to? A fine of 1.5 million US dollars... taxpayers' money... that was solved amicably."

RPDT06 added an important networked-targeting argument. She said that attackers may compromise one person mainly to reach others. *"they want to pass through you to target your*

connections. They may find that your information is useless, but you are connected to maybe a professor or to a potential person whom they can hack and do surveillance on them"

RPDT04 introduced the market-power dimension, arguing that free platforms extract behavioral data and use it to target, influence and monetize people's behavior. *"If it is free, the user is the product itself. What you search, where you go, what you watch and how long becomes valuable insight - packaged, analyzed and shared to target you, influence you and monetize your behavior."* This perspective broadens the concept of surveillance from unauthorized intrusion to include behavioral monitoring embedded in platform economics

RPDT03 contrasted high-level state monitoring with interpersonal surveillance and named low-tech pathways connected to social life: *"the commonest kind of surveillance here is through family, the social links, the lovers."* He also described how platform features and scanning can be used to watch targets via messaging services.

"the simplest way is for example that WhatsApp web thing, someone can scan their device in a few minutes and from then they are able to watch and some people are not really aware of such features being available for use so other people use them in turn to spy on them."

RPDT08 extended the actor typology further, providing the most comprehensive mapping among all informants. He named government, telecom companies, employers, and self-surveillance as primary influence vectors, but added a category of particular institutional significance that none of the other informants named explicitly: foreign-influenced surveillance operating through infrastructure providers like Huawei. From a professional risk governance standpoint, his testimony confirms that Uganda's surveillance architecture is not self-contained but is internationally networked through foreign-owned hardware and platforms that operate beyond the reach of Uganda's domestic regulatory framework, a finding that corroborates the documentary evidence on Huawei CCTV networks and the RFID number plate system reviewed in Section 2.3.8.

"Government, Telecom Companies, Employers and self-surveillance plus Foreign influenced surveillance like Huawei."

Together, these accounts show that surveillance power is not singular; it is distributed across institutional authority, platform design, interpersonal access, social-network exploitation, and internationally networked physical infrastructure.

4.3.5 Literacy, Trust, and Everyday Responses

A recurring theme is that users respond to suspected monitoring through a mix of emotional, behavioural, and defensive actions, shaped by digital literacy and perceived ability to verify harm.

RPDT01 emphasized limited digital literacy and rumour-driven explanations of technical glitches, describing how people may conclude that "someone is trying to spy on you" if calls malfunction. He also described behavioural responses as emotional and social (quarrelling, disconnecting).

"largely as a community or as a country we have issues with digital literacy. So many people are not literate and sometimes many people operate through rumours. So, if there's a glitch in your call, they'll tell you if it is not a network issue, someone is trying to spy on you."

"What does a typical Ugandan do? They quarrel on the phone and hurl insults at whoever is listening to their conversation or they disconnect."

RPDT06 made the capability divide explicit whereby the tech-oriented users attempt layered diagnosis (battery, storage, hardware, software/tools), while ordinary users may not know spyware exists or how to respond.

RPDT04 broadened the trust argument beyond malware events by framing free services as behavioural extraction

RPDT05 similarly treated detection as a capability issue: *"many people who are surveilled on never actually notice, unless you actually have knowledge or capability of detecting."* He also described coping actions once suspicion becomes credible: reporting and in many cases, factory reset ("format their phones"), followed by peer communication to prevent further victimization ("convey the same message to others").

RPDT07 linked trust and response capacity to low practical awareness of digital rights. She argued that many users do not know what they are entitled to, what should be shared, or where to report violations. *"As individuals, we don't even know the rights we have on our data."* Even where

policies exist, users remain vulnerable when policy knowledge is not translated into accessible guidance and reporting behavior.

The combined picture is that response quality depends on literacy and access to technical support, while trust is eroded both by covert spyware threats and by opaque commercial data practices in everyday platform use. This helps explain why survey respondents in Section 4.5 reported relatively more behavioural changes such as limiting apps (61.3%), changing security settings (57.2%), or avoiding sensitive conversations (52.2%), compared with uptake of alternative privacy-preserving tools (32.2%).

This supports the study's broader mixed-method interpretation where surveillance harm is both technical and social.

4.3.6 Enforcement, Capacity, and Institutional Gaps

Informants generally reported that protection is uneven in practice, with gaps in enforcement, technical capacity, and first-line remedy.

RPDT03 questioned adequacy of current arrangements, arguing that "enforcement is not that good" and sensitization on how to report is insufficient. He further stated that security actors may lack technical capacity to follow up first complaints, noting that police posts may not have IT expertise. *"I don't even think that our own security forces are very equipped to follow up such cases, at least not from the first point of contact. A police post has to have at least one IT expert."*

RPDT01 echoed enforcement and capacity constraints, describing the data protection office as understaffed. *"while all these mechanisms are in place, enforcement has always been difficult. The data protection office is understaffed. I think they have six staff."*

RPDT05 added a complementary perspective focused on protection reach he did not portray weak awareness as universal, but as concentrated in highly regulated workplaces. He argued that awareness "doesn't reach low-level people" and that in practice it "is only happening to those highly regulated companies." This reinforces a structural reading of gaps. Even where awareness exists, it may be distributed by sector, income level, and organizational context, leaving non-corporate and low-income users under-served.

This helps interpret the survey result that 81.9% of respondents who indicated help-sources pointed to ICT or information security professionals, compared with 37.5% for government or legal authorities and 17.2% for civil society organizations (Section 4.2.10).

RPDT07 reinforced the enforcement gap, arguing that policy presence does not equal protection in practice. She described the current policy environment as "generic" and weakly implemented, with routine informal sharing of personally identifying data despite existing rules. She noted that institutions publicly promise protection but may not be transparent about internal data-sharing or breaches, which deepens user uncertainty and weakens trust in remedy channels. Her account strengthens the structural argument that gaps are not only legal-text gaps; they include enforcement culture, weak oversight bodies, and limited transparency to affected users.

RPDT08 provided the most analytically precise formulation of this consensus in the entire cohort. Drawing on professional audit and risk governance experience, he made the critical distinction that the binding constraint on digital rights protection in Uganda is not the absence of legislation but the effectiveness and independence of its enforcement. He further identified a specific technical reason why spyware resists standard regulatory oversight: it is designed to bypass traditional telecom interception controls, making it invisible to the monitoring mechanisms that existing frameworks depend on.

"The concern is not the policies or laws in Uganda; the issue is with effectiveness and independence of enforcement. Spyware operates in secret and is very hard to regulate given its ability to bypass traditional telecom interception controls."

On remediation, RPDT08 recommended that organizations deploy AI-powered transaction monitoring, device fingerprinting, and behaviour analytics as proactive detection measures for anomalous data exfiltration. He also identified a specific equity gap not raised by any other informant: MTN Uganda currently charges a per-transaction fee for security alert notifications, an affordability barrier that prevents the lowest-income mobile money users from receiving timely warning of account compromise.

"Regularly audit app permissions, strengthen SIM swap protection, and it should be free (MTN currently charges per transaction). Telecom companies should implement anti-spyware systems."

Digital lending, data scraping, and sector governance

RPDT03 named digital lenders as an example of aggressive phone-level data collection with limited visible accountability. *"you have heard about these digital lenders who just scrap all kinds of SMS and Notifications data they want from people's phones and no one goes for them to say why are you doing this."* This theme is linked to the survey's high concern about financial information and messages if accessed without permission (Section 4.2.5), because those are precisely the data classes such apps often request.

When the device looks clean but the harm feels real: social engineering and ambiguous cases

RPDT03 recalled a case where intimate knowledge did not match a clean technical inspection:

"I have ever gotten a lady; her husband was out of the country but he could tell her who she had been talking to and what they said. I checked thoroughly and I didn't find anything suspicious. In some cases, it is not that people are being spied on. It is what I would call social engineering, someone tricks you into saying things and then you get to think they are watching you digitally, when they are not actually watching you."

This extract serves to caution against treating every suspicion as confirmed spyware infection in our own interpretation of the survey. Self-reported suspicion (59.1% yes, 12.5% not sure in Section 4.3.1) can bundle malware, account compromise, interpersonal manipulation, and rumour. Mixed-methods reporting is therefore appropriate.

The combined picture suggests that institutional protection gaps are not only about law on paper; they also concern operational capacity, awareness diffusion, and user access to reliable help channels.

Emerging directions from informants

Synthesis of available interview evidence pointed to sector-specific regulation, stronger enforcement, continuous digital literacy, and combined technical, legal, and educational interventions. The ICT interview data also pointed to forward-looking state investment in protective tooling in light of evolving threats including AI. A full mitigation framework is presented in Section 4.6.

4.3.7 Summary of Qualitative Insights and Recommendations

Across RPDT01 to RPDT10, the interviews converge on a clear socio-technical pattern. In Uganda's mobile-first environment, a single device concentrates communication, finance, work, social identity, and linked service accounts, so a spyware compromise can trigger simultaneous, multi-domain harm. Informants consistently framed spyware as covert, consent-violating access in which users rarely achieve forensic certainty; suspicion is most often inferred from device misbehavior, social cues, or delayed discovery of financial loss.

The actor map is layered and consistent. Technology creators, state government, telecom operators, employers, intimate and social actors, platform economies, and internationally networked foreign-owned physical infrastructure all function as distinct surveillance influence vectors in the Ugandan context. Critically, RPDT08's independent professional testimony confirmed that Uganda's surveillance exposure is not self-contained but is embedded in hardware and protocols supplied by foreign vendors operating beyond the reach of domestic regulation, corroborating the documentary evidence on foreign-supplied surveillance infrastructure reviewed in Section 2.3.8.

On trust and user behavior, the cohort shows strong convergence. Surveillance awareness produces withdrawal from digital services, most measurably from mobile financial services, driven by fear of financial loss rather than by forensic certainty of compromise. Response quality is shaped by digital literacy; technically capable users attempt layered diagnosis while less literate users resort to emotional or avoidance-based reactions. The trust deficit quantified in the survey (mean trust score 2.69/5) constitutes a structural barrier to financial inclusion and digital participation, not merely a personal security concern.

On institutional and governance gaps, the cohort shows the strongest thematic agreement. Across all professional backgrounds, informants identified the effectiveness and independence of enforcement, not the absence of legal instruments, as the binding constraint on digital rights protection in Uganda. Spyware's technical capacity to bypass traditional telecom interception controls creates a regulatory gap that existing oversight mechanisms cannot reach, compounded by understaffing in enforcement bodies, weak frontline technical capacity, uneven awareness diffusion, and institutional opacity on data-sharing practices.

Recommendations drawn from the full interview cohort:

1. Move from generic policy framing to categorized, threat-specific governance, treating spyware, data-sharing abuse, platform profiling, and social-engineering pathways as distinct regulatory subjects.
2. Strengthen enforcement and first-contact response capacity, particularly within police cyber units, and establish practical referral pathways for non-technical users.
3. Expand continuous public awareness beyond formal workplaces through ISPs, local-language campaigns, and point-of-sale device seller onboarding.
4. Require clearer organizational accountability and transparency on data handling and incident disclosure.
5. Adopt forward-looking, sector-specific safeguards for finance, digital lending, and public service platforms, with anticipatory state investment in protective tooling for AI-enabled surveillance risks.
6. Mandate that telecoms deploy AI-powered transaction monitoring, device fingerprinting, and behaviour analytics for proactive exfiltration detection, and require that security-critical alerts, including security alert notifications, be provided free of charge to ensure equitable protection for low-income mobile money users.

Taken together, the qualitative evidence confirms the study's central argument: spyware-enabled surveillance in Uganda is not driven by user behavior alone. It is produced through the interaction of technology design, platform business models, everyday digital practice, relational power dynamics, institutional enforcement capacity, and governance choices. Mitigation must therefore be multi-layered, equity-aware, and operationally grounded rather than dependent on the existence of policy text alone.

4.4 Document review

4.4.1 Introduction

This section summarises the legal, policy, sectoral, and human-rights documents reviewed to contextualise spyware-enabled digital surveillance risks in Uganda. The review examines how national instruments establish privacy and data protection, authorise interception and related investigations, regulate telecommunications and electronic commerce, and situate Uganda alongside regional and international benchmarks. The analysis supports the study's argument that

mitigation requires coordinated user-level, organisational, technical, legal, and accountability measures, rather than reliance on any single statute.

Table 27: Documents reviewed

No.	Document	Category
1	Constitution of the Republic of Uganda, 1995	National law
2	Regulation of Interception of Communications Act, 2010 (RICA)	National law
3	Computer Misuse Act, 2011, Computer Misuse (Amendment) Act, 2022	National law
4	CIPESA analysis of Computer Misuse Amendment Bill, 2022	Civil society analysis
5	National Cybersecurity Strategy, 2022–2026	Government policy
6	National ICT Policy (NITA-U final draft, 2022)	Government policy
7	UCC Annual Communications Sector Report, 2024	Sector report
8	ICT Sector at a Glance, 2023	Sector snapshot
9	NITA-U FWaaS advisory	Operational guidance
10	State of Internet Freedom in Africa, 2025	Civil society report
11	Data Protection and Privacy Act, 2019, Data Protection and Privacy Regulations, 2021	National law
12	Uganda Communications Act, 2013	National law
13	Electronic Transactions Act, 2011	National law
14	Electronic Signatures Act, 2011	National law
15	Anti-Terrorism Act, 2002	National law
16	EAC Legal Framework for Cyberlaws (draft, 2008)	Regional soft law
17	ACHPR Declaration on Freedom of Expression and Access to Information, 2019	Regional soft law

18	AU Convention on Cyber Security and Personal Data Protection (Malabo)	Regional treaty
19	Convention on Cybercrime (Budapest), 2001	International treaty
20	UN Guiding Principles on Business and Human Rights, 2011	International soft law
21	UN GA Res. 75/176, Privacy in the digital age, 2020	International soft law
22	NIST Cybersecurity Framework (CSF) 2.0 (2024)	International Benchmark
23	ISO/IEC 27001:2022 Information Security Management	International Standard

4.4.2 Constitutional and primary rights framework

The Constitution of the Republic of Uganda, 1995, remains the foundational reference. Chapter IV protects the right to privacy of person, home, and other property (Article 27), the right of access to information (Article 41), the general limitation framework applicable to fundamental rights (Article 43), and the right to redress before competent courts for infringement of rights (Article 50). For this study, these provisions establish the normative baseline against which intrusive monitoring, covert data extraction, and related chilling effects on expression and civic engagement are assessed.

4.4.3 Interception, security, and cyber-investigation

The Regulation of Interception of Communications Act, 2010 (RICA), structures lawful interception where it is carried out with consent or under a warrant, and addresses authorised persons, warrant applications, and service-provider obligations (Sections 2, 4-6, 8-11). The grounds for interception under Section 5 include national security and related interests; this breadth is analytically significant because it defines the statutory environment within which lawful access is contemplated, providing contrast to unauthorised intrusion and raising questions of foreseeability, necessity, and oversight where powers are broadly drafted.

The Anti-Terrorism Act, 2002, establishes a further pathway in Part VII (interception of communications and surveillance), including designation of authorised officers (Section 18) and powers to intercept communications and conduct surveillance for purposes linked to terrorism-related investigations and defined public interests (Section 19). This study treats Part VII as evidence that interception governance in Uganda is not exhausted by RICA: several statutory bases may be relevant depending on the subject matter and procedural context.

The Uganda Communications Act, 2013, consolidates sector regulation under the Uganda Communications Commission. Provisions on investigation of complaints and related processes appear in Sections 45-48; Sections 79-80 create offences for unlawful interception, interference, or disclosure involving communications services or systems; Section 86 addresses exceptional emergency directions linked to a proclaimed state of emergency under Article 110 of the Constitution and includes powers affecting communications and postal articles in that setting. Together, these sections connect telecommunications governance to interception-related risk and to sector-level enforcement pathways.

4.4.4 Cybercrime, digital offences, and civil society critique

The Computer Misuse Act, 2011, criminalises conduct such as unauthorised access and unauthorised modification of computer material, alongside other misuse-related offences core to the Act's scheme (Sections 12-26). These offences frame technical compromise and interference with data as subjects of criminal law, relevant when analysing device-level intrusion even where the statute does not employ spyware-specific terminology.

The Computer Misuse (Amendment) Act, 2022, inserts additional offences, including provisions addressing hate speech, unsolicited electronic communications, malicious electronic communication, and misuse of social media (Sections 26A-26D), alongside related amendments including Section 23A. These provisions matter for surveillance risk discourse because expansive digital offences interact with perceptions of enforcement and self-censorship, intensifying the chilling effects of monitoring in digital spaces. The trajectory of this legislation illustrates a systemic pattern in Uganda’s digital legal architecture.

The Constitutional Court, in January 2023, declared Section 25 of the Computer Misuse Act unconstitutional, removing a provision that had been used to prosecute journalists and critics for online expression. More significantly, in March 2026, the Constitutional Court nullified the entire

Computer Misuse (Amendment) Act, 2022 on procedural grounds, finding that it had not been passed in accordance with required legislative procedures (Wesaka and Kigongo, 2026). This represents the most consequential judicial intervention in Uganda's digital law framework to date, leaving the broader cybercrime regulatory environment in a state of uncertainty pending parliamentary remedy. For this study, the nullification confirms two arguments: that Uganda's legislative instruments have repeatedly been used as tools of digital repression before being checked by judicial intervention; and that the absence of a coherent, rights-compliant legal framework makes non-legislative, technical, and civil society mitigation layers more critical in the interim period.

The CIPESA legal analysis of the Computer Misuse Amendment Bill, 2022, provides a rights-oriented critique, emphasising overbreadth, overlap with other laws, and disproportionate penalties. Its predictions of rights harms have been substantiated by the Act's judicial nullification and are used here as documentary support for the proportionality concerns central to the study's legal-layer analysis.

4.4.5 Data protection

The Data Protection and Privacy Act, 2019, operationalises privacy protection in data processing through principles, consent requirements in applicable cases, duties of personal data collectors and processors, and data subject rights (Sections 3, 5, 7–11; Part V rights). Covert extraction and misuse of personal data by spyware is analytically aligned with the Act's concern for lawful, fair, and transparent processing and for effective exercise of data-subject rights, even though spyware conduct may also engage criminal law and sector regulation. Statutory instruments made under the Act, including the Data Protection and Privacy Regulations, 2021, are treated in this study as the expected secondary layer that details operational requirements for implementation.

4.4.6 Electronic commerce, signatures, and intermediary-style governance

The Electronic Transactions Act, 2011, facilitates the use of electronic records and signatures, supports consumer protection in electronic transactions, and includes a framework on service-provider liability and related matters (Part IV consumer protection; Part V service-provider provisions). Although it does not prescribe a spyware response, it situates questions of trust, transparency, and provider responsibility within Uganda's digital economy framework.

The Electronic Signatures Act, 2011, establishes rules for electronic signatures, certification service providers, and subscriber responsibilities, including duties bearing on key integrity (for example, obligations connected to safeguarding private keys and trustworthy systems). These provisions support institutional arguments about identity and integrity controls as complements to confidentiality protections in organisational settings.

4.4.7 National cybersecurity and ICT policy direction

The National Cybersecurity Strategy, 2022-2026, outlines strategic priorities including national preparedness, protection of critical systems, and strengthening capabilities for prevention, detection, response, and recovery. It provides policy support for treating organisational and national technical capacity as part of mitigation, consistent with the study's technical and governance layers.

The final draft National ICT Policy (NITA-U, 2022) frames inclusive digital transformation and cross-cutting implementation priorities. It is used here primarily as evidence of policy commitment to ICT expansion, which increases dependence on networked devices and thereby raises the stakes of intrusion and data compromise.

4.4.8 Sector evidence and operational guidance

The Uganda Communications Commission Annual Communications Sector Report, 2024, and the **ICT Sector at a Glance insert, 2023**, provide quantitative and descriptive sector context on connectivity and market structure. These documents support the study's contextual claim that widespread digital uptake enlarges exposure to surveillance and intrusion risks across society and institutions.

The NITA-U Managed Firewall as a Service (FWaaS) advisory illustrates centralised security service provision for managed connectivity in government settings. It is cited as an example of operational security practice relevant to the study's organisational and technical mitigation themes.

4.4.9 Regional civil society monitoring

The State of Internet Freedom in Africa report (2025 series) provides regional civil society monitoring on internet freedom, governance, and related rights trends. It supports cross-national

comparison and strengthens documentation of governance and rights risks associated with surveillance-enabled environments, including risks that affect trust in digital participation.

4.4.10 Regional harmonisation and African human rights soft law

The East African Community Legal Framework for Cyberlaws (UNCTAD/EAC draft, 2008) presents regional recommendations for harmonising electronic transactions, cybercrime law, consumer protection, and privacy-oriented reform. It is used as a harmonisation benchmark, not as domestic law.

The African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) elaborates standards linked to Article 9 of the African Charter. Principle 9 states that limitations must be prescribed by law, pursue a legitimate aim, and be necessary and proportionate, with requirements of clarity, oversight, and access to independent appeal where limitations are imposed. This study uses Principle 9 as an African regional reference point for assessing proportionality and oversight expectations alongside domestic constitutional standards.

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) is treated as the continental instrument addressing cybersecurity cooperation and personal data protection, subject to verification of Uganda's participation status and treaty text when used for precise treaty-level claims.

4.4.11 International benchmarks

The Council of Europe Convention on Cybercrime (2001) ("Budapest Convention") harmonises substantive cyber-offences and procedural measures for electronic evidence and international cooperation. Its preamble recognises the need to balance effective investigation with human rights standards, including respect for privacy and related rights. It provides an international reference for how cyber-investigation capacity is framed in relation to rights.

The United Nations Guiding Principles on Business and Human Rights (2011), endorsed by the Human Rights Council, operationalise the Protect, Respect, and Remedy framework: states should protect against human rights abuses; enterprises should respect rights; and victims should have access to remedy. These principles inform analysis where surveillance capabilities intersect with vendor ecosystems, telecommunications markets, and institutional procurement.

United Nations General Assembly Resolution 75/176 (2020) on the right to privacy in the digital age reaffirms that modern communications increase capacities for surveillance, interception, and data collection affecting privacy under the International Covenant on Civil and Political Rights and related instruments. It highlights risks linked to aggregated metadata, stresses procedural safeguards and remedies, and frames artificial intelligence and data-intensive technologies as requiring adequate safeguards. This resolution is used as a UN-level articulation of digital-age privacy expectations pertinent to proportionate surveillance governance.

NIST Cybersecurity Framework (CSF) 2.0 (2024): The NIST CSF 2.0 represents a global shift from protecting "critical infrastructure" to providing a universal taxonomy for all organizations. This study analysed the six core functions: Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024). The analysis found that while NIST 2.0 is exceptionally strong in defining organizational "outcomes," it remains a management-level tool that assumes a certain level of institutional maturity and resource availability. In the Uganda, where many mobile users operate in the informal economy, the NIST model requires "socio-technical translation" to account for low baseline digital literacy and the unique stealth of mercenary spyware.

ISO/IEC 27001:2022 (ISMS): ISO 27001:2022 was reviewed as the international gold standard for Information Security Management Systems (ISMS). This study examined its focus on a risk-based approach and the "Leadership" (Clause 5) and "Support" (Clause 7) requirements. ISO 27001 provided the structural "rigor" for the organizational and policy layers of this study's framework (ISO/IEC, 2022). However, the review established that ISO 27001 is a "compliance-heavy" standard designed for formal enterprises. It does not provide actionable guidance for individual citizens or civil society groups facing targeted, private and state-grade spyware surveillance in a socially, economically and politically sensitive environment.

While NIST CSF 2.0 and ISO 27001 provide excellent foundations for general corporate cybersecurity, they are insufficient for the specific challenge of spyware-enabled surveillance in Uganda for three reasons. First, Contextual Specificity: existing standards are 'context-blind' and do not account for the localized socio-political risks found in Uganda's electoral or conservation domains. Second, Socio-Technical Depth: NIST and ISO focus primarily on management and technical controls, whereas this study's framework addresses the 'Social' layer, specifically user suspicion and gendered vulnerabilities as an equal component of security. Third, Threat

Specialization: general frameworks treat all malware equally, but the proposed framework is surgically tuned for the unique exfiltration and "invisible control" characteristics of high-capability spyware

4.4.12 Synthesis

The reviewed materials converge on three points relevant to this study. First, Uganda's legal order recognises privacy and data protection as actionable policy concerns (Constitution; DPPA). Second, lawful interception and investigation are addressed through multiple statutory pathways (notably RICA; Anti-Terrorism Act Part VII; sector offences and emergency-related provisions in the Uganda Communications Act, 2013), which increases the importance of clear safeguards, oversight, and remedy. Third, national policy and sector growth emphasise digital reliance, raising the practical impact of intrusion and surveillance. These findings justify the study's integrated socio-technical mitigation framework: user empowerment, organisational governance, technical infrastructure, alignment of legal and policy safeguards, and public accountability, developed in the chapters that follow.

4.6.2 Framework Design Rationale and Theoretical Grounding

The Socio-Technical Framework for the Mitigation of Spyware-Enabled Digital Surveillance Risks in Uganda was developed not as a purely technical solution, but as a multi-layered response to the complex risk environment identified in this study. The rationale for its design is anchored in three foundational pillars.

1. Socio-Technical Systems (STS) Theory: As established in Chapter Two, STS theory posits that technological outcomes emerge from the interaction between machines and social structures (Trist and Bamforth, 1951). This study found that the risk of spyware in Uganda is exacerbated by a "capability gap" where high levels of user concern (82.5%) do not translate into technical protection due to limited literacy and institutional support. Consequently, the framework is designed to align technical safeguards (Layer 3) with social empowerment (Layer 1) and organizational governance (Layer 2), ensuring that mitigation is systemic rather than isolated.
2. Contextual Integrity (CI): Drawing on Nissenbaum's CI framework, the study conceptualizes spyware as a violation of "contextual norms" where information intended for private messaging or financial transactions is inappropriately diverted to third-party

actors (Nissenbaum, 2004). This informed the study's decision to include specific protections against "Inappropriate Information Flows" in Layer 4 (Legal & Policy) and Layer 5 (Civil Society), specifically targeting the aggressive data-scraping practices of digital lenders and the "stalkerware" used in interpersonal contexts.

3. Privacy by Design (PbD): The framework operationalizes PbD principles (Cavoukian, 2012). by advocating for a shift from "reactive user burden" to "proactive systemic resilience." Rather than placing the entire responsibility for safety on the individual user, a trend criticized by RPDT01 as a "neoliberal security failure", the framework demands that privacy be embedded at the "Point-of-Sale" (Layer 1) and through "State-Provisioned Tooling" (Layer 3).

Ultimately, the framework serves as an "Ecological Model" of resilience. It recognizes that in a mobile-first economy characterized by "fragile trust," mitigation must occur simultaneously across individual, organizational, and state levels. This architecture was rigorously validated through a Modified Delphi process with 8 experts, ensuring that the resulting interventions are both theoretically sound and practically relevant to the Ugandan digital ecosystem.

4.6.3 Socio-Technical Framework Structure and Components

The framework has been designed to address specific, high-capability threats posed by commercial spyware and covert surveillance. Moving away from generic cybersecurity heuristics, this validated matrix is divided into Proactive Controls (Prevention) and Reactive Controls (Response) across five interconnected layers.

Architecture of the Framework

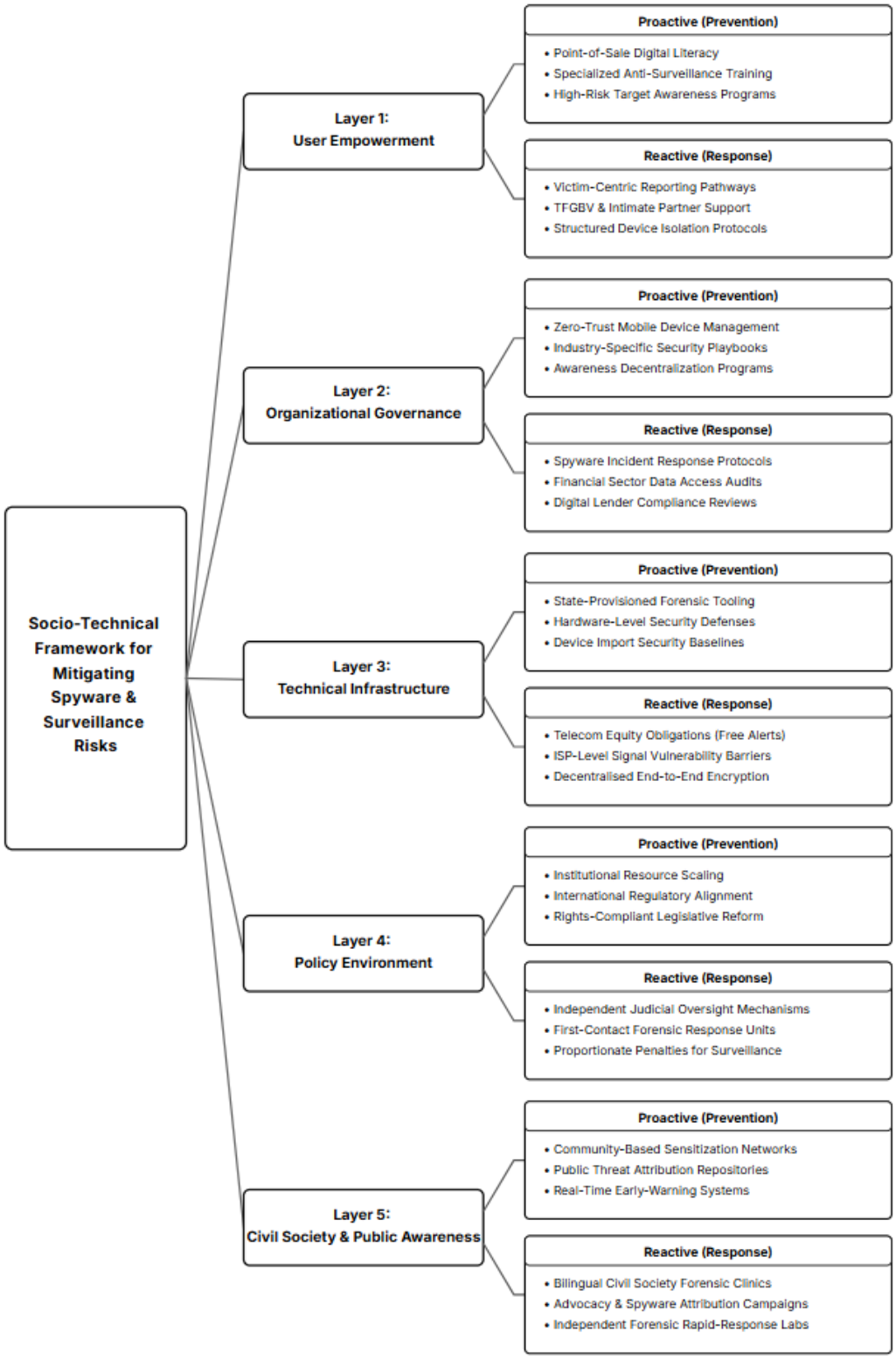

Figure 19: Architecture of the Framework

Table 28: The Framework Mitigation Matrix

Framework Layer	Proactive Controls (Prevention)	Reactive Controls (Response)
1. User Empowerment	**Point-of-Sale Digital Literacy:** Embedding security hygiene training into the device acquisition process. **Specialized Anti-Surveillance Training:** Targeted capacity building for high-risk targets on advanced surveillance vectors. **High-Risk Target Awareness Programs:** Localized outreach for vulnerable demographics.	**Victim-Centric Reporting Pathways:** Structured reporting flows that prioritize device isolation and psychological safety. **TFGBV & Intimate Partner Support:** Specialized support for victims of intimate partner and gendered surveillance. **Structured Device Isolation Protocols:** Technical guidance on air-gapping vs destructive resets.
2. Organizational Governance	**Zero-Trust Mobile Device Management:** Enforcing strict separation and auditing of corporate data on personal devices. **Industry-Specific Security Playbooks:** Developing formal incident response protocols tailored to institutional threat profiles. **Awareness Decentralization Programs:** Expanding organizational safety mandates to informal and grassroots economic actors.	**Spyware Incident Response Protocols:** Formal procedures for identifying and containing commercial monitoring tools. **Financial Sector Data Access Audits:** Rigorous auditing of digital lending and fintech platforms to prevent unauthorized data access. **Digital Lender Compliance Reviews:** Mandatory oversight of lending apps' data-scraping practices.

3. Technical Infrastructure	**State-Provisioned Forensic Tooling:** Government procurement and distribution of open-source detection tools for public use. **Hardware-Level Security Defenses:** Adoption of physical kill switches, Faraday protocols, and secure hardware baselines. **Device Import Security Baselines:** Mandating anti-surveillance standards for all imported mobile hardware.	**Telecom Equity Obligations (Free Alerts):** Mandating free-of-charge security alerts for subscribers. **ISP-Level Signal Vulnerability Barriers:** Technical protections against SS7 and signaling-layer exploits. **Decentralised End-to-End Encryption:** Promoting the use of peer-to-peer encrypted messaging as the default for sensitive communication.
4. Legal & Policy Environment	**Institutional Resource Scaling:** Ensuring digital protection offices have the staffing, funding, and technical capacity required for enforcement. **International Regulatory Alignment:** Forging partnerships to address the transnational supply chains of mercenary spyware. **Rights-Compliant Legislative Reform:** Drafting laws that prioritize individual digital rights over state monitoring.	**Independent Judicial Oversight Mechanisms:** Implementing mandatory, non-negotiable warrant requirements for all forms of digital interception. **First-Contact Forensic Response Units:** Deploying specialized IT units at local stations for immediate victim support. **Proportionate Penalties for Surveillance:** Establishing severe consequences for unauthorized state and commercial surveillance.

5. Civil Society & Public Awareness	**Community-Based Sensitization Networks:** Partnering with religious, market, and community groups to localize threat information. **Public Threat Attribution Repositories:** Supporting independent platforms that track and share real-time Indicators of Compromise (IoCs). **Real-Time Early-Warning Systems:** Automated alerts for emerging surveillance patterns.	**Bilingual Civil Society Forensic Clinics:** Establishing trusted, rapid-response centers parallel to the state apparatus. **Advocacy & Spyware Attribution Campaigns:** Shifting focus toward naming and shaming the commercial entities behind surveillance tools. **Independent Forensic Rapid-Response Labs:** Providing expert payload extraction and verification services for citizens.

The proposed framework has been operationalized through a functional prototype (https://ainedembe-denis.github.io/uganda-surveillance-watch/). In its current state, the dashboard demonstrates the "National Early-Warning" five-layered concept by providing users with an evidence-based attribution map. It shifts surveillance awareness from "generic" threats to "specific" actors by identifying vendors with documented links to the Ugandan context. While the current prototype is a technical demonstration in English, it provides the structural blueprint for a future, more accessible iteration that can support real-time threat intelligence and local language integration.

Elaborating the Layers

Layer 1: User Empowerment (Addressing Interpersonal & Point-of-Sale Risks). The foundation of the framework shifts away from generic digital safety toward hyper-specific anti-surveillance literacy. Proactively, this layer mandates Point-of-Sale Digital Onboarding, requiring device retailers to configure baseline security at purchase. This approach builds on established regional precedents, including the GSMA's Connected Women Commitment Initiative, which has demonstrated that retail-point literacy distribution is a cost-effective and scalable model for reaching underserved users in Sub-Saharan Africa (GSMA, 2025). It emphasizes specialized

training for both the general public and high-risk targets on the realities of spyware risks and how to protect themselves. Reactively, it establishes Clear Reporting Mechanisms. This includes a structured interaction flow where suspicion immediately triggers safe device isolation (air-gapping) rather than destructive factory resets, followed by escalation to a trusted helpline and professional forensic experts. This structured flow provides specific support pathways for victims of Technology-Facilitated Gender-Based Violence (TFGBV) and Intimate Partner Surveillance.

Layer 2: Organizational Governance (Addressing Remote Work & Digital Lenders). To address the expanded attack surface caused by remote work, proactive governance must implement strict, high-target device auditing protocols. This includes enforcing Zero-Trust Mobile Device Management (MDM) to ensure compromised personal devices cannot laterally infect corporate networks. Reactively, institutions must discard generic IT policies in favour of formal Commercial Spyware Incident Response Playbooks. Crucially, this layer also demands strict accountability audits for Digital Lenders. The Uganda Microfinance Regulatory Authority (UMRA) Digital Lending Guidelines (2024) already prohibit licensed providers from accessing contact lists or private data beyond the scope of loan assessment; however, the framework advocates for mandatory auditing to include unlicensed mobile lending applications that continue to engage in predatory data scraping and surveillance-based debt collection (Uganda Microfinance Regulatory Authority 2024).

Layer 3: Technical Infrastructure (Addressing Ecosystem & State Provisioning). Traditional antivirus software is functionally obsolete against mercenary spyware. Proactively, this layer demands State-Provisioned Protective Tooling: the government should procure and distribute open-source forensic detection tools, with the Amnesty International Security Lab's Mobile Verification Toolkit (MVT) adopted as the minimum institutional baseline (Amnesty International Security Lab, 2021). This is supported by Hardware-Level Security Defenses and Device Import Security Baselines. Establishing an MVT-capable independent forensics laboratory in Uganda represents the credible first step toward domestic spyware attribution. This layer also advocates for AI-powered transaction monitoring, device fingerprinting, and behaviour analytics within institutional networks to detect anomalous data exfiltration in real time. Reactively, technical infrastructure must focus on Telecom Equity Obligations (Free Alerts), ISP-Level Signal Vulnerability Barriers, and Decentralised End-to-End Encryption as the default for sensitive communication. Critically, these safeguards must include ISP-level barriers against Signalling

System 7 (SS7) vulnerabilities, and a mandatory obligation that security alert notifications be provided to subscribers free of charge.

Layer 4: Legal & Policy Environment (Addressing Capacity & Enforcement). The qualitative analysis criticized the current policy environment as "generic" while also others argued with particular analytical precision that Uganda's binding digital rights problem is not the absence of legislation but the effectiveness and independence of enforcement.

Proactively, this layer demands Institutional Capacity Building (Resource Scaling), International Regulatory Alignment, and Rights-Compliant Legislative Reform. A comparative benchmark is instructive here; Kenya's Office of the Data Protection Commissioner (ODPC) has invested significantly in institutional capacity and complaint management since its 2025-2029 Strategic Plan (Kenya Office of the Data Protection Commissioner 2025), providing a regional model for resourcing. Reactively, this layer addresses the response gap through Independent Judicial Oversight Mechanisms, First-Contact Forensic Response Units deployed directly to local police stations, and Proportionate Penalties for Surveillance. Amending RICA (2010) to mandate strict judicial oversight of all lawful interception, combined with severe DPPA financial penalties for telecom and operator breaches, completes the enforcement architecture.

Layer 5: Civil Society & Public Awareness (Addressing Trust & Grassroots Reach). Despite vulnerability, only 17.2% of respondents sought help from civil society. Proactively, this layer establishes Community-Based Sensitization Networks, Public Threat Attribution Repositories, and Real-Time Early-Warning Systems to share information from global repositories (SurveillanceWatch.io, 2025). Reactively, the framework proposes the creation of Bilingual Civil Society Forensic Clinics and Independent Forensic Rapid-Response Labs. Operating as a bilingual (English/Local languages) clinic, this lab provides trusted support parallel to the state apparatus, enabling deep-level payload extraction using open-source tools like MVT (Amnesty International Security Lab, 2021) and aggressive Advocacy & Spyware Attribution Campaigns against spyware operators.

4.6.4 Framework Validation Process and Results

The framework was subjected to a structured expert validation process prior to finalization. Validation was conducted to assess the framework's content validity, practical relevance,

contextual appropriateness, and completeness, and to ensure that its components were grounded in both the empirical evidence and the lived realities of stakeholders in Uganda's digital ecosystem.

The validation process followed a modified Delphi methodology (Linstone and Turoff, 1975), involving two rounds of expert consultation. In the first round, eight purposively selected experts comprising two ICT security practitioners, one legal and policy specialist with experience in digital rights, two representatives from civil society digital advocacy organizations, and two academic researchers were provided with a draft framework document and asked to evaluate each layer using a structured questionnaire.

Table 27: Expert Validation Results by Framework Layer

Framework Layer	Relevance (/5)	Clarity (/5)	Feasibility (/5)	Completeness (/5)	Mean Score
1. User Empowerment	4.8	4.5	4.2	4.6	4.53
2. Organizational Governance	4.7	4.4	3.9	4.5	4.38
3. Technical Infrastructure	4.9	4.6	4.0	4.7	4.55
4. Legal and Policy Environment	4.6	4.3	3.7	4.4	4.25
5. Civil Society & Public Awareness	4.5	4.4	4.1	4.3	4.33
Overall Framework	4.70	4.44	3.98	4.50	4.41

Source: Primary Data, 2026

The overall mean validation score across all framework layers and criteria was 4.41 out of 5.0, reflecting strong expert endorsement of the proposed architecture. The Technical Infrastructure layer received the highest mean score (4.55), which experts attributed to their confidence that operationally feasible detection and hardware-level defenses exist to address the identified risks. The User Empowerment layer also scored highly (4.53), underscoring the critical importance of digital literacy and awareness-building in the mitigation strategy. The Legal and Policy Environment layer received the lowest feasibility rating (3.7), which experts attributed to the political sensitivity of legislative reform in a context where the state itself is a documented

surveillance actor. The framework acknowledges this constraint, positioning legal reform as a longer-term strategic objective requiring multi-stakeholder coordination rather than immediate operational deployment.

Following the first round of expert consultation, the feedback was systematically collated and used to refine the framework. Key revisions included: first, the incorporation of an explicit gender dimension into Layer 1, addressing the disproportionate surveillance risks faced by women journalists and activists; second, the formal designation of mobile network operators as accountability stakeholders within Layer 2; third, the clarification of roles, responsibilities, and timelines within each layer; and fourth, the integration of monitoring and evaluation indicators to enable assessment of implementation progress. In the second validation round, experts assigned positive ratings to the revised framework, with all layers scoring above 4.0 on average and no major structural modifications recommended. The validation process thus confirmed the framework's internal consistency and contextual relevance, providing a rigorous, practitioner-endorsed basis for its adoption within Uganda's digital security governance landscape.

CHAPTER FIVE: DISCUSSION, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter synthesizes the empirical evidence gathered through a mixed-methods investigation into spyware-enabled surveillance, utilizing Uganda's mobile digital ecosystem as a case study. The discussion traverses the four primary research objectives, interpreting the quantitative trends of 320 respondents alongside the nuanced, qualitative lived experiences of ten key informants and a rigorous document review. Guided by Socio-Technical Systems (STS) theory, Contextual Integrity, and Privacy by Design, this chapter defines how technological affordances, user practices, and regulatory gaps converge to shape a unique landscape of digital risk. Finally, it validates the proposed framework as a necessary intervention for restoring trust and agency in digital environments.

5.2 Discussion of Findings

5.2.1 Spyware-Enabled Surveillance Practices and Actors: Insights from the Case Study

The findings establish that spyware-enabled surveillance, as observed in the case of Uganda, is not a peripheral threat but a structural feature of the mobile ecosystem studied. The quantitative data reveals a profound convergence of life functions on single devices, with 92.2% of users relying on mobile devices for core communications and 81.3% for financial services. This "device hyper-dependence" transforms the mobile phone and other devices into what RPDT03 described as a "vulnerable container" of a user's entire social and financial identity.

The suspicion of unauthorized monitoring (71.6% combined concern) indicates a pervasive "surveillance anxiety" that mirrors global trends but is intensified by the Ugandan context. While 35.4% of users identified anomalous device behavior as a primary indicator, symptoms often linked to mercenary tools, the qualitative interviews revealed a more intimate threat landscape. Participants highlighted a "dual-front" of surveillance that is; high-level state monitoring for national security targets and a burgeoning market for "stalkerware" used by partners, employers, or family members. This aligns with the findings of Chatterjee et al. (2018), suggesting that spyware has been commodified into a tool for interpersonal coercion, disproportionately affecting those in asymmetric power relationships.

5.2.2 Impacts on Privacy, Trust, Power, and Control

The study reveals that surveillance has effectively neutralized the "Privacy Calculus", (Dienlin, 2023) for many Ugandan users. With a mean privacy concern score of 4.37out of 5, the anxiety is near-universal. However, a significant "Privacy Paradox" exists (Gerber et al., 2018). while 68.1% of users reported maximum concern, only 32.2% utilized advanced encryption or VPNs. The document review and interviews suggest this is not a result of apathy, but of a "technical efficacy gap." Users feel that against state-grade or even sophisticated commercial spyware, individual defensive measures are futile.

Trust in digital platforms has reached a critical low (mean score 2.69/5). From a socio-technical perspective, this erosion of trust is not merely a psychological state but a behavioral driver. As (Lyon, 2018) argues, pervasive surveillance triggers "anticipatory compliance," where users self-censor or withdraw from digital participation to avoid perceived risks. In Uganda, this is worsened by a "Power Asymmetry" where the surveilling actor (whether a state agency or a commercial platform) holds the technical and legal upper hand, leaving the user feeling alienated and monitored within their most intimate digital spheres.

5.2.3 Factors Shaping Exposure: Practices, Policies, and Organizations

The analysis of mediating factors identifies a systemic "responsibility shift." Currently, 39.4% of respondents believe they are solely responsible for their own digital protection. This reflects a global trend of "responsibilities" (Lupton, 2016), where the burden of security is shifted from powerful institutions to the individual user.

However, the study finds that individual caution is insufficient. The document review of the Data Protection and Privacy Act (2019) and RICA (2010) identify a critical Implementation Gap. While 62.2% of users were unaware of their legal protections, experts interviewed noted that the very institutions meant to enforce these laws often lack the forensic capacity or the political will to challenge surveillance abuses. Furthermore, the 54.1% gap in digital safety training highlights a structural failure in digital onboarding. For the average Ugandan user, digital resilience is currently a matter of "luck" or informal social support (IT friends/family) rather than a state-guaranteed right.

5.2.4 The Framework: A Socio-Technical Response

The overwhelming support for a structured mitigation framework (mean utility score 4.14/5) underscores the inadequacy of current ad-hoc security measures. The framework addresses the "Detection Gap" by shifting from reactive individual fixes to proactive, multi-layered systemic accountability

Expert validation (mean score 4.41/5) confirmed that while the technical layers of the framework are robust, the "Legal and Policy" layer (score 3.7) remains the most challenging to implement due to the political sensitivity of surveillance governance. By integrating Privacy by Design principles, the framework advocates for "State-Provisioned Tooling"; moving the burden of detection to the infrastructure layer, thereby humanizing the response by protecting the most vulnerable users who lack technical expertise.

5.3 Conclusions

The study concludes that spyware-enabled surveillance, as observed in the case of Uganda, represents a fundamental breach of "Contextual Integrity." It is a socio-technical phenomenon where the convergence of mobile-first economies and sophisticated monitoring tools has created a landscape of persistent vulnerability.

The primary conclusion is that digital resilience cannot be achieved through individual user behavior alone. It is a systemic outcome that requires the alignment of technical infrastructure, organizational accountability, and legislative reform. The "surveillance anxiety" documented across all age groups indicates that unless trust is restored through the implementation of the mitigation framework, the democratic and economic potential of digital transformation in similar contexts will remain compromised by self-censorship and fear.

5.4 Recommendations

The following recommendations are proposed to enhance digital resilience and mitigate the risks of spyware-enabled surveillance, based on insights from the Ugandan mobile ecosystem.

5.4.1 For Individual Users

It is recommended that individual users adopt a "Zero-Trust" security posture toward mobile applications. This involves utilizing decentralized end-to-end encrypted (E2EE) platforms and

hardware-level protections where feasible. Users are further advised to adhere to the "Isolation First" protocol; in the event of suspected device compromise, the device should be air-gapped to preserve forensic evidence for attribution rather than being subjected to a factory reset.

5.4.2 For Organizations and Employers

Organizations are encouraged to transition beyond generic IT policies and implement specific "Spyware Incident Response Playbooks." These should prioritize the provision of secure, audited devices for high-risk communications and mandate regular technical audits of mobile financial platforms to prevent unauthorized data scraping and exfiltration.

5.4.3 For Government and Regulatory Bodies

The state should transition from a surveillance-centric digital policy to a "protection-first" framework. It is recommended that the government provides dedicated funding for independent forensic units at local police stations and Innovation Labs. Furthermore, the Data Protection and Privacy Office must strictly enforce the Data Protection and Privacy Act (2019), particularly the Section 40 penalty provisions, by imposing severe financial sanctions for unauthorized data access and surveillance breaches, regardless of the actor involved.

5.4.4 For Civil Society

Civil society organizations should address the existing "Trust Gap" by establishing independent, bilingual (English and local languages) digital forensic clinics. These clinics are envisioned as safe havens for victims of institutional monitoring and technology-facilitated harm. It is further recommended that civil society coordinates a National Early-Warning System to share real-time threat intelligence and Indicators of Compromise (IoCs), shifting toward a strategy of evidence-based public attribution for commercial spyware operators.

5.4.5 Gender-Responsive Recommendations

To address the intersectional risks identified in this study, digital safety initiatives must prioritize gender-responsive interventions. This includes the development of specialized forensic support pathways for women human rights defenders and victims of intimate partner surveillance. Public awareness campaigns should be tailored to address the unique ways in which surveillance is utilized as a tool of coercive control in interpersonal and domestic contexts.

5.5 Limitations of the Study

The study acknowledges that the sample, consisting largely of digitally engaged individuals, may present an “optimistic” view of digital literacy. The 66.9% male skew in the sample also limits a full intersectional analysis of how gendered power relations shape surveillance. Future research should employ longitudinal forensic device analysis to bridge the gap between “perceived” and “actual” infection rates.

Finally, the digital artefact developed for this study - the Uganda Surveillance Watch dashboard is a proof-of-concept with identified UI and functional limitations. For example, its current reliance on a central interactive globe can impact user navigation on certain devices, and its data remains limited to existing API-integrated sources. These technical constraints highlight the need for further UX refinement and the development of more accessible, mobile-optimized interfaces for future surveillance-awareness tools in the Ugandan context.

5.6 Avenues for Future Research

While this study establishes a socio-technical foundation for spyware mitigation in Uganda, several avenues for future inquiry remain.

First, longitudinal forensic studies are needed to track how mercenary spyware evolves specifically within the East African mobile infrastructure. Second, further research should explore the gendered dimensions of surveillance using a larger, more representative sample to understand how power asymmetries affect digital safety in domestic contexts.

Finally, future work could involve the technical implementation and testing of the Mitigation framework within a live organizational environment to measure its real-world efficacy in reducing infection rates.

REFERENCES

AMNESTY INTERNATIONAL 2023. *Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products*.

AMNESTY INTERNATIONAL SECURITY LAB 2021. Mobile Verification Toolkit (MVT).

ANDREJEVIC, M. 2014. Big data, big questions| the big data divide. *International Journal of Communication,* 8**,** 17.

ANGLANO, C. 2025. A Review of Mobile Surveillanceware: Capabilities, Countermeasures, and Research Challenges. *Electronics,* 14**,** 2763.

ATOMICMAIL. 2025. *Is WhatsApp Safe? The Truth About Your Privacy in 2025* [Online]. AtomicMail Blog. Available: https://atomicmail.io/blog/is-whatsapp-safe-the-truth-about-your-privacy [Accessed 20 Nov 2025].

AZUNGAH, T. 2018. Qualitative research: deductive and inductive approaches to data analysis. *Qualitative research journal,* 18**,** 383-400.

BARAN, G. 2025. *Unremovable Spyware on Samsung Devices* [Online]. Cybersecurity News. Available: https://cybersecuritynews.com/spyware-on-samsung-devices/ [Accessed 12 Jan 2026].

BARTH, S. & DE JONG, M. D. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics,* 34**,** 1038-1058.

BROWN, L. S., J.; WABWIRE, A.; DU TOIT, L.; TJIRONGO, J.; MACAULEY, D 2024. Understanding Technology Facilitated Gender-based Violence (TFGBV) in Uganda. *Journal of Psychology and Neuroscience,* 6**,** 1–10.

BUDAK, J., RAJH, E., SLIJEPČEVIĆ, S. & ŠKRINJARIĆ, B. 2020. Theoretical concepts of consumer resilience to online privacy violation. *Radni materijali EIZ-a***,** 7-43.

CAVOUKIAN, A. 2012. Privacy by design [leading edge]. *IEEE Technology and Society Magazine,* 31**,** 18-19.

CHATTERJEE, R., DOERFLER, P., ORGAD, H., HAVRON, S., PALMER, J., FREED, D., LEVY, K., DELL, N., MCCOY, D. & RISTENPART, T. The spyware used in intimate partner violence. 2018 IEEE Symposium on Security and Privacy (SP), 2018. IEEE, 441-458.

CHISALA-TEMPELHOFF, S. & KIRYA, M. T. 2024. Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda. *Palgrave Communications,* 2**,** 1-10.

DAHL, R. A. 1957. The concept of power. *Behavioral science,* 2**,** 201-215.

DANNELS, S. A. 2018. Research design. *The reviewer's guide to quantitative methods in the social sciences.* Routledge.

DEIBERT, R. 2022. Protecting society from surveillance spyware. *Issues in Science and Technology,* 38**,** 15-17.

DIENLIN, T. 2023. Privacy calculus: Theory, studies, and new perspectives. *The Routledge handbook of privacy and social media.* Routledge.

EISEND, M. 2019. Explaining digital piracy: A meta-analysis. *Information Systems Research,* 30**,** 636-664.

EMERY, F. E. & TRIST, E. L. 1960. Socio-technical systems. *Management science, models and techniques,* 2**,** 83-97.

FELDSTEIN, S. 2019. *The global expansion of AI surveillance*, Carnegie Endowment for International Peace Washington, DC.

GERBER, N., GERBER, P. & VOLKAMER, M. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security,* 77**,** 226-261.
GHANAD, A. 2023. An overview of quantitative research methods. *International journal of multidisciplinary research and analysis,* 6**,** 3794-3803.
GSMA 2025. The Mobile Gender Gap Report 2025.
HARKIN, D., MOLNAR, A. & VOWLES, E. 2020. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, media, culture,* 16**,** 33-60.
HENRY, N. & POWELL, A. 2016. Sexual violence in the digital age: The scope and limits of criminal law. *Social & legal studies,* 25**,** 397-418.
HOLDEN, K. & HARSH, M. 2024. On pipelines, readiness and annotative labour: Political geographies of AI and data infrastructures in Africa. *Political Geography*.
IBRAHIM, S., MARCELLA, R. & MACLENNAN, A. 2025. Investigating intersectionality and its influence on information behaviours of women and immigrant digital entrepreneurs in Nigeria: Overcoming social inequalities through information strategies. *Journal of Librarianship and Information Science***,** 09610006251329031.
IMAM, M., MANIMEKALAI, N. & SUBA, S. 2025. From Data to Discrimination: Gender, Privacy, and the Politics of Digital Surveillance. *Synergy: International Journal of Multidisciplinary Studies,* 2**,** 52-64.
INTERNATIONAL TELECOMMUNICATION UNION. 2025. *Measuring digital development: Facts and Figures 2025* [Online]. International Telecommunication Union. Available: https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2025-3-pdf-e.pdf [Accessed 18 May 2026].
ISO/IEC 2022. 27001:2022 Information Security Management. International Organization for Standardization.
KATIBAH, L. 2023. The Politics of Pegasus Spyware: Examining the Impact of Surveillance on Journalism.
KATUSIIME, I. 2025. *Analysis: How Uganda's Digital Number Plates Became Spy Tools* [Online]. Pulitzer Center. Available: https://pulitzercenter.org/stories/analysis-how-ugandas-digital-number-plates-became-spy-tools [Accessed 15 Mar 2026].
KEEN, C. 2022. Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy. *New Media & Society,* 24**,** 50-69.
KENYA OFFICE OF THE DATA PROTECTION COMMISSIONER 2025. Strategic Plan 2025–2029. Nairobi: ODPC.
KHANDAY, S. A. & KHANAM, D. 2019. The research design. *Journal of critical reviews,* 6**,** 367-376.
KNIJNENBURG, B. P., PAGE, X., WISNIEWSKI, P., LIPFORD, H. R., PROFERES, N. & ROMANO, J. 2022. *Modern socio-technical perspectives on privacy*, Springer.
LEAVY, P. 2022. *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*, Guilford publications.
LEESE, M. 2021. Security as socio-technical practice: Predictive policing and (non-) automation. *Swiss political science review,* 27**,** 150-157.
LINSTONE, H. A. & TUROFF, M. 1975. *The delphi method*, Addison-Wesley Reading, MA.

LIU, E., RAO, S., HAVRON, S., HO, G., SAVAGE, S., VOELKER, G. M. & MCCOY, D. 2023. No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*.

LU, B. & YI, X. 2023. Institutional trust and repurchase intention in the sharing economy: The moderating roles of information privacy concerns and security concerns. *Journal of Retailing and Consumer Services,* 73**,** 103327.

LUBOWA, H. 2025. *Traitor or Companion? The Digital Spy in Your Palm: A Ugandan Perspective* [Online]. Oxfam Uganda. Available: https://uganda.oxfam.org/latest/blogs/traitor-or-companion-digital-spy-your-palm-ugandan-perspective [Accessed 18 Feb 2026].

LUPTON, D. 2016. The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society,* 45**,** 101-122.

LYON, D. 2018. *The culture of surveillance: Watching as a way of life*, John Wiley & Sons.

MADDEN, M. & RAINIE, L. 2015. Americans' attitudes about privacy, security and surveillance.

MADOI, R. 2026. *Big Brother is Watching: Surveillance in Uganda* [Online]. Daily Monitor. Available: https://www.monitor.co.ug/uganda/news/national/big-brother-is-watching-surveillance-in-uganda-5366416#story [Accessed 04 Mar 2026].

MATZNER, T. 2016. Beyond data as representation: The performativity of Big Data in surveillance. *Surveillance & society,* 14**,** 197-210.

MIREMBE, D. P., LUBEGA, J., KIBUKAMUSOKE, M. & NAMBOGO, F. 2022. Survey on the State of Digital Human Rights Management and Internet Use in Uganda. *Archives of Business Research,* 10.

MUSOKE, R. 2025. *Targeted, Tracked, and Silenced* [Online]. The Independent (Uganda). Available: https://www.independent.co.ug/targeted-tracked-and-silenced/ [Accessed 13 Dec 2025].

MYERS, M. D. & AVISON, D. 2002. *Qualitative research in information systems: a reader*, Sage.

NASSUUNA, N. & KIMBUGWE, H. N. 2025. *Uganda's Move to Procure Social Media Tracking Tool* [Online]. Defenders Protection Initiative. Available: https://www.defendersprotection.org/wp-content/uploads/2025/04/Ugandas-Move-to-Procure-Social-Media-Tracking-Tool-.pdf [Accessed 19 Feb 2026].

NGAMITA, R. 2025. *Surveillance or Security? Uganda's Digital License Plates* [Online]. Thraets. Available: https://thraets.org/surveillance-or-security/ [Accessed 25 Mar 2026].

NISSENBAUM, H. 2004. Privacy as contextual integrity. *Wash. L. Rev.,* 79**,** 119.

NIST 2024. Cybersecurity Framework (CSF) 2.0.

OHCHR 2022. The right to privacy in the digital age. Geneva: United Nations.

OLTMANN, S. Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. Forum: Qualitative social research, 2016. 1-16.

ORLIKOWSKI, W. J. & BAROUDI, J. J. 1991. Studying information technology in organizations: Research approaches and assumptions. *Information systems research,* 2**,** 1-28.

OUMA, S. 2023. Ascendant recentralisation: the politics of urban governance and institutional configurations in Nairobi. *Journal of Eastern African Studies,* 17**,** 363-383.

PIERAZZI, F., MEZZOUR, G., HAN, Q., COLAJANNI, M. & SUBRAHMANIAN, V. 2020. A data-driven characterization of modern Android spyware. *ACM Transactions on Management Information Systems (TMIS),* 11**,** 1-38.

PLONSKY, L. 2017. Quantitative research methods. *The Routledge handbook of instructed second language acquisition.* Routledge.

PRIVACY INTERNATIONAL. 2015. *For God and My President: State Surveillance in Uganda* [Online]. Privacy International. Available: https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf [Accessed 14 Aug 2025].
QABALIN, M. K., NASER, M. & ALKASASSBEH, M. 2022. Android spyware detection using machine learning: a novel dataset. *sensors,* 22**,** 5765.
ROBERTS, T. & MARE, A. 2025. *Digital surveillance in Africa: Power, agency, and rights*, Bloomsbury Academic.
ROGERS, R. W. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology,* 91**,** 93-114.
RYAN, C. M. & TYNEN, S. 2020. Fieldwork under surveillance: Rethinking relations of trust, vulnerability, and state power. *Geographical Review,* 110**,** 38-51.
RYAN, G. 2018. Introduction to positivism, interpretivism and critical theory. *Nurse researcher,* 25**,** 41-49.
SAUNDERS, M. N., LEWIS, P. & THORNHILL, A. 2019. Research methods for business students (Eighth). *Harlow: Pearson education limited*.
SCHWANDT, T. A. 1994. Constructivist, interpretivist approaches to human inquiry.
SHEPPARD, V. 2024. *Research methods for the social sciences: An introduction*, BCcampus.
SITTIG, D. F. & SINGH, H. 2016. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics,* 7**,** 624-632.
SPENS, B. 2024. The spyware industrial complex.
STEFANI, E., COSTA, I., GASPAR, M. A., GOES, R. D. S., MONTEIRO, R. C., PETRILI, B. R. & PEREIRA, A. D. P. 2025. Information Security Risk Framework for Digital Transformation Technologies. *Systems,* 13**,** 37.
STEVENS, A., FUSSEY, P., MURRAY, D., HOVE, K. & SAKI, O. 2023. 'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe. *Big Data & Society,* 10**,** 20539517231158631.
SUN, H., YUAN, C., QIAN, Q., HE, S. & LUO, Q. 2022. Digital resilience among individuals in school education settings: a concept analysis based on a scoping review. *Frontiers in psychiatry,* 13**,** 858515.
SURVEILLANCEWATCH.IO 2025. *Global Spyware Attribution Map*.
TABASUM, T., IRAM, S., ALI, S., AKHTAR, M. & HUSSAIN, M. 2025. Digital Surveillance and Privacy Concerns the Changing Dynamics of Trust in Modern Societies: A Mediation Moderation Model. *ACADEMIA International Journal for Social Sciences,* 4**,** 747-759.
TEKELI, E. S. 2021. Digital Surveillance and Ethics as a New Risk Factor Within the Context of Regulations on the Internet Law. *İletişim Kuram ve Araştırma Dergisi,* 2021**,** 65-78.
TRIST, E. L. & BAMFORTH, K. W. 1951. Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. *Human relations,* 4**,** 3-38.
UGANDA COMMUNICATIONS COMMISSION 2023. *Annual Communications Sector Report 2023* [Online]. UCC. Available: https://www.ucc.co.ug/wp-content/uploads/2023/Sector-Report.pdf [Accessed 14 Aug 2025].
UGANDA COMMUNICATIONS COMMISSION 2024. *Annual Communications Sector Report 2024* [Online]. UCC. Available: https://www.ucc.co.ug/wp-content/uploads/2024/Sector-Report.pdf [Accessed 14 Aug 2025].

UGANDA COMMUNICATIONS COMMISSION. 2026. *Uganda Engages in Global Telecom Governance at ITU Council 2026* [Online]. Uganda Communications Commission. Available: https://www.ucc.co.ug/uganda-engages-in-global-telecom-governance-at-itu-council-2026/ [Accessed 18 May 2025].
UGANDA MICROFINANCE REGULATORY AUTHORITY 2024. Digital Lending Guidelines, 2024. Kampala: UMRA.
UGANDA MINISTRY OF ICT 2023. National Cybersecurity Strategy 2023 – 2028. Kampala: Government of Uganda.
UNWANTED WITNESS. 2025. *Surveillance/Spyware: An Impediment to Civil Society* [Online]. Unwanted Witness. Available: https://www.unwantedwitness.org/wp-content/uploads/2025/03/Surveillance-Spyware-Report.pdf [Accessed 16 Aug 2025].
VOLOSEVICI, D. & ISBASOIU, G. D. 2025. Surveillance as a Socio-Technical System: Behavioral Impacts and Self-Regulation in Monitored Environments. *Systems,* 13**,** 614.
WESAKA, A. & KIGONGO, J. 2026. All smiles as court strikes down Computer Misuse Act. *Daily Monitor*, March 18.
WESTIN, A. F. 1967. Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM,* 10**,** 533-537.
WISNIEWSKI, P. J. & PAGE, X. 2022. Privacy theories and frameworks. *Modern socio-technical perspectives on privacy.* Springer.
WOICESHYN, J. & DAELLENBACH, U. 2018. Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers. *Qualitative research in organizations and management: An International Journal,* 13**,** 183-195.
WOMEN OF UGANDA NETWORK 2024. *Impact of Spyware on Civic Space* [Online]. WOUGNET. Available: https://wougnet.org/impact-spyware-civic-space-feminist-organising-uganda/ [Accessed 26 Nov 2025].
ZUBOFF, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs.

APPENDICES

Appendix 1: Questionnaire for General Mobile Device Users

Survey Title

Mobile Device Use and Spyware-Enabled Digital Surveillance in Uganda

Introduction

My name is Ainedembe Denis, a Master's student at Uganda Martyrs University. I am conducting academic research on mobile device use and spyware-enabled digital surveillance in Uganda. The purpose of this study is to understand users' awareness, experiences, and perceptions related to privacy, trust, control, and digital safety when using mobile devices.

You are invited to participate in this short survey. Your honest responses will be very valuable to the study. Participation is completely voluntary, and all responses will remain anonymous and will be used only for academic purposes.

The survey takes approximately **3-5 minutes** to complete. By continuing with the survey, you indicate that you consent to participate.

Thank you for your time and participation.

Definitions of Key Terms

- **Spyware:** Software that secretly monitors a mobile phone, such as reading messages, tracking location, or accessing photos without the user's knowledge.
- **Digital Surveillance:** Monitoring people's digital activities through phones, apps, or online platforms.
- **Privacy:** Your ability to control who can access your personal information and activities on your phone.
- **Trust:** Your confidence that digital services or platforms will protect your data and not misuse it.
- **Power**: Ability of individuals or institutions to impose, access or control others' behaviour and their outcomes.
- **Digital Resilience:** Your ability to recognize digital risks, protect yourself, adapt your behaviour, and recover from digital harm.

SECTION A: BACKGROUND INFORMATION

Q1. What is your age group?

18–24

25–34

35–44

45–54

55 and above

Q2. What is your gender?

- Male

- Female

Q3. Which best describes you? *(Choose one)*

- Journalist / Media worker
- Civil society / Digital rights advocate
- ICT / Technology professional
- Health professional
- Corporate Employer/Employee
- Business owner / Entrepreneur / Business person
- Student
- Other: _____

SECTION B: MOBILE DEVICE USE

Q4. How often do you use your mobile phone/tablet/Laptop to access the internet?

- Several times daily
- Daily
- A few times per week
- Rarely
- Never

Q5. What do you mainly use your device for? *(Select all that apply)*

☐ Calls and messaging

☐ Social media

☐ Mobile money / Online banking

☐ Work or study

☐ News / Information

SECTION C: AWARENESS AND EXPERIENCE

Q6. Before this survey, were you aware that phones and other mobile devices can be secretly monitored using spyware?

- Yes

- No
- Not sure

Q7. Have you ever suspected that your phone or laptop was monitored without your consent?

- Yes
- No
- Not sure

Q8. If yes or unsure, what made you suspicious?

- Unusual device behaviour
- Unauthorized access to messages, calls or accounts
- Information from media or other people
- Not sure

SECTION D: PRIVACY AND RISK PERCEPTION

Q9. How concerned are you about privacy when using your phone?

(1 = Not concerned, 5 = Very concerned)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Q10. Which information concerns you most if accessed without permission? ***(Select all that apply)***

☐ Messages and calls

☐ Location information

☐ Photos and videos

☐ Financial information

☐ Medical information

☐ None

SECTION E: TRUST AND CONTROL

Q11. How much do you trust digital platforms and applications to protect your personal data?

(1 = No trust, 5 = Full trust)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Q12. How much control do you feel you have over your data on your mobile device?

(1 = No control, 5 = Full control)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

SECTION F: BEHAVIOURAL CHANGE

Q13. Have surveillance concerns changed how you use your device?

- o Yes
- o No
- o Not sure

Q14. If yes, what changes have you made? ***(Select all that apply)***

☐ Avoid sensitive conversations

☐ Limit certain apps

☐ Change device security settings

☐ Use alternative tools

☐ No changes

SECTION G: SKILLS AND PREPAREDNESS

Q15. Have you ever received digital safety training?

- o Yes
- o No
- o Not sure

Q16. How confident are you in identifying the signs of and protecting yourself from spyware and digital surveillance?

- o Not confident
- o Slightly confident

- Moderately confident
- Very confident

Q17. Who should play the biggest role in protecting users against threats posed by spyware and digital surveillance? (Choose one)

- Individual users
- Digital platforms
- Employers
- Government regulators
- Civil society
- Shared responsibility

SECTION H: SUPPORT AND MITIGATION

Q18. Are you aware of laws or policies protecting users from digital surveillance?

- Yes
- Somewhat
- No

Q19. If you suspected surveillance, where would you seek help? ***(Select all that apply)***

☐ ICT professional

☐ Civil society organization

☐ Government or legal authority

☐ Friends or colleagues

☐ Not sure

Q20. How useful would clear guidance or a framework be in helping users reduce surveillance risks?

(1 = Not useful, 5 = Very useful)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Appendix 2: Interview Guide for Key Informants

SEMI-STRUCTURED INTERVIEW GUIDE

Introduction

Thank you for agreeing to participate in this study. The purpose of this interview is to understand people's experiences and perceptions of spyware and digital surveillance when using mobile devices (phones, Tablets, Laptops).

I am interested in your understanding, personal experiences, thoughts, on how spyware and digital surveillance affects everyday digital life. There are no right or wrong answers. Your responses will remain confidential and used only for academic purposes.

With your permission, I would like to record this interview to ensure accuracy.

1. From your perspective, how do mobile users interact with digital services in Uganda?
2. How do you understand spyware and digital surveillance risks and what types of surveillance risks are most common?
3. How do you think surveillance affects users' privacy and trust?
4. Who do you think has the most influence over users' digital behaviour through surveillance?
5. How do users usually respond when they suspect monitoring?
6. How effective do you think current policies or institutions are in protecting users against spyware-enabled surveillance risks?
7. If you were advising policymakers, technology companies, or user communities, what changes would you recommend?