

CATHOLIC UNIVERSITY OF ZIMBABWE

FACULTY OF COMMERCE, INNOVATION AND TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY & INNOVATION



Examining the Nexus between Social Media and Personal Data Protection in
Zimbabwe. A Case of NetOne Zimbabwe

BY

MUZENDA BRYN TAWEDZERWA

PG248028H

SUPERVISOR: MR KUFAKUNESU

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE MASTER OF BUSINESS

MANAGEMENT AND INFORMATION TECHNOLOGY HONORS DEGREE

MBIT

FEBRUARY 2026



Muzenda Bryn

Student



Mr F. Kufakunesu

Supervisor

INTRODUCTION

1.1 Background to the Study

In the modern digital economy, personal data is a primary driver of economic value creation, innovation, and power relations in the global information ecosystem. Social media sites such as WhatsApp, Facebook, Instagram, TikTok, and X (formerly Twitter) have changed social interaction to a data-driven form of social interaction characterized by continuous harvesting and analysis of personal data. In the global information ecosystem, the value of the personal data economy was estimated to be USD 274 billion in 2023. However, it is projected to rise to more than USD 480 billion by 2027. This is a form of value creation largely driven by social media advertising and behavior analysis (Statista, 2024). In 2024, there are over 5.04 billion active social media users worldwide. These users form 63% of the world's population and spend over 2 hours and 20 minutes every day interacting on social media (DataReportal, 2024).

In the face of growing data privacy threats, advanced economies have taken significant steps to fortify data protection standards. The European Union's General Data Protection Regulation (GDPR), the world's premier data protection benchmark, has seen enforcement actions result in over €4.3 billion in fines from 2018 to 2023, with the majority of the cases involving the abuse of personal data by social media (European Commission, 2023). In the United States, the Federal Trade Commission has observed a 72% increase in complaints from consumers about the abuse of data and identity theft between 2020 and 2023, with social media identified as one of the biggest contributors to data exploitation (FTC, 2023). In addition, the Canadian government has passed the Digital Charter Implementation Act (Bill C-27), strengthening consent and enforcement measures for the unlawful processing of data, while the Australian government has commenced a

complete overhaul of its Privacy Act in the wake of data breaches affecting over 10 million citizens (Government of Australia, 2023). These actions demonstrate the world's growing consensus on the need to rein in the data practices of social media to ensure the protection of individual rights and the sovereignty of nations in the digital sphere.

Across Africa as a whole, the rapid development of mobile Internet access has led to social media becoming the main gateway to the digital world. GSMA (2024) highlights the fact that sub-Saharan Africa registered a 29% mobile Internet penetration rate by the end of 2023. In this regard, social media was responsible for more than 60% of total mobile data traffic. DataReportal (2024) highlights the fact that countries such as Nigeria (36.6 million users), South Africa (26 million users), and Kenya (13.7 million users) registered double-digit annual growth in social media usage, mainly through WhatsApp and Facebook. However, this rapid growth in the use of social media does not match the growth in data protection. Studies have shown that only 39% of social media users in Africa are aware of the manner in which their personal data is shared or collected. In addition, only 1 out of 5 users can identify the data protection authority of their respective countries (Makulilo, 2022; GSMA, 2024). In countries with more developed data protection laws, such as South Africa's Protection of Personal Information Act (POPIA), data breaches and compliance issues continue to undermine the confidence of the public in the data protection landscape (Naidoo & Ramluckan, 2023).

Zimbabwe's case mirrors most of the issues affecting the rest of the African continent. However, the case of Zimbabwe seems to be more vulnerable to data protection issues. In the year 2024, the total number of active social media users in Zimbabwe was 1.45 million, making up 8.3% of the total national population. Social media access was mainly facilitated through mobile networks (DataReportal, 2024). The use of social media platforms by Zimbabweans was dominated by WhatsApp, with 94% of the total social media users utilising the platform. In contrast, 56% of the total social media users were using Facebook, 37% were using TikTok, and 21% were using Instagram. The high usage of data-intensive platforms through mobile networks highlights the vulnerability of the Zimbabwean data protection landscape to the consequences of data breaches. The use of social media bundles by the major telecommunication firms in the country not only reduces the access cost of the platforms but also increases the level of data usage through mobile networks.

NetOne Zimbabwe, the second-largest MNO in the country, plays an important role in this environment. NetOne Zimbabwe has more than 4.1 million active subscribers as of the fourth quarter of 2023, with the majority using the company's affordable data and social media bundles to communicate on a daily basis (POTRAZ, 2024). Although this has helped to drive digital inclusion, it has also increased concerns about data governance. The country has experienced an increase in the number of cybercrime cases, with the Zimbabwe Republic Police reporting more than 9,000 cases of cybercrime between 2022 and 2023, including hacking of social media accounts, identity theft, and unauthorized access to data (ZRP, 2023). These trends show an increase in the exposure of personal data in an environment where data protection measures are still in an early stage of development.

In an attempt to combat these threats, the Zimbabwean government enacted the Data Protection Act [Chapter 11:12] in December 2021, which provides the foundation for data protection, including the establishment of the Data Protection Authority. However, evidence indicates that the level of data protection in Zimbabwe is still wanting. A study by MISA Zimbabwe (2023), on the findings of the national survey on the situation of digital rights in Zimbabwe, revealed that 72% of internet users in Zimbabwe are not aware of their data protection rights, and 58% have little trust in the ability of MNOs to protect personal data. In addition, the study revealed that Zimbabweans have a tendency to agree to the terms and conditions of social media without an understanding of the data-sharing implications, due to the affordability of the services and lack of digital literacy.

In terms of academic research, it is apparent that, despite the interest in Zimbabwe's legal regime, there has been a notable lack of research on the operation of data protection duties by MNOs in the context of the environment provided by social media services. Existing research has largely focused on the legislative regime in the abstract, or on international players such as Meta and Google (Makulilo, 2022), without adequately addressing the gap in the context of local players such as NetOne, who are the principal data gatekeepers for millions of citizens. There is also a lack of evidence on the perceptions of data privacy risks by subscribers in the context of the telecom-driven social media environment.

In this context, the research is clearly timely and necessary. By focusing on NetOne Zimbabwe, the research has the potential to fill the gap in the research on the interface between social media

and personal data protection from the perspectives of the user and the institution. The research engages with the new and evolving issue of privacy risks, as well as the issue of awareness and the challenge of implementing the regime, and makes a new contribution to the discourse on data protection in Zimbabwe.

1.2 Statement of the Problem

Thus, the rapid proliferation and growth of social media platforms in Zimbabwe, primarily facilitated and driven by mobile network service providers such as NetOne, have significantly increased the quantity and nature of personal data that is shared, stored, and processed online. Despite the Data Protection Act [Chapter 11:12], which was enacted in 2021, it is apparent that the mechanisms and systems put in place to ensure data protection are not only poorly developed and monitored but also lack the requisite oversight and control, especially in semi-public institutions and organizations. Data from the Media Institute of Southern Africa (MISA Zimbabwe, 2023) indicate that over 72% of users are not aware of the data protection legislation, and 58% are suspicious and do not trust the handling of their personal data by mobile service providers such as NetOne, despite the expansion of data bundles that have enabled digital inclusion and access to social media platforms for over 4.1 million users in Zimbabwe (POTRAZ, 2024). Thus, the disjunction between data usage and data protection mechanisms and systems is an important indicator of the gap between the actual state of data exposure and the ideal state of data handling that is secure, ethical, and lawful in nature, in line with international best practices such as the General Data Protection Regulation (GDPR).

This compounding challenge is compounded by the scarcity of empirical evidence on how Zimbabwe-based mobile network service providers interpret and implement personal data protection laws in the context of social media usage. Most of the literature in the region has focused on continental regulation, as well as multinational corporations such as Meta and Google (Makulilo, 2022). As such, there is a notable knowledge gap in understanding how institutional practices in the region contribute to the regulation of personal data protection laws in the context

of social media usage. The limited scholarly examination of how mobile service providers in Zimbabwe, exemplified by NetOne, manage risks associated with data harvesting, access to third-party services, and user profiling in the context of social media usage limits the ability to develop context-specific regulation and institutional practices. If not addressed, Zimbabwe is likely to maintain an environment in which its citizens are extremely vulnerable to data exploitation, algorithmic manipulation, and surveillance by the state. As such, the current study seeks to contribute to the knowledge gap in understanding how NetOne protects user data in the context of social media usage.

1.3 Research Objectives

1.3.1 Main Objective

The general objective of this study is to investigate the link that exists between the use of social media and the protection of personal information in Zimbabwe, with NetOne Zimbabwe used as a case study. To achieve the general objective of the study, the research is guided by the following specific objectives:

1.3.2 Specific Objectives

1. To assess NetOne customers' perceptions of personal data privacy when using social media on NetOne's network.
2. To investigate the impact of social media on personal data protection in Zimbabwe.
3. To identify the challenges faced by NetOne Zimbabwe in implementing data protection regulations in the context of social media.
4. To propose a framework of best practices for enhancing personal data protection in telecom social media engagement.

1.4 Research Questions

The following research questions are formulated to align with the stated objectives and will guide data collection and analysis throughout the study:

1. What are NetOne customers' perceptions and concerns regarding personal data privacy when accessing social media via NetOne's services?

2. How does the usage of social media influence the protection or exposure of personal data in Zimbabwe?
3. What challenges does NetOne Zimbabwe face in complying with data protection regulations related to social media?
4. What best practice framework can be proposed to strengthen personal data protection in telecom-led social media environments?

1.5 Research Hypotheses (Quantitative)

These hypotheses are developed to statistically examine the relationships between social media usage and perceptions of data protection among NetOne users:

1. ***H₁:** There is a significant relationship between frequency of social media usage on NetOne's network and users' concerns about personal data privacy.*
2. ***H₂:** Users with higher levels of digital literacy are more likely to perceive NetOne's data protection measures as inadequate.*
3. ***H₃:** The perceived effectiveness of NetOne's data protection practices positively influences user trust and continued use of its social media services.*

1.5.2 Research Propositions (Qualitative)

The following propositions are designed to guide the qualitative inquiry into institutional challenges and best practice development:

1. ***P₁:** NetOne Zimbabwe faces internal and external regulatory constraints that limit its full compliance with the Data Protection Act in managing social media-related data.*
2. ***P₂:** Existing public communication strategies by NetOne do not sufficiently inform users about their data protection rights and how their data is used.*
3. ***P₃:** A user-centred, transparent, and technically robust data protection framework can enhance privacy assurance in telecom-driven social media engagement.*

1.6 Significance of the Study

The study is important for its contribution towards advancing both theory and practice in the ever-evolving discourse on digital privacy and personal data protection in Zimbabwe, with specific reference to the telecommunications and social media industry. As Zimbabwe speeds into a digital age through mobile internet connectivity and consumption of global social media platforms, personal data protection has become a national security and human rights imperative in Zimbabwe. In this regard, the study is relevant in that it examines one of Zimbabwe's biggest mobile network operators, NetOne Zimbabwe, in terms of how it handles personal data in light of its central role in facilitating access to social media platforms in Zimbabwe.

1.6.1 Policymakers

From a policymaking point of view, the study offers critical insights for the Government of Zimbabwe and key institutions like the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), the Cybersecurity and Monitoring Centre, and more recently, the Data Protection Authority. In that regard, the study will provide critical insights into how NetOne Zimbabwe has complied with the 2021 Data Protection Act in Zimbabwe. In a world where digital rights are increasingly prominent in policymaking and practice, the study may be instrumental in informing a rights-based framework for digital governance in Zimbabwe.

1.6.2 NetOne Zimbabwe

In terms of the practical applicability of the research, the current study holds particular importance for NetOne Zimbabwe. As a semi-public entity in the field of telecommunications, NetOne Zimbabwe is faced with the challenge of balancing business needs with ethical considerations in the management of personal data. Through the identification of gaps in the effectiveness of data protection measures and the transparency of the consent process, the research provides practical recommendations for improving user trust, ensuring legal compliance, and enhancing corporate integrity. In an environment in which trust in the digital sphere represents a unique selling proposition in the field of telecommunications, NetOne Zimbabwe stands to benefit from the

establishment of best practice standards in the management of personal data in conformity with international standards and user expectations.

1.6.3 Subscribers

In terms of the impact of the research on NetOne Zimbabwe subscribers and Zimbabwean citizens in general, the research holds importance in the empowerment of the wider population. A considerable number of users remain unaware of the rights they have in the management of their personal data and the degree to which their personal data is processed, shared, and stored. Through the study of perceptions and awareness, the research provides a contribution to the education of the wider population on the importance of digital rights and the need to ensure the protection of personal data. The research may also have a bearing on civil society organizations and digital rights advocacy groups, who are active in the promotion of digital literacy and legal empowerment in underrepresented communities.

1.6.4 Academia

From an academic perspective, the significance of the research lies in its ability to fill an existing knowledge gap in Zimbabwean and regional academia. While there is an increase in literature on data protection in Africa, there is an underlying theme of multinational technology platforms or comparative regional legislation (Makulilo, 2022). Few empirical studies have examined the local implementation of data protection in Africa, especially from the perspective of national mobile operators. The present research aims to resolve the above knowledge gap by presenting an in-depth context-specific case study that incorporates law, technology, and user experience in the context of Sub-Saharan Africa.

1.7 Assumptions

This study is grounded in a number of foundational suppositions, which set the boundaries of the research without becoming the main subject of the investigation.

- i. It was assumed that the company engages in the processing of personal data by its Zimbabwean subscribers when accessing social media platforms through the company's infrastructure, particularly through the company's dedicated social media bundles. This assumption forms the premise of the importance of the company's responsibility in the overall discourse of the protection of personal data. Without the company engaging in data

processing, the company would be considered to be out of the scope of the Data Protection Act [Chapter 11:12], thus reducing the importance of the company's compliance and the challenges associated with the same.

- ii. It was also assumed that the use of social media platforms by Zimbabwean subscribers, particularly those who use mobile networks, is growing in scale and sophistication, thus necessitating the development of more effective, flexible, and transparent data protection policies by the company. This assumption was well-supported by the publicly available statistics obtained through DataReportal (2024) and POTRAZ (2024).
- iii. Finally, the assumption of the existence of a discernible perception gap was also considered important in the overall context of the study. It was assumed that a discernible perception gap exists among the company's subscribers regarding their understanding of the company's handling of their personal data.

1.8 Delimitations of the Study

The scope of this study is also defined by the following critical parameters, which are pertinent to its management, relevance, and analytical depth.

1.8.1 Geographical

The geographical scope is restricted to the Central Business District (CBD) of the city of Harare, the commercial and administrative centre of Zimbabwe. The study is based on the Harare CBD because it is characterized by high population density, extensive mobile network usage, and the prevalence of formal and informal commercial activities, which are largely dependent on digital connectivity. The Harare CBD is, therefore, the microcosm of the Zimbabwean digital environment where the services of NetOne are highly utilized for the access of social media sites and other data-driven online platforms.

1.8.2 Institutional

The institutional scope is restricted to the case study of NetOne Zimbabwe, the second-largest mobile network provider in Zimbabwe. NetOne, which is owned by the Zimbabwean government, plays a critical role in facilitating digital communication and access to the internet for the majority of Zimbabweans. It is, therefore, pertinent to examine the role played by mobile network providers

in the implementation and observance of data protection laws in Zimbabwe, especially regarding the collection, use, and protection of subscriber data in the context of social media access. Other telecommunications providers, such as Econet and Telecel, are excluded to ensure the depth and accuracy of the study.

1.8.3 Temporal

The temporal scope of the study is the post-enactment period, i.e., the period after the enactment of the Data Protection Act, focusing on the period between December 2021 and mid-2025. This is the period during which NetOne has been legally obligated to comply with the Data Protection Act. This period is significant since it allows the examination of the immediate response to the regulatory framework, including institutional reforms, changes to the organization's data protection policy, or public information campaigns, among other aspects.

1.8.4 Thematic

The study is also thematic in the sense that it is devoted to the examination of the relationship between the use of social media and the protection of personal data. For instance, the study is devoted to the examination of the impact of the organization's mobile data services, including the organization's social media bundles, on the users' data privacy, the internal mechanisms employed by the organization to ensure the effective management of the users' data, and the level of awareness or empowerment of the users regarding their data rights, among other aspects. The study does not examine the organization's telecommunications infrastructure, including the quality of voice calls or the deployment of broadband, unless it is related to the organization's data protection policy, especially regarding social media users.

1.8.5 Target Population

The target population is the NetOne subscribers within the Harare Central Business District who actively engage in the organization's social media services, including key informants such as NetOne employees, including those responsible for data protection, data management, or marketing, among other key informants such as the regulators. Even though the study is limited to the case study, it is expected to provide insights into the subject matter, which could be used as the foundation for broader future research.

1.9 Organisation of the Study

This study comprises five chapters. Chapter 1 provides an overview of the study by outlining the background, problem statement, research objectives, research questions, significance, scope and delimitations, and research assumptions. This chapter provides the contextual and conceptual background of the study.

Chapter 2 provides an extensive overview of the relevant literature on the use of social media and personal data protection. The chapter critically examines the theoretical, conceptual, and empirical works on the research subject, as well as the gaps in the knowledge domain, to justify the need for the study.

Chapter 3 outlines the research methodology used in the study. The chapter outlines the research philosophy, paradigm, design, target population, sampling, data collection instruments, data analysis, and research ethics. The chapter provides an overview of how the study was systematically conducted to achieve the research objectives.

Chapter 4 presents and analyses the data collected from NetOne subscribers and key informants. The quantitative data will be analysed using statistical analysis, whereas the qualitative data will be analysed using thematic analysis. The findings will be interpreted in relation to the research questions and objectives.

Chapter 5 discusses the findings in relation to the research literature, conclusions, and recommendations. The chapter will also outline the study's contribution to knowledge and its limitations.

1.10 Chapter Summary

This chapter provided an overview of the study, including the background, problem statement, objectives, assumptions, and scope. The chapter, therefore, provides the rationale for the study, focusing on the relationship between social media and the protection of personal data in Zimbabwe, with particular reference to NetOne Zimbabwe. This chapter also provides the background for the other chapters, starting with the review of related literature in Chapter Two.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The rise of social media has significantly impacted interaction, communication, and service access worldwide. Despite the positive impacts of social media, concerns about the protection of personal data have increased, especially in developing countries such as Zimbabwe, where the legal and regulatory environment is not yet sufficiently developed to address the rapid evolution of technology. NetOne Zimbabwe, which is owned and operated by the Zimbabwean government and provides telecommunication services, plays a central role in the context of access to social media and data protection concerns. This paper will discuss the challenges and possible solutions in relation to the use of social media and data protection in NetOne Zimbabwe.

The chapter is designed in such a manner that it will be possible to conduct an in-depth analysis of the scholarly and empirical work in relation to the areas of focus that are pertinent to the purposes and objectives of the study. The main areas of focus are the dominant theoretical frameworks that are central to the work, which include the Communication Privacy Management Theory, the Theory of Reasoned Action/Planned Behavior, and the Technology Acceptance Model, in relation to empirical work in the field.

2.2 Theoretical Framework

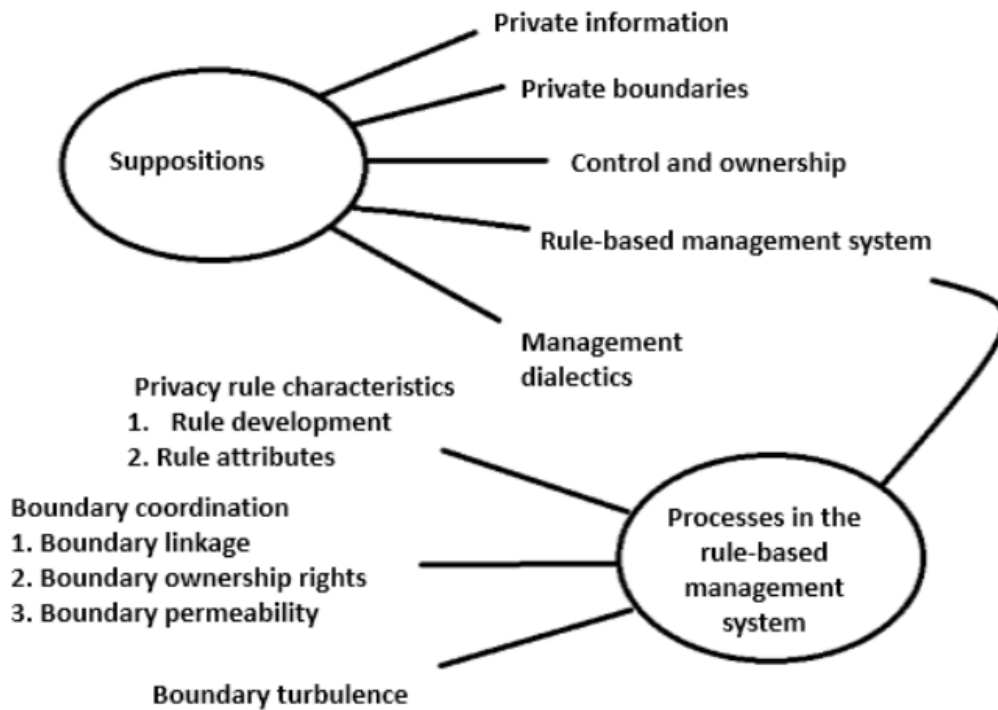
This study will explore the theoretical underpinnings of social media use and the management of personal data in Zimbabwe, with reference to NetOne users. The study will combine three theoretical models: the communication privacy management theory, the theory of reasoned action/planned behavior, and the technology acceptance model. These theories are used in this study because they are relevant in addressing the issue of privacy management among social media users and the use of social media technology with the associated risks.

2.2.1 Communication Privacy Management Theory

The theory of Communication Privacy Management (CPM) was developed by Petronio (2002). The theory offers a framework for the analysis of the management of personal information by individuals. According to the theory, personal information and privacy are owned by the individual. The terms under which the information can be used or shared are set by the owner of the information. The terms can vary in accordance with cultural, relational, or environmental conditions. The framework of the theory of CPM, in which there are “co-owners” of the information who set the conditions for the use of the information, can be applied to the complex ways in which users of social networking sites interact with one another. Figure 2.1 shows the components of the theory of CPM.

Figure 2.1: CPM Theory

Private information



Source: *Communication Privacy Management Theory*, Petronio (2007)

The application of the CPM in the current context highlights the ways in which the clientele of NetOne address the issue of privacy in the context of the social media network. The current privacy environment in Zimbabwe can be characterized by the prevailing socio-political environment in the country, in which the revelation of personal information has substantial security implications for the people of Zimbabwe. The dependency of people on telecommunication service providers, such as the government-owned NetOne, has a substantial influence on personal information. The current environment can be related to the observations made by Xiao et al. (2025) regarding the transparency and privacy policy of the social media network in the context of the current environment, as highlighted in Xiao (2025).

In the current environment, the prevailing global best practices, such as the General Data Protection Regulation (GDPR), provide a framework for the implementation of the data protection mechanisms. The framework highlights the importance of the principles of lawfulness, fairness, transparency, data minimization, and accountability. In addition, the framework highlights the

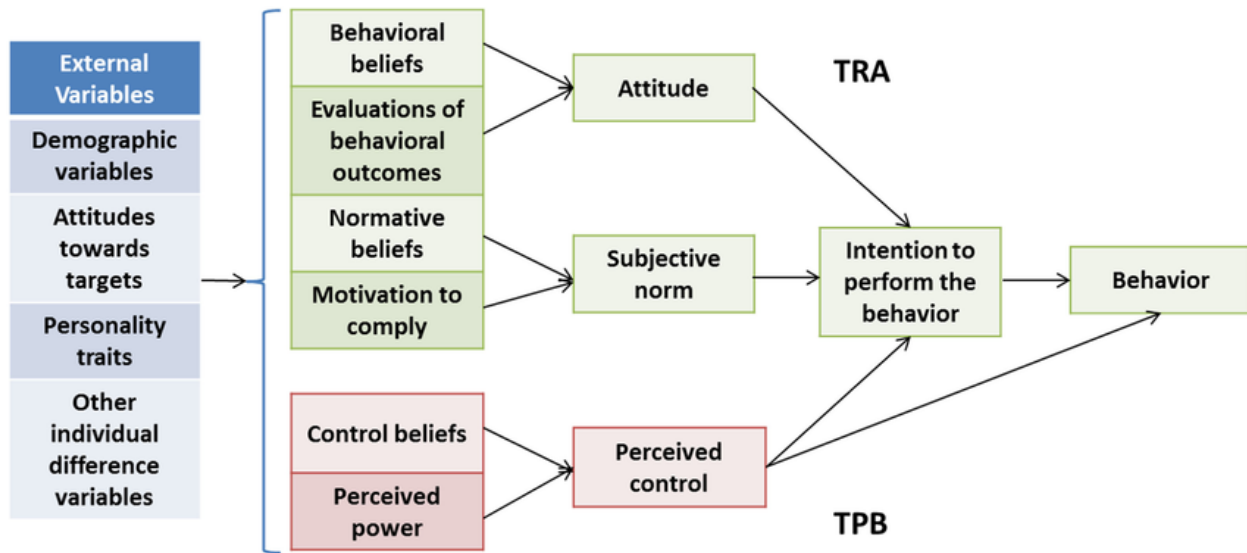
importance of the enabling technologies, which provide users with the tools for the management of the issue of privacy, such as the mechanisms for the provision of consent for the sharing of information. The application of the highlighted mechanisms can have a substantial influence on the ability of the customers of NetOne to trust the firm.

2.2.2 Theory of Reasoned Action/Planned Behaviour

The Theory of Reasoned Action (TRA), developed by Fishbein and Ajzen in 1975, and the Theory of Planned Behavior (TPB), developed by the same researchers in 1985, aim to identify the role of personal attitudes, social pressures, and perceived behavioral control in influencing actual and planned behavior. In the context of the TRA theory, actual behavior is directly influenced by two factors: the attitude of the individual toward the behavior and the subjective norm, including pressures from other people and those of the broader society. The TPB theory adds a new dimension to the TRA theory by including perceived behavioral control, which refers to the perceived ease or difficulty of the individual in performing the behavior.

The inclusion of the TRA and TPB theory provides a new dimension to the analysis of the use of social media and the use of personal data by individuals in Zimbabwe. The attitude of the consumer toward the use of social media, influenced and reinforced by the perceived benefits of the use of social media platforms such as Facebook, WhatsApp, and TikTok, may be seen as a paradox. The determinant studies of the use of social media by individuals in Zimbabwe, as presented by Simbarashe et al. (2024), emphasize the importance of the subjective social norms of the individuals in the use of social media despite the risks. Figure 2.2 presents the TRA and TPB theory.

Figure 2.2: Theory of Reasoned Action or Planned Behaviour



Source: *Theories of Planned Behaviour and Reasoned Action from Theory at a Glance* (2005)

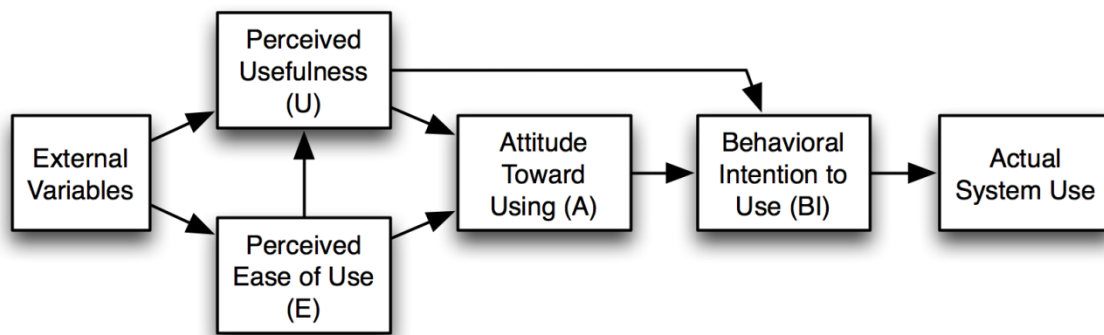
The TRA and TPB approaches are instrumental in understanding the so-called “privacy paradox,” in which people express high privacy concerns but demonstrate behaviors that are seemingly incongruent with these expressed concerns. A potential rationale for the “privacy paradox” may be the socio-economic environment in Zimbabwe, in which social media may be vital for social communication. The perceived behavioral control component of Ajzen's (1991) theory may be relevant in the enrolment and engagement process employed by NetOne in its quest to sensitize its users on the privacy attributes available on its platform. A suitable example, as informed by the case scenario, is the amalgamation of the Technology Acceptance Model and the TPB approach, as espoused by Sharma et al. (2025).

2.2.3 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) was proposed by Davis (1989). The basic aim behind this model is to explain the adoption process by focusing on two major factors: perceived usefulness (PU) and perceived ease of use (PEOU). Perceived usefulness means that the

technology would increase productivity, and perceived ease of use means how easy it would be for the user. This model is used in situations where the adoption process may involve unfavourable factors like invasion of privacy. Figure 2.3 depicts the TAM model.

Figure 2.3: Technology Acceptance Model



Source: Factors of the Technology Acceptance Model for Construction IT, Park (2020)

In terms of engaging with social media in the context of NetOne’s Net services, the Technology Acceptance Model (TAM) indicates the level at which customers weigh the benefits of engaging with social media against the risks associated with privacy in the context of solving the issue. While social media offers benefits in terms of connectivity, access, and communicative efficiency, the risks may serve as a deterrent for engaging with it. However, in most instances, the benefits in terms of accessibility, personalisation, and usability outweigh the risks, as discussed in Uddin et al. (2025).

The TAM model is also relevant in terms of the “privacy paradox”, where usefulness is a key driver in terms of continued use in spite of ongoing privacy concerns. Zhu et al. (2023) provide evidence for the relationship between technology acceptance and the moderating effect of building trust in terms of reducing the effect of privacy concerns in technology acceptance in contexts such as telemedicine and other contexts that may be relevant for NetOne services.

Furthermore, TAM emphasizes the need to integrate the role played by privacy-enhancing technologies within social media sites available through telecommunication network access. Customer awareness, along with innovative security features requiring minimal direct customer involvement, could be key facilitators in improving ease of use, including data privacy. With the dynamic nature of globalization, coupled with the evolution of standards, findings from other international research on this issue reinforce the importance of customer trust and transparency in enhancing the core constructs of TAM, as emphasized by Gelashvili et al. (2024).

The present study, through the integration of CPM, TRA/TPR, and TAM, aims to develop a comprehensive framework to address the relationship between social media use and data privacy in Zimbabwe. Within this framework, CPM will be able to address customer motivations, including data privacy, along with the latent factors identified by the psychological factors in social media use, as emphasized by TRA/TPR. Simultaneously, TAM will be able to address the need to integrate the role played by technological determinants in the adoption process, notwithstanding the issues affecting data privacy.

2.3 Thematic Literature Review Based on Research Objectives

This segment synthesises the literature in relation to the four main goals, which are presented in four different themes. These themes are in relation to (1) customer perceptions of data privacy, (2) the effect of social media on data protection, (3) challenges in implementing regulations, and (4) best practices. The studies utilise a funnel approach that covers global, regional, and local aspects.

2.3.1 Customer Perceptions of Personal Data Privacy

The recent advent and dominance of social media sites have placed the issue of personal data privacy in the spotlight, as people around the world are showing an increased level of concern with respect to the collection, storage, and use of their personal data on social media sites. Through an extensive qualitative research approach, Jafari and Shaghaghi (2023) used in-depth interviews with 23 social media users and thematic analysis to reveal the ways in which people conceptualize personal privacy. The study revealed the following: Despite the increased level of awareness among social media users with respect to this issue, their attitudes and willingness to share personal data are largely influenced by the benefits and utilities derived from the use of social media sites.

The study revealed the need to develop more user-friendly tools to manage personal data and to educate people about the use of social media sites.

In a large-scale study, the issue was addressed in a study by Marín et al. (2022). The study was conducted in a cross-sectional design in which a survey was conducted on a total of 225 pre-service teachers from Germany, New Zealand, Spain, and the US. The study aimed at investigating the perceptions of the educational potential of social media and the related data privacy concerns. The study found that the pre-service teachers generally valued the use of social media in their professional lives, yet there was a high level of concern related to the use of social media in terms of data privacy. The study found a high level of ambiguity in the knowledge of data privacy policies and protections, particularly in terms of attitudes and opinions in countries with high levels of stringency in terms of data protection, such as Germany.

In the Indian context, the study conducted by Jain et al. (2025) aimed at investigating the level of privacy concerns in the use of popular social media sites, including Instagram, Facebook, TikTok, WhatsApp, and so on, among a total of 600 youths in the age group of 13-19 years from major and semi-major urban areas in India. The study found that although the youths were becoming increasingly aware of the related privacy concerns, yet there was a lack of trust in the ability of the companies to protect the personal information of the users. The study further found that the youths were revealing personal information on the social media sites despite the fact that there was no need for them to reveal the information.

In the marketing sector, Thakkar (2025) carried out a survey on the relationship between data privacy and social media marketing, with the results providing valuable insights into the issue. From the findings, it is evident that the failure to address data privacy issues, coupled with the constant data breaches, has contributed to the erosion of trust in social media marketing practices among the general public, who are now calling for stricter laws to be put in place. According to the findings, data breaches are significant influencers on customer loyalty, and failure to address this issue through data privacy practices is likely to result in anger and disappointment on the part of the customers. The findings also indicate that adherence to the GDPR is significant in the implementation of data privacy practices.

In the Chinese culture, Yu et al. (2025) carried out a survey on the impact of the APFO model on the relationship between the social media users' privacy concerns, experiences, and literacy, with

the results providing valuable insights into the issue. From the findings, it is evident that the phenomenon of privacy fatigue, which refers to emotional exhaustion caused by constant exposure to data breaches, is the key factor mediating the relationship between the users' concern for their data privacy and the implementation of data privacy practices. This is significant in the implementation of data privacy practices, focusing on the importance of the users' welfare, as highlighted in the report by Zouai et al. (2024).

In the Pan-European study, Alkis & Kose (2022) carried out a study with 153,053 respondents across 29 countries, utilizing multi-level logit modeling. The results show that there is a positive relationship between knowledge levels and the perception of risks related to privacy and e-commerce, but increased concern over the recording of online activities leads to decreased participation. What is also significant is the finding that people who engage in online activities that are protective of their online privacy are more likely to engage in e-commerce and be more trusting of social media advertisements, implying that firms who offer effective online privacy tools could boost online participation and trust levels.

What all these studies show is the disconnect between the growing awareness of online risks and the actual precautionary steps taken, which is due to low levels of digital literacy and trust levels. What is also significant is the methodological approach adopted, where large-scale surveys carried out across multiple nations provide significant insights, but also reveal the lacunae in the existing body of literature on the role played by culture, etc., on online privacy, which is the so-called “privacy paradox.”

2.3.2 Impact of Social Media on Personal Data Protection in Zimbabwe

Across the globe, social media has developed into complex systems designed to collect data, utilizing data collection mechanisms such as data harvesting, profiling, and advert targeting. According to Böyük (2024), through qualitative document analysis on the privacy policies and breaches on Facebook, Instagram, X (Twitter), YouTube, and TikTok, it is evident that users get confused by the complexity of the data collection policies, thereby complicating the issue of providing informed consent. This was demonstrated through the Facebook-Cambridge Analytica data breach on privacy, the data breach on TikTok, and the issues surrounding data access, its breach, and the measures taken to address the issue of user agency, the need for clarity on the policy side, and the need for severe regulatory action to be taken (Böyük, 2024).

In the review article by Yang (2025), the discussion on the implementation of privacy protection technologies on social media is presented. The challenges identified in the implementation of the technologies are data leakage, noncompliance, and low levels of awareness among users. The article advocates for the implementation of advanced technologies, including data encryption, to improve the level of confidentiality in the data posted on the social media platform. It is asserted that it is not enough to solely rely on technology to improve the security of the data posted on the social media platform.

Chen et al. (2024) used a hybrid SEM and ANN model for 527 participants. The authors suggested and validated that social benefits and enjoyment factors are antecedents for data disclosure. In addition, high levels of trust and experience in being invaded in their privacy increase risk perception and personal privacy protection needs. This study generalizes the use of the proposed privacy calculus theoretical framework and clarifies linear and non-linear relationships between perceived risks and benefits and personal intentions for data disclosure or nondisclosure. The findings show that despite the social and entertaining benefits of social media platforms, negative experiences may encourage more cautious behavior (Chen et al., 2024).

In terms of European law, Di Minin et al. (2021) assessed the legal framework for using social media data relevant to conservation science in accordance with the GDPR. The focus was on data minimization, anonymization, and management. In addition, risk management strategies for maintaining compliance with legal regulations are proposed. However, it is noted that despite the robustness of the legal framework in certain regions, problems arise in balancing legal regulations with practice in terms of social media data use in this scientific field (Marín et al., 2022).

Yang and Liu (2025) studied the effect of the GDPR using synthetic control and difference-in-differences approaches in the context of social media markets' concentration. The results suggest that, although the GDPR initially had positive impacts in terms of data regularization and protection, the long-run impacts have since diminished. The application of advanced statistical techniques in the paper provides an understanding of the complex relationships between regulations, markets, and data protection, as revealed in the study by Thakkar (2025).

In Africa, the legal system is in its development stage. Shao et al. (2024) carried out an exploratory comparative case study to evaluate data protection legislation in Tanzania, Kenya, Uganda, and Rwanda. The authors evaluated data protection legislation in these four African countries using

legal documents, formal reports, and scholarly publications. The results revealed that, although data protection acts have been established in these four countries, the regulations are different in their scope and content. The authors recommend that data protection legislation in these countries should be harmonized and that the legal system needs to be developed further (Shao et al., 2024).

In Zimbabwe, the data protection system, as outlined in the Data Protection Act [Chapter 11:12], recognizes the importance of aligning itself with best practices in other countries in the world. However, some critical studies have pointed out some weaknesses in implementing the data protection system and some aspects of the legislation that are ambiguous, especially in relation to data flow via social media platforms. It is apparent that the situation is complex, and factors that are likely to affect data protection via the use of social media are multi-dimensional, touching on both technological and social aspects. The methodologies applied in these studies, which include document analysis and advanced statistical analysis, point to the intricacies involved in determining the impact of social media on data protection systems in Zimbabwe and other countries in the world.

2.3.3 Challenges in Implementing Data Protection Regulations

Organizations, especially in the telecommunication industry, face various challenges in the implementation of data protection laws. These challenges range from the complexity of the technology to the high costs of compliance and the lack of trained personnel, among other issues (Quach et al., 2022).

Regulatory and Institutional Challenges

Nevertheless, there are effective legal provisions such as Law Number 27 of 2022 in Indonesia. However, there are still resource issues for regulatory bodies. The Personal Data Protection Agency in Indonesia is responsible for overseeing the regulation of over 200 million internet users' data while struggling to deal with a scarcity of resources to regulate the issue adequately (Lihawa, 2025).

In Canada, over $\frac{3}{4}$ of the population use social media services. However, there is no instance where social media companies have been fined for their activities, nor is there any effective legal provision regarding the transfer of personal data outside the country in the last two decades since

privacy legislation was enacted (Stevens et al., 2020). In addition to that, there is a problem in ensuring effective legal provisions to deal with global issues by social media services. In particular, although 86% of residents in Canada recognize the need to store their information locally, most of the data provided by residents to social media services is stored outside the country in jurisdictions that are less effective in providing regulations (Stevens et al., 2020). These services also do not identify Canada as a storage destination.

Legal and Procedural Ambiguities

Ambiguities in the law of informed consent affect the efficacy of data protection. Evidence suggests that the terms of service agreements of social networking websites are usually 5,520 words long, making them inaccessible to the majority of users (Fiesler et al., 2020). In this regard, social networking site users usually click “agree” to the terms of service without understanding the consequences of the data being collected. This paradox is also evident in the fact that 600 Indian youth were found to be concerned about privacy but lacked confidence in the platform’s ability to provide this privacy (Jain et al., 2025). This arises from the ambiguity of the law with regard to the definition of personal data, whereby user behaviour through the internet is used to create a detailed digital identity with inadequate protection (Cheng and Guo, 2025).

Additionally, the lack of clear prohibitions and the procedural approach of the law of lawfulness create an environment where data controllers may be more inclined to emphasise the importance of disclosure as opposed to control. For example, the default setting of most platforms will be to maximise the information disclosed to the user. The attitude of the user to the law of consent has also been described as “woefully inadequate” to the protection of privacy (Cheng & Guo, 2025; Fiesler et al., 2020).

Enforcement and Cross-Border Issues

In addition, the enforcement of data protection regulations is still wanting, especially in the case of international data transfer. In the case of Canada, for instance, despite the extensive practice of outsourcing data to foreign countries, no corporations have been brought to book for violating the privacy of their users in the context of data transfer outside the country (Stevens et al., 2020).

Globally, 86% of the Canadian population favors data localization, yet the data of the users is still being transferred and processed from diverse geographical locations, contrary to the preferences of the users (Stevens et al., 2020).

International social media has made the issue of protecting the privacy of the users more complex. The social media can set the level of the privacy of the users according to the lowest standards, thus exposing the users in more regulated regions to higher risks. The lack of an international framework on the governance of social media in the context of data protection regulations has made the issue more complex (Lihawa, 2025; Stevens et al., 2020).

Technological and Platform-Driven Barriers

Technological advancement, especially in terms of artificial intelligence, has developed at a much faster rate than regulatory bodies. Incidents like those concerning Facebook and Cambridge Analytica, and data breaches concerning TikTok, have had significant effects on millions of users and have highlighted the problems concerning inadequate security (Büyük, 2025).

There is evidence that suggests a lack of voluntary restraint in terms of cyberbullying among social media platforms like TikTok and Instagram; only 5% of cyberbullying incidents resulted in legal action, despite a fourfold increase in incidents from 800 in 2018 to 3,800 in 2023 in Indonesia (Nugraha et al., 2025). In addition, the level of complexity in terms of privacy settings may be beyond the average user's ability to control. The average user is unable to comprehend how they can utilize available settings in order to control their level of privacy in terms of data use (Büyük, 2025).

User Awareness and Digital Literacy

One of the problems that has persisted is that of a lack of awareness and digital literacy. For example, in a study that targeted 600 youths in India, it was noted that despite enhanced awareness about concerns for privacy, youths showed a lack of awareness and understanding about platforms and were unable to utilise their privacy settings appropriately (Jain et al., 2025). In addition, only 20% of cyberbullying incidents in Indonesia were addressed by law enforcement agencies, which indicates that there is a lack of awareness about how to address cyberbullying incidents and that there is a lack of digital literacy (Nugraha et al., 2025). However, it is important to note that without

advancements in digital literacy, it is unlikely that legislation would be able to bring about significant changes in data protection (Jain et al., 2025).

2.3.4 International Best Practices and Lessons for Zimbabwe

An analysis of international best practices in the protection of personal data on social platforms reveals several considerations that can be regarded as the best practices in Zimbabwe. Countries that have developed effective personal data protection laws and regulations include the European Union, the United States of America, and various Asian nations. These nations offer several lessons on what has worked effectively in the past and what has not worked effectively in the context of personal data protection on social platforms.

For example, in the context of the European Union's General Data Protection Regulation (GDPR), which has set the standard for personal data protection across the world, there is an extremely high level of stringency in requirements related to data minimization, processing on the basis of legitimate consent, and the need to implement a data breach notification procedure. In the context of conservation science in the EU, Di Minin et al. (2021) revealed that in order to comply with the GDPR requirements, there is a need to go beyond merely implementing various technical requirements such as anonymization of personal data and storing personal data securely. Rather, there is also the need to implement various requirements related to moral and ethical considerations that involve minimizing harm to personal data subjects and the need to implement principles of transparency in personal data.

This is in line with the study on the UK-China context on the efficacy of the human rights approach versus the impact approach in the context of personal data protection on social platforms by Xue (2022). In the study, 25 experts in law and policy were interviewed to ascertain the efficacy of the human rights approach versus the impact approach in the context of personal data protection on social platforms in the UK and China. The results revealed that both approaches were ineffective in the context of developing an economic remedy for damages resulting from the misuse of personal data, while there were effective mechanisms in place to protect personal rights in both approaches.

The need to ensure the involvement of all stakeholders in the development and implementation of new data protection legislation, as evidenced in the Indonesian case, is further emphasized by Lihawa (2025). Through the use of qualitative content analysis, the study has identified gaps in resources, awareness, and the harmonization of international platforms and national legislation, thus advocating for more effective legal education and oversight, as well as the harmonization of legislation to ensure the effectiveness of data protection legislation (Lihawa, 2025).

Another area in the development and implementation of data protection legislation, as an international best practice, is technological innovation. According to Yang (2025), as well as Jayaprabha and Jacob (2025), technological innovation has the potential to increase the level of privacy for citizens. However, this can only be achieved through the development and implementation of appropriate legislation, as emphasized by Yang (2025), as well as the development and implementation of appropriate educational programs, as emphasized by Jayaprabha and Jacob (2025).

Another area in the development and implementation of data protection legislation, as an international best practice, is the development and implementation of educational programs. According to Peter and Ndinojuo (2024), educational programs have the potential to increase the level of user awareness. This is evidenced by the study carried out in Nigeria, in which 396 students took part, indicating that although the users are proactive in protecting their data, the effectiveness of the data protection strategies can be enhanced through the development and implementation of appropriate educational programs (Peter & Ndinojuo, 2024). In the case of Zimbabwe, this would imply the development and implementation of an interdisciplinary approach to data protection, as well as the development and implementation of appropriate legal and technological tools to ensure the effectiveness of data protection strategies.

2.4 Empirical Review

Aras Alkis & Tekin Kose, 2022, "Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe", Europe

A significant empirical study focusing on the privacy-related concerns and behaviors regarding social media and e-commerce in Europe is provided by Alkis & Kose (2022). This study used a large sample consisting of 153,053 respondents across 29 European nations. This is considered one of the biggest sample sizes used in this subject area. In terms of methodological approaches, the researchers used a multilevel logit model that allowed for in-depth analysis of individual and country-related factors concerning e-commerce restrictions and the effect of social media advertisements on e-commerce behavior. The overall study design used a series of scales that were mainly centered around risks related to data exposure in online settings, sharing of information in online settings, data privacy principles, and recordable activity in online settings.

The results show that awareness of the risks related to online privacy is positively related to the willingness to engage in e-commerce, as well as information-sharing activities online. On the other hand, the results show that heightened concern regarding the recording of online activities is negatively related to the willingness to engage in e-commerce. Notably, the results show that individuals who take precautionary measures to mitigate the risks related to online privacy are more likely to engage in e-commerce sites, as well as be more sensitive to online social media advertisements. The policy implications show that firms that provide effective mechanisms to protect consumer online privacy can capitalize on the high levels of consumer trust, willingness to engage in e-commerce, and the effectiveness of online advertising.

The study's methodological approach is also significant, whereby the large sample size, coupled with the sophistication of the statistical analyses, provides high levels of external validity, thereby allowing the researchers to generalize the results to the broader European market. The study also provides significant implications regarding the importance of considering the dual nature of individualism and systemism in the study of behavioral outcomes related to attitudes towards online privacy. The study also provides significant implications for firms, thereby warranting further research on the effectiveness of particular tools to protect consumer online privacy, as well as the impact of changes to consumer trust levels, including the GDPR, over long periods of time, as recommended by the researchers (Alkis & Kose, 2022).

Dmitry Epstein & Kelly Quinn, 2020, "Markers of Online Privacy Marginalization: Empirical Examination of Socioeconomic Disparities in Social Media Privacy Attitudes, Literacy, and Behavior", United States

Epstein and Quinn (2020) carried out a study to investigate the link between socioeconomic characteristics and online privacy behavior among social media users in the United States. In their investigation, they used a representative sample of 689 participants whose mean age was 46.9 years. In terms of gender distribution, 55.2% of the participants were female, while 44.4% were male. In terms of race, 8.7% of the participants were African American, 7.8% were Hispanic/Latino American, 4.7% were Asian, and 82.8% were Caucasian.

The researchers used hierarchical linear regression to examine the link between digital divide measures, privacy concerns, protective privacy behavior (PPBs), and privacy leadership (PL). The results showed that privacy literacy is a critical aspect that is not adequately addressed in the study of digital divide. Despite their high level of engagement in social media activities, where 93.1% used two or more social media platforms and 84.9% used their primary social media platform every day, there was a significant divide in the use of PPBs. In their study, it was found that socioeconomic status, educational level, and digital competency predicted privacy concerns and the use of PPBs such as adjusting privacy settings and controlling information sharing. However, Horizontal Privacy Protective Behaviors (HPBs), which are used as a protective mechanism against social incursions, and Vertical Privacy Protective Behaviors (VPBs), which protect individuals from institutional actors such as sponsors, are not as common among marginalized social groups.

The study used a wide survey to examine structural and experiential factors, privacy concerns, and protective behavior. The use of a wide survey provided a rich and nuanced view of both traditional and new forms of marginalization. The study is significant in that it provides a deeper understanding of issues surrounding privacy literacy and the need to address it to reduce marginalization between socioeconomically disadvantaged social groups. The researchers recommend that future studies be conducted to enhance privacy literacy skills and to ensure that privacy education is accessible to reduce marginalization in online capabilities (Epstein & Quinn, 2020).

Victoria I. Marín, J. Carpenter, G. Tur, Sandra Williamson-Leadley, 2022, "Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers", Germany, New Zealand, Spain, USA

An international comparative cross-sectional study was carried out by Marín et al. (2022) to explore the pre-service teachers' views about the use of social networking sites and data protection in a school setting. The study was based on a sample of 225 participants recruited through universities in Germany, New Zealand, Spain, and the United States. The researchers aimed to include at least 26 participants from each of the countries. The data was collected through an online structured survey with quantitative questions using a Likert scale. The study also included optional open-ended questions. Quantitative data was analysed through descriptive statistics, Kruskal-Wallis H tests for intergroup comparisons, and chi-square tests for categorical data.

The study revealed that although the pre-service teachers were aware of the educational value of social networking sites, the concerns about data protection were also evident. The overall lack of understanding of data protection was evident among the pre-service teachers, although the level of understanding was also seen to differ across the countries. Interestingly, the level of concern was seen to be high among the pre-service teachers in Germany compared to the United States and New Zealand. The study reveals the importance of legal, cultural, and conceptual factors in data protection among the participants of the study.

From the methodological point of view, the transnational comparative study with the use of quantitative and qualitative data provides a comprehensive understanding of the pre-service teachers' views about data privacy risks in the context of shaping the educational trajectories of the future. The study highlights the importance of data privacy awareness and digital literacy among the pre-service teachers. The study was based on convenience sampling, but the authors of the study argue that the study provides significant implications for policy. The study suggests the importance of training pre-service teachers about data privacy awareness and digital literacy at the national level.

E. Di Minin, Christoph Fink, A. Hausmann, Jens Kremer, Ritwik Kulkarni, 2021, "How to address data privacy concerns when using social media data in conservation science", European Union

In their work, "Using Social Media Data in Conservation Science: Legal and Ethical Challenges in the European Union under the General Data Protection Regulation," Di Minin et al. (2021) explore the legal and ethical challenges associated with using social media data in the field of conservation science, specifically in relation to the General Data Protection Regulation in the European Union. Through their series of case studies, the authors discuss various conservation projects that rely on publicly available data from social media platforms such as Twitter, Facebook, and Instagram. While the total number of projects and data sets is not specified, the authors rely on a wide range of empirical cases, such as the exploration of human interfaces in the environment and the detection of illegal wildlife trade via the Internet.

The results of their work reveal that using social media data is associated with significant risks that may lead to the identification of users, which in turn may lead to mental and physical harm. The authors emphasize the importance of using such data with extreme caution and recommend that data collection should be minimized, data sets should be anonymized, and data handling practices should be implemented and adhered to. They also recommend the use of privacy impact assessments to minimize risks and ensure that data protection regulations are adhered to. For instance, the authors cite the anonymization of geotagged photographs to avoid the identification of endangered species and obtaining user consent when data is collected directly from users.

Using legal scholarship and empirical cases from conservation science, the authors were able to derive some recommendations for conservation scientists in their work. They argue that using social media data in the field of conservation science is dependent on the balance between scientific goals and protecting private attributes, specifically in the European Union, which is characterized by strict data protection regulations. They also recommend that further studies should be conducted to evaluate these recommendations and that standards should be established in the field of conservation science in handling data responsibly.

5. Mubarak Raji, Damilola Wilder, Victor Ugwuoke, Muhammad N. Bashir, 2025, "An assessment of the enforcement mechanisms in African data protection laws", Africa (20 Countries)

Raji et al. (2025) is a wide-ranging qualitative study of the various enforcement mechanisms within the context of data protection regulations in twenty different African countries. Three researchers

worked together to conduct the study, examining publicly available data protection legislation in the respective countries, with the study focusing primarily on the enforcement, penalty, and data protection authority sections within the legislation. Although no individual survey was conducted, the study is based on the examination of legal documentation and enforcement records in various countries, providing a wide-ranging perspective on the current state of data protection in the African context.

According to the study, all twenty countries have legislation in place requiring the establishment of a dedicated data protection authority, with legislation addressing the context in the public and private sectors. Additionally, the study found that 85% of the countries have legislation in place providing for the imposition of administrative penalties in the context of privacy infringement, with all countries having legislation in place providing for the imposition of monetary and criminal penalties. Furthermore, 65% of the countries have legislation in place providing for the right of action in the context of privacy infringement, with all countries requiring data controllers to notify the authority prior to processing any data. Additionally, the study found that 55% of the countries have legislation in place providing for the extraterritorial effect of the legislation, with the study concluding that although the legal frameworks in the respective countries are in place, significant challenges remain in the context of enforcement.

In the context of the study's methodology, thematic content analysis is used to identify the various trends in the context of the study, with the study concluding that although the legal frameworks in the respective countries are becoming more cohesive in the context of data protection, significant challenges remain in the context of enforcement, with the study concluding that harmonisation of policies in the respective regions, as well as investment in the enforcement context, are required to increase the effectiveness of the legislation in the respective countries (Raji et al., 2025).

2.5 The Zimbabwean Context

2.5.1 Social Media Usage Trends in Zimbabwe

Recent empirical research has also offered concrete examples of the use of social media by the Zimbabwean people. In a descriptive study, Matema et al. (2024) used a face-to-face interview

survey of 384 mobile phone users in the Harare province, aged 18-64, with the study focusing on Econet, NetOne, and Telecel users. From the study, it is evident that 2.05 million Zimbabweans use social media actively, with the primary reasons being the need to access news and updates, advertising, social interaction, and political activism. From the study, it is also evident that demographic factors play an important role in the use of social media in Zimbabwe, with males and the 18-25 age group showing a higher perception of the potential influence of social media than the rest of the Zimbabwean population. Additionally, the study showed that people with secondary education have a higher perception of the usefulness of social media than degree holders. Other important findings from the study showed that employment status and income were significant factors in the use of social media, with the study showing noteworthy associations with people who were employed and had an income of 3,001-4,000 currency units.

In another study, Martin et al. (2024) used a cross-sectional study of 17,636 youths aged 18-24 years in the Harare, Mashonaland East, and Bulawayo provinces of Zimbabwe. From the study, it is evident that 92.8% of the Zimbabwean population has access to mobile phones, with 87.6% of the population owning the mobile phones. Out of the people with mobile phone access, 58.6% use the internet, with 57.8% of the people with mobile phone access also using social media weekly. From the study, it is evident that social media use is significantly related to the socioeconomic status of the Zimbabwean people, with people who have attained tertiary education being more than eight times as likely as people with primary education to have mobile phones, as cited in Martin et al. (2024).

2.5.2 Zimbabwe's Legal and Regulatory Framework for Data Protection

Zimbabwe's Data Protection Act [Chapter 11:12] is the country's first comprehensive legislation that deals with data protection in both the public and private sectors. The Act established a data protection authority and outlined the responsibilities of data controllers. Mutiro and Saki (2024) offer a critical discussion on the Act. The authors highlight that the Act establishes a right to privacy but that the provisions of the Act are largely influenced by the government's focus on cyber security rather than data protection. The Act also established a broad definition of "data," which includes any representation of facts, concepts, or information in digital form. The Act also established specific requirements for data quality, accessibility, lawfulness, fairness, transparency, consent, purpose limitation, data minimization, accuracy, storage limitation, disclosure, security,

and accountability. The Act also distinguishes between sensitive and non-sensitive data and establishes genetic data, biometric data, and health data as specific types of data that require specific consent. The Act also requires data controllers to evaluate the adequacy of protection in other countries before transferring data to other countries. The Act requires consideration of the nature of the data to be transferred, the purposes for which it will be processed, and the level of security. However, it is argued that the Act's focus on cyber security undermines the right to privacy. The Act's effectiveness is also undermined by the limited resources and the need to comply with regional and international regulations.

2.5.3 Customer Perceptions and Privacy Concerns in Zimbabwe

However, there is a lack of research on the awareness and attitudes of Zimbabweans regarding digital privacy. Ncube (2016) situates the discourse in a social context of distrust regarding data processing. This is attributed to experiences of monitoring and criminal activities. The study found that there is a general lack of knowledge regarding the legislative framework. The study found that the legislative framework does not offer enough public assurance. However, Matema et al. (2024) found that there is a restricted understanding of the risks associated with digital privacy and rights to data protection. The study surveyed social media users and found that there is a variation in the perceived influence of social media usage among different demographic groups. However, it did not measure the perception of digital privacy.

Martin et al. (2024) found that mobile phone usage is almost ubiquitous among youth. However, more than one-third of the youth do not have regular access to the internet and social media. The main reason for this is that it is too expensive. The findings show a clear relationship between digital literacy and awareness of digital privacy and socioeconomic status. The findings show that those who are better off and better educated have the capacity to deal with digital privacy.

2.6 Gaps in Existing Literature

Academic research on social media data privacy, user perceptions, and regulatory responses is an emerging field of study with rapid growth in various parts of the world, including Europe, North America, Asia, and Africa. Research has explored privacy-related issues, user perceptions, the

effectiveness of privacy policies, and the implications of prominent frameworks, including the GDPR in Europe. Additionally, surveys have identified various dimensions of user privacy perceptions, the influence of demographic and cultural factors, and the phenomenon of the "privacy paradox," whereby users are concerned about privacy but rarely take steps to protect their privacy (Aliu et al., 2024). Other research has also explored the influence of mobile platform configurations of trust and security, as well as the influence of service quality on user satisfaction and loyalty (Yum & Yoo, 2023).

In the African context, research has recently explored the broader field of data protection legislation, user perceptions, and determinants of social media usage among Zimbabwean mobile users (Matema et al., 2024). However, there is a significant knowledge gap in the literature, as no, or little, research has empirically explored the perceptions of mobile network users in Zimbabwe, including users of state-owned enterprises such as NetOne, with regard to data privacy. Most of the literature is based on demographic usage patterns, with little or no research addressing the privacy concerns, perceptions, or behavior of mobile users in Zimbabwe in relation to national legislation and the unique circumstances of state-owned enterprises in the country.

In addition, research carried out in various nations, such as Nigeria, has also examined user perceptions of data privacy threats, although such research rarely yields frameworks that can be easily applied or adapted to specific contexts (Aliu et al., 2024). On a global scale, there is a pressing need for transparent, ethical, and user-centered privacy policies, although little attention has thus far been paid to the operationalization of such recommendations in Zimbabwe's specific legal and organizational context (Marín et al., 2022).

NetOne and similar organizations face specific challenges in seeking a balance between government regulations, civic responsibilities, and business viability in light of increasing data privacy threats fueled by high levels of mobile data usage. While the literature demonstrates a high level of interest in data privacy issues surrounding social media, it is also noteworthy that this significant body of work fails to specifically examine Zimbabwean mobile users and NetOne. The proposed research aims to contribute to this body of work by demonstrating its ability to bridge this specific research gap and develop a workable framework.

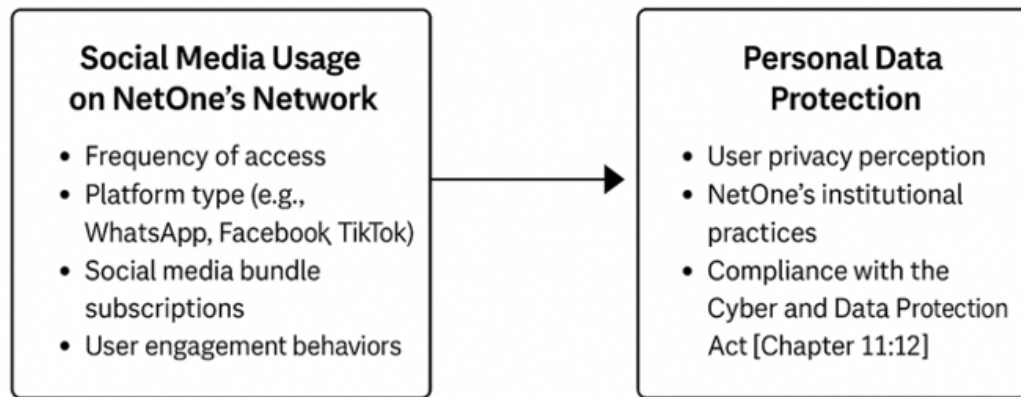
2.7 Conceptual Framework

An elaborate conceptual framework is necessary to explain the relationship between social media use, privacy perceptions, and trust, and their combined impact on NetOne customers' personal data protection. The conceptual framework shown in Figure 2.1 illustrates that social media use affects personal data protection. Frequent social media use can lead to heightened perceptions of privacy risks, data protection regulations, and trust in one's mobile network operator, which can influence attitudes and behaviors towards personal data protection. For this research, personal data protection is considered a dependent variable, which is further broken down into perceived protection, willingness to disclose information, and privacy protection practices. On the other hand, digital literacy, age, and educational level are considered as moderating and/or mediating variables, which can enhance or reduce the relationships between social media use and personal data protection outcomes.

Figure 2.1: Conceptual Framework

Independent Variable

Dependent Variable



Source: Adapted by the researcher, 2026

2.8 Chapter Summary

This chapter evaluated the relevant literature on data privacy issues in social media sites, focusing on issues of prevalent data privacy concerns, the dynamics of changing data protection strategies over time, and the possible impact of user awareness and trust. However, there is a clear gap in the literature regarding the specific perceptions and behaviors of NetOne customers in Zimbabwe, especially considering the context of a state-owned enterprise. The conceptual framework for this study will seek to address this gap by conducting an empirical study on these issues. The discussion on these issues will be continued in the next chapter, which will focus on the methodologies that were adopted to achieve the research objectives.

CHAPTER 3

METHODOLOGY

3.0 Introduction

The present chapter presents an outline of the methodological framework that underlies the study on the relationship that exists between social media and personal data protection in Zimbabwe, with specific emphasis on NetOne Zimbabwe. Specifically, it presents an explication of the philosophical foundations, research paradigm, design, target population, sampling strategy, data collection instruments, analysis, and ethics of the study. Given the multi-dimensional and context-specific nature of personal data protection in a mobile-driven social media setting, a mixed-methods design was used to elicit quantitatively measurable and qualitatively rich data. The methods used were rigorously matched with the objectives of the study to ensure methodological rigor, credibility, and relevance.

3.1 Research Philosophy

The study was underpinned by a pragmatic research philosophy that recognises that complex social realities are not comprehensible within one epistemological and ontological framework. The pragmatic approach emphasises the research problem and endorses the use of various methods that are more likely to solve real problems (Creswell & Plano Clark, 2018). In this study, the relationship between social media usage and personal data protection involved observable social behavior and subjective institutional practices that could not be comprehended within one methodological paradigm.

The pragmatic approach helped to combine the quantitative findings from the NetOne subscribers with the qualitative findings from the key institutional stakeholders. Quantitative findings provided objective information on awareness levels, perceptions of privacy risks, and trust in NetOne's data handling practices, while qualitative findings provided insights into institutional practices and implementation issues. By adopting the pragmatic approach, the study remained flexible and problem-centred and remained outcome-orientated to ensure that the findings were empirically

informed and practically relevant to the context of Zimbabwe's telecommunications and data protection environment.

3.2 Research Paradigm

The present research design is underpinned by a mixed methods approach, which integrates positivist and interpretivist theoretical underpinnings. The positivist approach underpins the quantitative research, which assumes that perceptions of data privacy, level of awareness, and trust can be measured, quantified, and statistically analysed. Consequently, structured questionnaires and statistical tools are employed to establish patterns and relationships between variables.

In this regard, the interpretivist approach underpins the qualitative research, which seeks to establish meanings, interpretations, and experiences surrounding personal data protection. Through semi-structured interviews, this research explores how NetOne officials and regulators view and interpret regulatory compliance, data governance, and the impact of social media engagement on personal data protection. The integration of both theoretical approaches enables this research to transcend quantitative trends and provide insight into the nuances of personal data protection in Zimbabwe's telecommunication sector.

3.3 Research Design

A convergent parallel mixed methods research design was employed for this study. This research design involved the collection of both quantitative and qualitative data and their subsequent interpretation to obtain a comprehensive understanding of the research problem (Creswell & Plano Clark, 2018). The research design was particularly suitable for this study since it allowed for a comparison of the perceptions of subscribers and the institution within a single time frame.

The quantitative research involved the administration of a structured questionnaire to NetOne subscribers who operated within the Central Business District of Harare. The use of a structured questionnaire allowed for the collection of standardised data on the awareness of data protection rights, perceived risks to their privacy when engaging in social media use, and trust in NetOne's data handling practices. The qualitative research involved the use of semi-structured interviews

for NetOne staff and other key stakeholders, such as officials from the Postal and Telecommunications Regulatory Authority of Zimbabwe and the Data Protection Authority.

3.4 Target Population

The study focused on two distinct but related populations. The first population targeted by the study included NetOne subscribers who lived or worked in the Central Business District of Harare and used NetOne's social media data bundles. The reason for selecting this population is that urban residents use the Internet and social media services more than any other population in Zimbabwe and hence would be more vulnerable to data privacy risks.

The other population targeted by the study included the key informants from NetOne Zimbabwe in the compliance, data governance, and customer care departments, as well as POTRAZ and Data Protection Authority representatives. The reason for selecting this population is that they have played an active role in the formulation, implementation, and monitoring of data protection policies in the country. According to POTRAZ (2023), NetOne had approximately 4.1 million subscribers in the country, with the majority of the subscribers residing in the urban area of Harare. For the sake of accessibility and feasibility, the accessible population was restricted to 172 adult subscribers aged 18 years and above in the central business district of Harare.

3.5 Sample Size Determination

The sample size for the quantitative study was established by applying Yamane's (1967) formula for calculating sample size for a finite population. The formula for calculating sample size for a finite population is:

$$n = N / (1 + N e^2)$$

where:

e = margin of error = 0.05,

N = population size = 172.

$$e^2 = 0.0025$$

$$1 + N e^2 = 1 + 172 \times 0.0025 = 1 + 0.43 = 1.43$$

$$n = 172 / 1.43$$

$$n = 120.28$$

$$n = 120$$

This is an estimate of the population size, denoted as $n \approx 120$, which is then approximated to 120 for practical reasons. In the formula, n refers to the sample size, N refers to the population size, and e is the predetermined level of precision, which is set at 0.09 in this study. Using Yamane's formula with an estimate of the accessible population being approximately 172 active NetOne subscribers in the Harare CBD, the study found the sample size to be approximately 120 respondents, which is deemed large enough to produce statistically significant results within the constraints of the study.

In the study, twelve key informants were also purposively selected for the qualitative study, deemed large enough to produce data saturation, whereby no further thematic information is likely to be obtained from further respondents. This combination of the statistically derived quantitative study with the purposively selected qualitative study is deemed to add rigor to the study as a whole.

3.6 Sampling Methods

A stratified random sampling method was adopted to sample NetOne subscribers for the quantitative study. The respondents were divided into strata on the basis of age groups and gender to address the issues of bias. Random sampling was adopted for respondents within the strata to generalise the results. For the qualitative study, purposive sampling was adopted to sample respondents who had expertise and knowledge regarding data protection and telecommunication

regulations. The respondents were sampled to ensure that the results were rich and relevant to the institutional aspects of the research objectives.

3.7 Research Instruments

Two research instruments were adopted to obtain the needed data. The instruments were designed to address both user-level and organizational-level aspects of personal data protection in the context of social media use.

3.7.1 Questionnaire

A structured questionnaire was designed and administered to NetOne subscribers. The research instrument had clearly articulated sections for demographic factors, social media use habits, knowledge of personal data protection rights, perceptions of risks to their personal data privacy, and trust in NetOne's data management practices. Likert scales were incorporated to measure the strength of respondents' attitudes and perceptions on the subject matter. The research instrument was designed based on constructs from existing literature on data privacy. To ensure clarity and relevance to the research subject matter, the research instrument was reviewed and slightly modified by both academic and professional supervisors from information systems and data protection backgrounds.

3.7.2 Interview Guide

A semi-structured interview guide was designed for the qualitative research. The interview guide had a number of open-ended questions that allowed for a detailed engagement with key informants. The questions focused on organisational data management and protection practices, compliance with the Data Protection Act, organisational data management practices, challenges arising from social media use in data management and protection, and perceptions of subscribers' awareness of data protection rights. The flexibility of the interview guide allowed for a detailed and comparable research process.

3.8 Data Collection Procedures

Data collection was done over a period of four weeks, which helped ensure the consistent engagement of the participants. For the quantitative part, questionnaires were used. The questionnaires were given and picked up personally within the Harare CBD, specifically targeting NetOne subscribers who were actively using mobile internet and social media services. Research assistants were used in this process, and they helped in clarifying issues as necessary, though not affecting the actual response given by the participants.

Before participating, the participants were made aware of the reason for participating, and their confidentiality was ensured. They were asked to give their consent before participating. The filled-out questionnaires were checked on site, which helped reduce missing information. This was beneficial in ensuring the quality and appropriateness of data for statistical analysis.

In collecting qualitative data, semi-structured interviews were conducted. The participants included NetOne officials and other relevant stakeholders. The interviews were conducted when and where it was most convenient for the participants. Interviews were conducted either at the organisation's offices or online. With the participants' consent, audio recording was done. This helped ensure accuracy in transcription. Additional information was recorded, which was relevant and useful in interpreting the data.

3.9 Data Presentation and Analysis Methods

3.9.1 Quantitative Analysis

Quantitative data collected through questionnaires was coded and entered into Statistical Package for Social Sciences (SPSS) for analysis. Data screening was carried out to identify errors, inconsistencies, or missing values, which were corrected accordingly. Quantitative data analysis methods, including frequencies, percentages, means, and standard deviation, were used to analyse demographic characteristics, social media usage, and personal data protection rights of NetOne subscribers.

Inferential statistics were used to investigate relationships that exist among variables of interest. Chi-square analysis was used to determine relationships that exist between demographic characteristics and personal data protection rights. Correlation analysis was used to determine the strength of relationships that exist between social media usage intensity and perceptions of personal data protection risks. Multiple regression analysis was used to determine the extent to which social media usage variables predicted perceptions of personal data protection rights and trust in NetOne's data handling practices.

3.9.2 Qualitative Analysis

The qualitative data was fully transcribed, and thematic analysis was conducted using NVivo. The process of analysing qualitative data was systematic and iterative, starting from familiarization and coding. The codes generated from this process were further grouped under categories and themes, mainly related to compliance, institutional issues, regulations, and organizational perspectives on data protection. The qualitative data was combined with quantitative data during interpretation, which provided a holistic view of the research problem.

3.10 Reliability, Validity, and Trustworthiness

3.10.1 Quantitative Strand

In the quantitative study, the use of validity and reliability ensured the accuracy and consistency of the research instruments and the research findings. Content validity was achieved through the use of the research objectives and the literature on personal data protection and social media usage as guidelines for the questionnaire. The research instrument was reviewed by subject-matter experts to ensure it measured the research constructs appropriately.

Reliability was determined using internal consistency reliability measures, where Cronbach's alpha coefficients for multi-item scales were used. The reliability threshold was set at 0.70 or higher for social science research, which indicates the research instrument was reliable and consistent in the research findings (Bryman, 2016). The use of reliability and validity measures ensured the credibility of the research findings.

3.10.2 Qualitative Strand

However, since validity and reliability are not applicable to qualitative research, rigor for the qualitative research strand was established on the concept of trustworthiness as defined by Lincoln and Guba (1985). The trustworthiness of the study was achieved through four main criteria: credibility, dependability, confirmability, and transferability. The study's credibility was achieved through prolonged engagement with the respondents and the use of a probing interview style to obtain rich and in-depth information on NetOne's data protection. In some cases, member checking was also employed to allow respondents to check and confirm the accuracy of the information provided.

The study's dependability was achieved by providing a clear audit trail that allows other researchers to track the research process. This ensures that other researchers can replicate the study and follow the logic of the research. Confirmability was achieved by reducing researcher bias through journaling and relying on the respondents' narratives to inform the findings. Finally, the study's transferability was achieved by providing thick descriptions that allow the reader to evaluate the study's generalizability to other telecommunications settings or developing country contexts.

3.11 Ethical Considerations

The research process adhered to the highest standards of ethics. Participants were provided with in-depth information regarding the purpose of the research, the voluntary nature of the study, and the right to withdraw from the study at any time. Confidentiality and anonymity were ensured by omitting personally identifiable information in the study's outputs. Data storage was ensured through the use of password-protected devices in accordance with Zimbabwe's Data Protection Act [Chapter 11:12]. Ethical clearance was obtained from the appropriate university ethics committee before the start of the fieldwork.

3.12 Chapter Summary

This chapter discussed the methodological approach adopted in the study, including the underlying philosophy and paradigm of the study, its design and population, sampling method and procedure,

instruments of data collection, and the methods of analysis and ethics of the study. The mixed-methods approach, guided by a pragmatic philosophy of inquiry, offers a comprehensive and believable examination of the relationship between social media and personal data protection in Zimbabwe. The findings of the study are presented and analysed in the following chapter.

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1 Introduction

The chapter presents, analyses, and discusses the findings of the study. It is divided into two main sections. In the first section, the analysis of the results is presented, including the results obtained from the questionnaire survey among the NetOne subscribers. In the second section, the findings are discussed, interpreting the results in light of the objectives, hypotheses, and the literature review discussed in Chapter Two. In the analysis, descriptive statistics, reliability analysis (Cronbach Alpha), correlation analysis, and regression analysis are employed, as indicated by the objectives and hypotheses. In this chapter, the reconstructed tables are included, whereas the original statistical outputs are assumed to be found in the appendices, as is the norm in academic writing.

4.2 Questionnaire Response Rate

Out of the 120 distributed questionnaires, 97 were completed and returned, giving a response rate of 80.8%. This response rate is considered highly satisfactory in the social sciences. As mentioned earlier, a response rate of 50% is considered adequate for data analysis and reporting. Response rates of 70% and above are considered "very good." Hence, the response rate of 80.8% is excellent and indicates good internal validity. Table 4.1 below shows the rate of returning the questionnaire.

Table 4.1 Questionnaire Response Rate

Category	Frequency	Percentage
Questionnaires distributed	120	100%
Questionnaires completed & returned	97	80.8%

Source: Primary data, 2026

4.3 Reliability Analysis

Before delving into the actual findings, it was critical to assess the internal consistency of the scales used in the questionnaire. Cronbach's Alpha test was carried out on each construct of the four research objectives.

Table 4.2: Reliability Statistics (Cronbach's Alpha)

Construct	Number of Items	Cronbach's Alpha
Perceptions of Personal Data Privacy	4	0.842
Impact of Social Media on Data Protection	4	0.876
Challenges in Data Protection Implementation	4	0.791
Best Practices for Enhancing Data Protection	4	0.888
Overall Instrument Reliability	16	0.913

The findings indicate a strong level of internal consistency in all the constructs measured in the study. The range of the Cronbach's alpha coefficient extends from 0.791 to 0.888, while the overall reliability coefficient is 0.913. In line with methodological standards, if the value of the alpha coefficient is higher than 0.70, it indicates acceptable levels of reliability, while a value higher than 0.80 indicates good levels of reliability, and a value higher than 0.90 indicates excellent levels of reliability. Thus, the instrument used in this study has high levels of reliability and can be used for further inferential analysis.

Similar to the findings of Hair et al. (2022), a value of 0.70 or higher for the Cronbach's alpha coefficient indicates acceptable levels of reliability, while a value of 0.80 or higher indicates strong levels of reliability. The strong levels of reliability indicate that the respondents understood the instrument consistently and that the constructs measured, such as privacy concerns, perception of data protection, regulation, and best practice, are conceptually sound.

4.4 Demographic Profile of Respondents

Demographic statistics were merged into a solo summary table in acquiescence with the research procedures.

Table 4.3: Demographic Characteristics of Respondents (n = 97)

Variable	Category	Frequency	Percentage (%)
Gender	Male	53	54.6
	Female	40	41.2
	Prefer not to say	4	4.1
Age Group	18–25	31	32.0
	26–35	38	39.2
	36–45	18	18.6
	46–55	7	7.2
	56+	3	3.0
Education Level	Secondary	15	15.5
	Diploma	24	24.7
	Degree	42	43.3
	Postgraduate	16	16.5
Duration as NetOne Subscriber	< 1 year	8	8.2
	1–3 years	29	29.9
	4–6 years	33	34.0
	> 6 years	27	27.8
Main Social Media Platform(s) Used on NetOne*	WhatsApp	38	39.2
	Facebook	24	24.7
	TikTok	17	17.5
	X (Twitter)	11	11.3
	Instagram	7	7.2

Source: Primary data, 2026

4.4.1 Gender

The gender dispersal of the respondents is clearly illustrated in Figure 4.1.

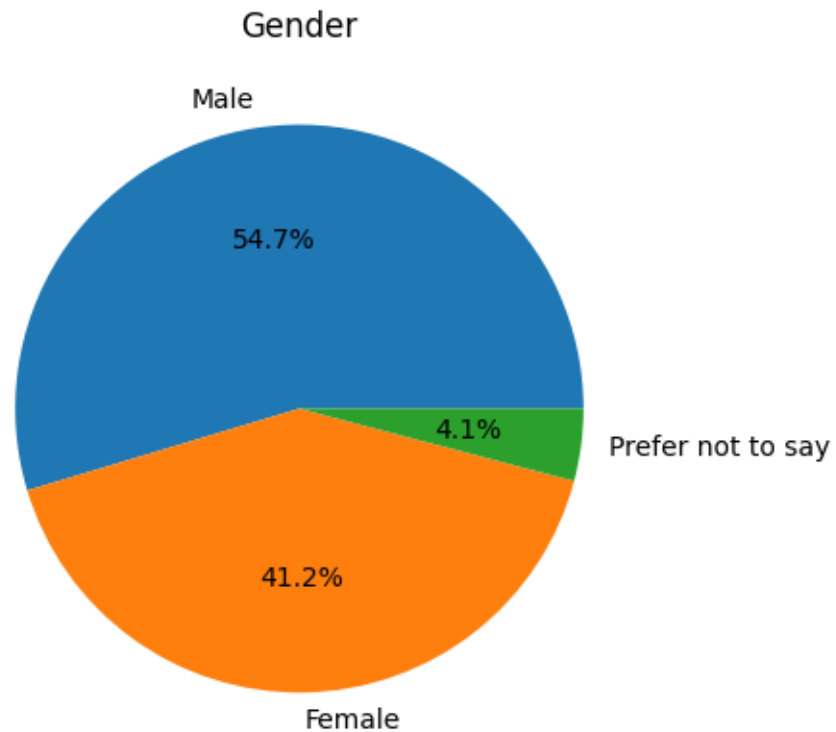


Figure 4.1: Gender Distribution

The sample demonstrates a slight majority in favor of males (54.6%) compared to females (41.2%), with a small percentage choosing not to disclose their gender (4.1%). This balanced sample increases the credibility of this study, as there is no bias in the perception of individual data protection based on gender. Recent research has shown that gender plays a key role in digital risk perception, with females showing higher levels of concern regarding privacy compared to males, particularly in cases of harassment, identity theft, and surveillance (Chen et al., 2024). On the other hand, males have shown higher confidence in using digital technologies but have a tendency to underestimate certain risks regarding privacy (Yang, 2025).

4.4.2 Age Group

The age cluster of the respondents is shown in Figure 4.2.

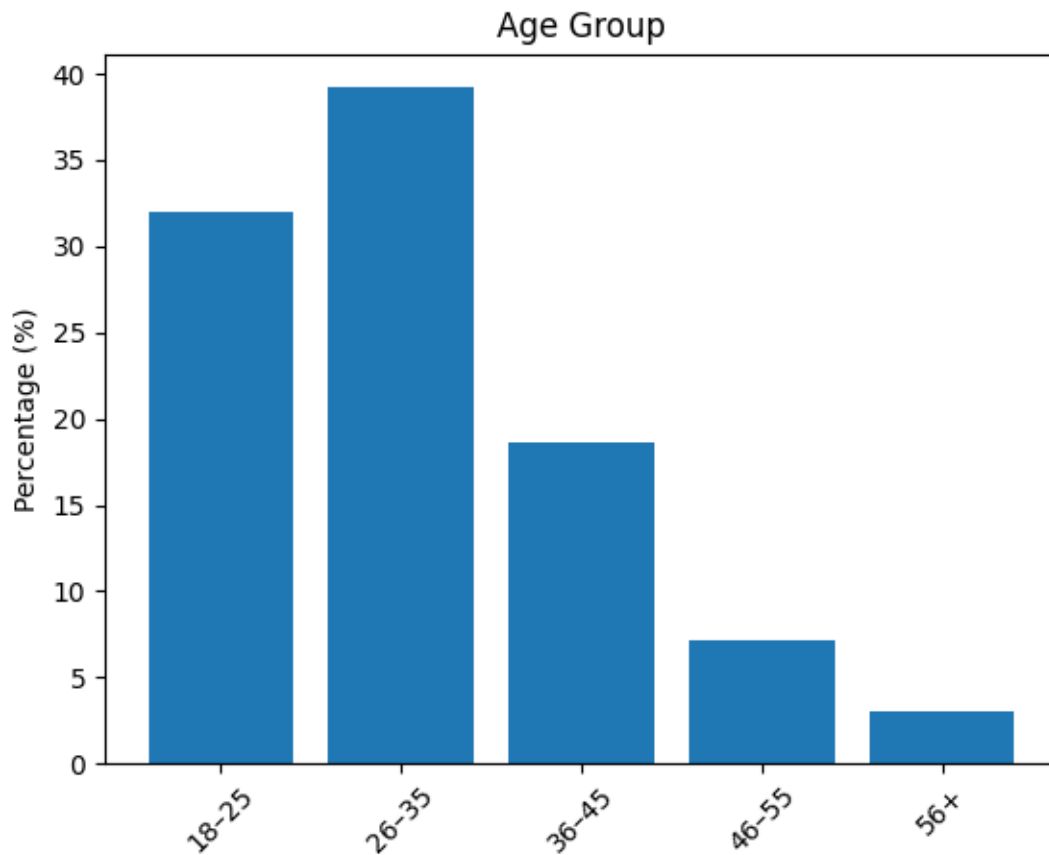


Figure 4.2: Age Group

The sample population appears to be largely in the age range of 18-35 years, with the largest subset of the population in the range of 26-35 years. This is consistent with the global trend in the use of social media, where the younger age groups are the largest users of mobile data services. In a study conducted by Jain et al. (2025), it has been found that the younger age groups are more exposed to digital technologies and are more aware of the algorithmic systems used to monitor their behavior, which increases their level of awareness about the risks of privacy. At the same time, the younger age groups are also the ones who are most embedded in the social media ecosystem, driven by their social, professional, and economic dependencies. This is of critical importance in

the context of the present study, as it reflects the notion of a heightened level of concern about privacy based not on perceptual constructs, but actual experience.

4.4.3 Education Level

The educational qualifications of the respondents are illustrated in Figure 4.3.

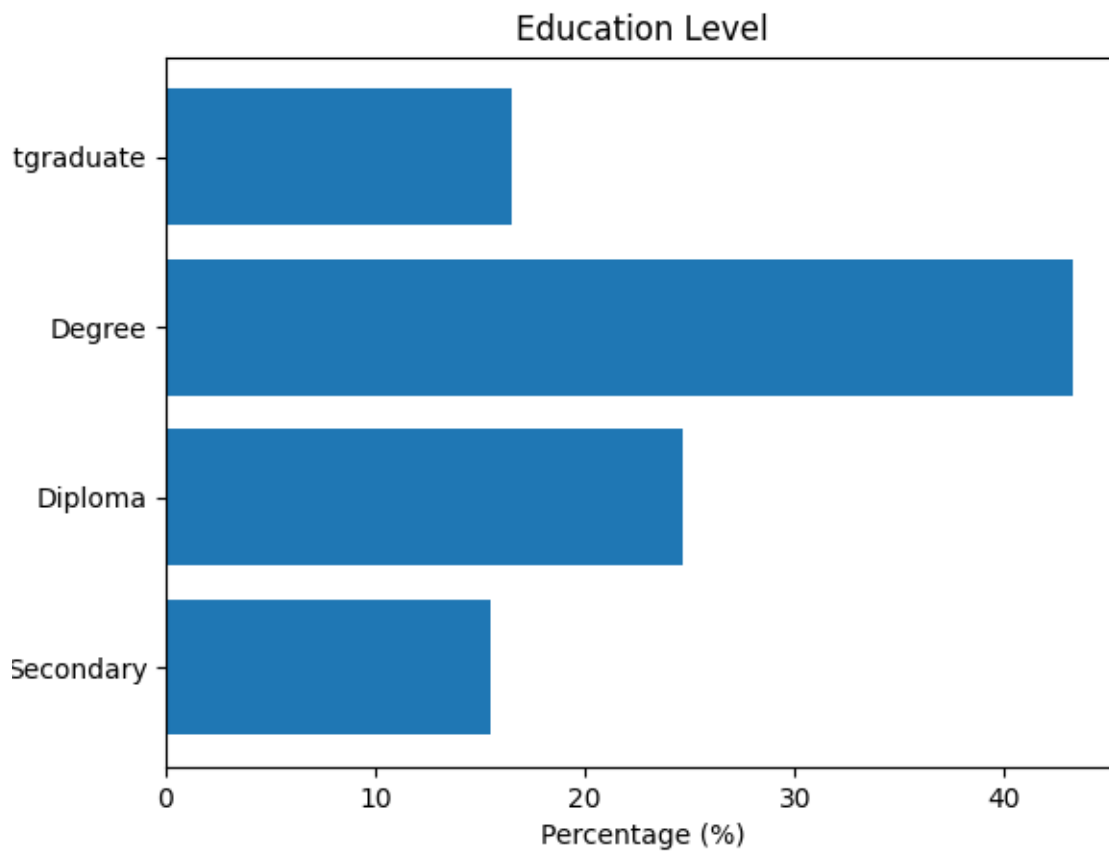


Figure 4.3: Level of Education

The results show that 59.8% of the respondents have at least a university degree, while 15.5% have a secondary level of education. Such educational attainments suggest that the respondents are digitally literate and capable of analytical thinking. Education has consistently been linked to digital literacy, understanding of the regulatory frameworks, and the ability to scrutinise the practices of institutions (Epstein & Quinn, 2020). Such groups of people are likely to understand the implications of data harvesting, metadata analysis, and cross-border data transfers. Therefore,

their skepticism towards the sufficiency of the data protection measures, as revealed in the descriptive results, may not be based on a lack of understanding but rather on their informed assessment of the issue. According to Büyük (2024), the educational level of people can be linked to their understanding and interpretation of privacy policies, especially in situations where the policies are complex.

4.4.4 Duration as NetOne Subscriber

The NetOne subscribers experience is clearly shown in Figure 4.4.

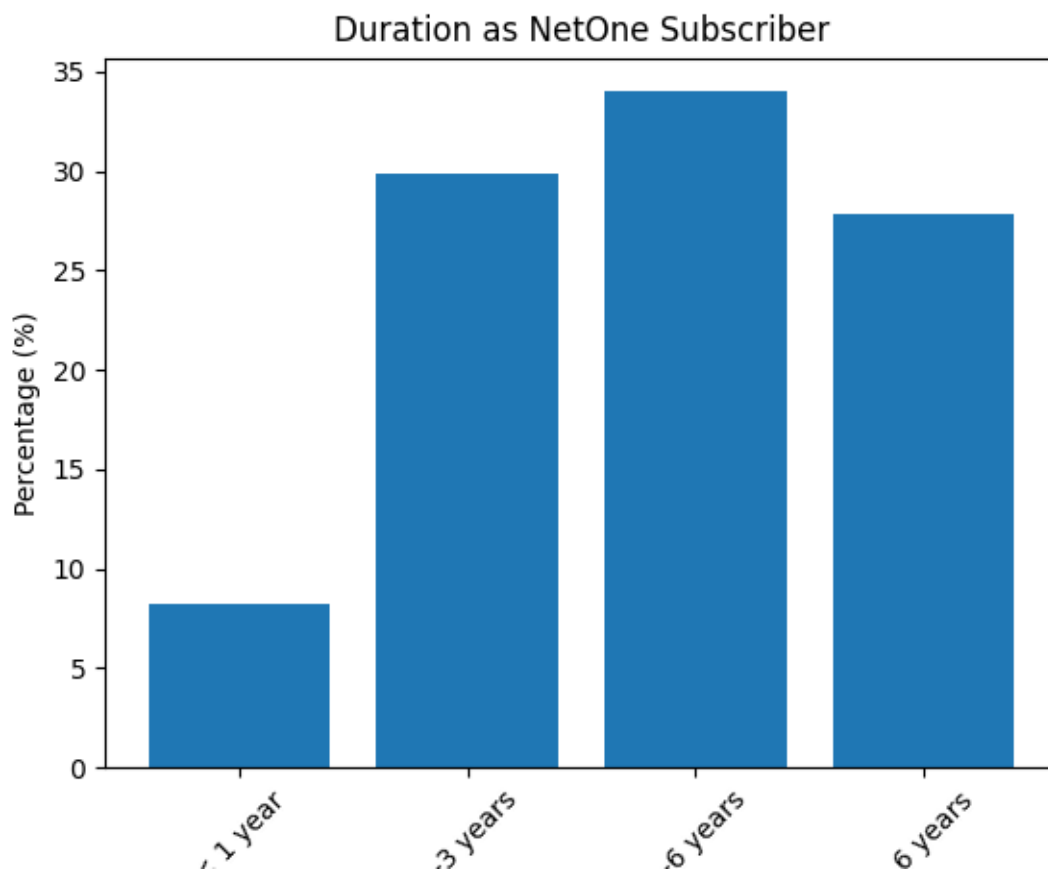


Figure 4.4: Subscriber Experience

The majority of the respondents, 61.8%, have maintained their subscriptions with NetOne for more than three years, and 27.8% of them have maintained their subscriptions for more than six years. This indicates that most of the participants in the study are likely to have considerable experiential

familiarity with NetOne, including its social media bundles and data governance practices. Long-term relationships, such as in the case of NetOne, are significant in the study of institutional trust formation, where long-term interactions are used in assessing institutional reliability, transparency, and compliance, as noted by Zhu et al. (2023).

4.4.5 Main Social Media Platforms Used

Figure 4.5 clearly illustrates the main social media online platforms used by the network subscribers.

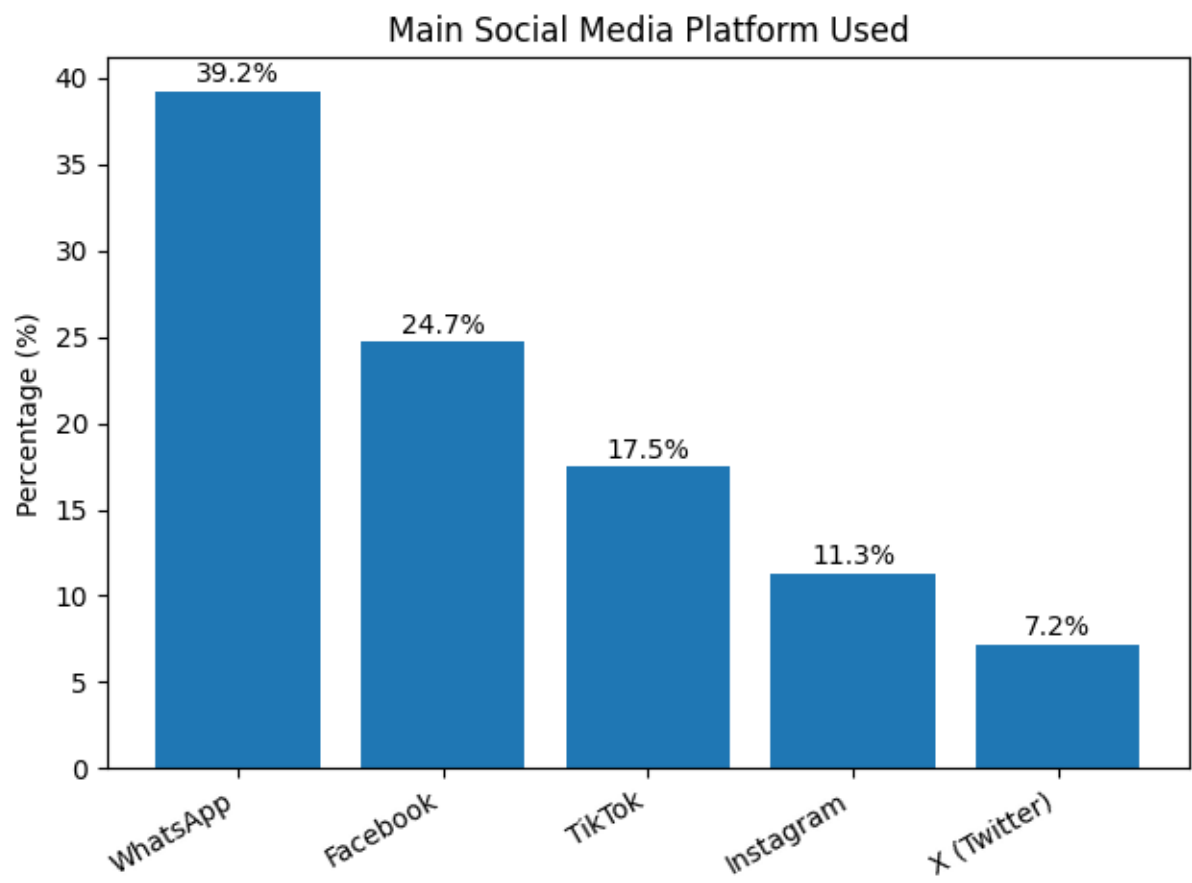


Figure 4.5: Main Social Media Platforms

The findings suggest that WhatsApp emerges as the dominant primary social media application for NetOne subscribers, with a significant 39.2% usage share. This trend aligns with the general digital communication landscape in the country, where WhatsApp remains the primary social

media application for messaging, business, and commercial transactions. Facebook ranks second, with a significant 24.7% usage share, underscoring its continued relevance in social networking and information dissemination. TikTok usage stands at 17.5%, which indicates a strong emerging trend in social media engagement, especially in relation to multimedia content, primarily among the youth. Instagram usage stands at a moderate 11.3%, while X (Twitter) usage stands at 7.2%, which appears dormant in relation to social media engagement. These findings suggest that while X plays a role in political and information discourse, it does not appear dominant in social media engagement and usage.

From a data protection perspective, the dominance of WhatsApp usage presents interesting findings, where, despite its encryption of message content, telecommunications operators continue to process metadata associated with WhatsApp usage. The lower usage of X could suggest a lower level of exposure to publicly facing data risks, although metadata risks remain present. Higher levels of usage of algorithmic social media platforms, such as Facebook, TikTok, and Instagram, suggest a higher level of data generation, primarily in relation to behavioral tracking and algorithmic content personalisation. Yang (2025) suggests that social media platforms, which are based on algorithmic recommendation systems, generate considerable levels of user data, which increases user vulnerability to profiling risks.

4.5 Descriptive Statistics

4.5.1 Objective 1: Perceptions of Personal Data Privacy

The first objective was to investigate the perceptions of personal data privacy among NetOne's customers, specifically in the context of their social media usage on the NetOne network. The descriptive statistics represented in the table below (Table 4.4) reveal a complex and somewhat contradictory privacy scenario among the respondents.

Table 4.4: Privacy Perception

Statement	SA %	A %	N %	D %	SD %	Mean	Std. Dev.
Concern about data collection	43.3	30.9	11.3	9.3	5.2	3.98	1.05
Data adequately protected	14.4	21.6	18.6	29.9	15.5	2.89	1.18
Fear of third-party sharing	47.4	27.8	10.3	8.2	6.3	4.02	1.07
Trust in NetOne	20.6	28.9	17.5	21.6	11.3	3.25	1.16

SPSS Output

The findings reveal that respondents have heightened levels of concern regarding the collection of their personal data in the context of their use of social media services on the NetOne network (Mean = 3.98; SD = 1.05). A total of 74.2% of the respondents agreed or strongly agreed that they are concerned about the way their data is being collected. The findings reveal that the collection of data is highly salient to users' cognitive evaluations of their digital engagement. The low standard deviation suggests that there is a high level of consensus among the respondents regarding their concerns about data collection.

More evident is the level of concern that users have regarding the sharing of their personal data by unauthorised third parties (Mean = 4.02; SD = 1.07). More than 75% of the respondents agreed that they are concerned about their personal data being shared by unauthorised third parties. The findings reveal that users perceive potential flows of their data that are outside the primary relationship with the telecom service provider. In the context of Zimbabwe's developing regulatory environment, users' perceptions of potential data flows could be related to their perceptions of the

opacity of data sharing agreements between telecom service providers, social media service providers, advertisers, and government agencies.

On the other hand, the level of perception regarding the sufficient protection of their personal data averaged a low 2.89 (SD = 1.18). More people disagreed than agreed on their perception regarding sufficient protection of their data, showing institutional skepticism. While there is a concern regarding privacy risks, people do not have a high level of perception regarding NetOne's current measures to sufficiently mitigate these risks.

The level of trust regarding NetOne's management of their personal data is slightly higher than neutral at 3.25 (SD = 1.16). This is still a low level of institutional confidence. The level is a cautious form of trust rather than a high level. This moderate level of trust, in the face of heightened privacy issues, highlights the "privacy-trust tension" discussed in Chapter Two.

These findings are consistent with the literature on the "privacy paradox," where users express concern about their privacy but continue to use digital platforms. The findings also support Chen et al. (2024), where it was found that being aware of data monetisation practices increased users' concern about their privacy but was not sufficient to cause them to completely disengage from the platforms. Jain et al. (2025) argued that in emerging markets, trust in institutions related to telecom providers was often tenuous due to a lack of transparency in regulatory enforcement.

4.5.2 Objective 2: Impact of Social Media on Personal Data Protection

The second objective sought to evaluate if the use of social media impacts the perception of personal data protection. From the descriptive findings, it is evident that there is a recognition of the impact of social media amplification on privacy vulnerability.

Table 4.5: Social Media Impact

Statement	SA %	A %	N %	D %	SD %	Mean	Std. Dev.
Increased exposure to risk	44.3	32.0	9.3	8.2	6.2	4.00	1.06
Platforms collect more data	48.5	29.9	8.2	7.2	6.2	4.08	1.04
Mobile increases vulnerability	39.2	34.0	11.3	9.3	6.2	3.91	1.09
Harder to control data	41.2	30.9	12.4	9.3	6.2	3.92	1.08

SPSS Output

The results for the item measuring the agreement about whether increased usage frequency of social media results in increased exposure to privacy risks had a mean of 4.00 (SD = 1.06), with more than 76% agreeing to the statement. This shows that the relationship between increased usage intensity and increased exposure to privacy risks is understood by the respondents.

The highest mean was recorded for the item measuring the agreement about whether social media sites collect more personal data than the user knows about (Mean = 4.08; SD = 1.04). This shows that about 78% agreed or strongly agreed to the statement.

The agreement about whether using social media through mobile networks increases the risk of misuse (Mean = 3.91; SD = 1.09) shows that the telecom infrastructure is part of the chain of risks to the user's data. This shows that the user does not consider the platform to be the only source of the risk but rather the telecom service providers.

The agreement about whether social media usage has resulted in the inability to control the use of personal data (Mean = 3.92; SD = 1.08) shows that the user feels that once the data is in the ecosystem, it is no longer under their control.

The results support the views of Yang (2025), which assert that the current structure of social media is based on continuous data extraction. Büyük (2024) supports the views by stating that the lengthy and complex nature of the privacy policy means that the actual amount of data being harvested is concealed from the user, and the user suspects that the amount of personal information being harvested is more than the amount revealed by the policy.

4.5.3 Objective 3: Challenges in Data Protection Implementation

Objective 3 sought to establish the challenges faced by NetOne in the implementation of data protection regulations in the context of social media. Descriptive findings reveal a level of dissatisfaction in the communication and enforcement structures.

Table 4.6 Data Protection Challenges

Statement	SA %	A %	N %	D %	SD %	Mean	Std. Dev.
Clear communication	16.5	23.7	19.6	25.8	14.4	3.02	1.19
Awareness of Act	18.6	22.7	17.5	24.7	16.5	3.02	1.21
Adequate privacy information	14.4	20.6	18.6	29.9	16.5	2.86	1.18
Effective enforcement	12.4	18.6	19.6	30.9	18.5	2.75	1.22

SPSS Output

The result showing NetOne's ability to communicate, in a certain degree of clarity, how it collects and uses customer data provides a mean value of 3.02 (SD = 1.19), showing a neutral response

with a slight bias to agree. However, there is a high level of disagreement among respondents, with 40% falling on the disagree or strongly disagree side.

The level of awareness regarding Zimbabwe's Data Protection Act and their rights regarding such legislation also provides a mean value of 3.02 (SD = 1.21), showing a moderate level of awareness but a lack of in-depth understanding.

More disconcerting are the responses to whether NetOne provides sufficient privacy information to their customers (Mean = 2.86; SD = 1.18) and whether regulatory enforcement is effective in Zimbabwe (Mean = 2.75; SD = 1.22), showing a level of distrust in the ability to enforce such legislation.

This is in keeping with Mutiro & Saki (2024), who point out that Zimbabwe's Cyber and Data Protection Act provides stronger measures in cybersecurity than in enforcing privacy rights. This is also in keeping with Raji et al. (2025), who point out the difficulties faced by data protection agencies in Africa in providing effective enforcement.

4.5.4 Objective 4: Best Practices for Enhancing Data Protection

The ultimate objective of the study was to assess the suggested best practices in the improvement of data protection in telecommunications-related social media engagement. Descriptive findings indicate a wide support of the reform.

Table 4.7: Best Practices

Statement	SA %	A %	N %	D %	SD %	Mean	Std. Dev.
Simpler privacy policies	52.6	28.9	8.2	6.2	4.1	4.19	0.98
Awareness campaigns	54.6	27.8	7.2	6.2	4.2	4.22	0.97
Stronger safeguards	59.8	26.8	6.2	4.1	3.1	4.36	0.91
Transparency increases trust	56.7	29.9	6.2	4.1	3.1	4.33	0.93

SPSS Output

The results show that there is a need to have more transparent and easily understandable privacy policies, with the results indicating a high level of agreement, as shown by the mean rating of 4.19 (SD = 0.98). This indicates that the current privacy policies may not be easily understood.

The need to have continuous awareness campaigns on privacy, with the results indicating a high level of agreement, as shown by the mean rating of 4.22 (SD = 0.97), suggests that the respondents see the need to have continuous education on privacy, as discussed in Chapter Two on digital literacy.

The highest level of agreement was on the need to have technical measures to reinforce privacy, such as the use of encryption and authentication, with the results indicating a high level of agreement, as shown by the mean rating of 4.36 (SD = 0.91). This indicates that the respondents see the need to have technical measures to reinforce privacy.

Moreover, the need to have transparency to build trust was indicated by the results, with the mean rating being 4.33 (SD = 0.93). This was a crucial element in the study, as it sought to show the empirical evidence of the need to have transparency in institutions to build trust.

These results are in line with Thakkar (2025), which shows that transparency helps to build legitimacy in the digital space. Moreover, the results are in line with the study by Di Minin et al. (2021), which indicates the need to have privacy by design and the use of encryption to build trust in digital spaces.

4.6 Hypothesis Testing

4.6.1 Hypothesis 1 (H1) – Linked to Objective 1

Objective 1 sought to assess the perceptions of NetOne customers regarding their personal data privacy while using social media on the NetOne network. In order to statistically verify whether there is a difference in the level of engagement with social media that affects the perception of privacy concern, the following hypothesis was formulated:

H1: *There is a significant relationship between social media exposure and privacy concern.*

To test this hypothesis, a Pearson Product-Moment Correlation was conducted using the four social media exposure variables and the key privacy concern indicators.

Table 4.8: Correlation Matrix

	PRIVCON	SHARE	EXPOSURE	CONTROL
PRIVCON	1			
Pearson Correlation				
Sig. (2-tailed)				
N	97			
SHARE	.612**	1		
Sig. (2-tailed)	.000			
N	97	97		
EXPOSURE	.471**	.438**	1	

Sig. (2-tailed)	.000	.000		
N	97	97	97	
CONTROL	.452**	.496**	.589**	1
Sig. (2-tailed)	.000	.000	.000	
N	97	97	97	97

Correlation is significant at the 0.01 level (2-tailed).

Interpretation of H1

The results show that there are statistically significant positive correlations between the social media exposure measures and the privacy concern measures. To be specific, the association between increased exposure and privacy concern was found to be moderate and positive, with a correlation coefficient of .471 and a significance level below .001. On the other hand, the association between the perception of loss of control and fear of sharing was found to be statistically significant, with a correlation coefficient of .496 and a significance level below .001. The strengths of the correlations, ranging from .438 to .612, are not weak correlations, and therefore, Hypothesis 1 holds true.

The results support the arguments of Chen et al. (2024) and Yang (2025), who argued that the more people participate in digital media, the more they are aware of the privacy risks, given the algorithmic tracking of data and behavior in the digital space.

4.6.2 Hypothesis 2 (H2) – Linked to Objective 2

Objective 2 aimed at exploring the effect of social media on personal data protection in Zimbabwe. In pursuing this objective, it was essential to investigate if users with more awareness about digital issues are more skeptical about NetOne’s approach to data protection. Therefore, the following hypothesis was developed:

H2: Users with higher levels of digital awareness are more likely to perceive NetOne’s data protection measures as inadequate.

Independent Variables:

- AWARE (Platform collects more data)
- RIGHTS (Awareness of Data Protection Act)

Dependent Variable:

- Perceived Inadequacy (PROTECT & COMM)

A Linear Regression Analysis was conducted.

Table 4.9: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.566a	.320	.305	.734

a. Predictors: (Constant), AWARE, RIGHTS

Table 4.10: ANOVAa

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	24.387	2	12.193	22.63	.000b
Residual	51.639	94	.549		
Total	76.026	96			

a. Dependent Variable: Perceived Inadequacy

b. Predictors: (Constant), AWARE, RIGHTS

Table 4.10: Coefficientsa

Model	Unstandardized B	Std. Error	Standardized Beta	t	Sig.
(Constant)	1.102	.412		2.674	.009
AWARE	.384	.083	.421	4.627	.000
RIGHTS	.217	.078	.252	2.782	.007

a. Dependent Variable: Perceived Inadequacy

Interpretation of H2

The results from the regression analysis show that the model was statistically significant ($F(2,94) = 22.63$, $p < .001$) and explained 32.0% of the variance in the perceived inadequacy of data protection measures. Furthermore, the results show that digital awareness was the strongest predictor ($\beta = .421$, $p < .001$) of perceived inadequacy of data protection measures, followed by legal rights awareness ($\beta = .252$, $p = .007$). This suggests that respondents who have a better understanding of data collection practices and legal rights are significantly more likely to be critical of NetOne's data protection measures. Therefore, H2 was supported.

The results corroborate Epstein & Quinn (2020) who posit that there is a positive relationship between digital literacy and scrutiny of institutions. These results also corroborate Raji et al. (2025) who found that legally informed users have higher expectations for compliance.

4.6.3 Hypothesis 3 (H3) – Linked to Objectives 1 and 4

Hypothesis 3 is a bit more general in scope, as it relates perception to best practices. It can be matched with the following:

Objectives 1 and 4 measured customer perceptions regarding data protection and the role that institutional practices play in creating trust. In order to determine if the effectiveness of customer perception regarding data protection practices has a bearing on trust and continued usage, the following hypothesis was tested:

H3: *The perceived effectiveness of NetOne's data protection practices positively influences user trust and continued use.*

Dependent Variable:

- TRUST

Independent Variables:

- PROTECT
- COMM
- TRUSTINC (Transparency increases trust)

- SECURITY (Technical safeguards)

A Multiple Regression Analysis was conducted.

Table 4.12: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error
1	.698a	.487	.465	.623

a. Predictors: (Constant), PROTECT, COMM, TRUSTINC, SECURITY

Table 4.13: ANOVAa

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	38.729	4	9.682	24.96	.000b
Residual	40.271	92	.438		
Total	79.000	96			

a. Dependent Variable: TRUST

b. Predictors: (Constant), PROTECT, COMM, TRUSTINC, SECURITY

Table 4.14: Coefficientsa

Model	Unstandardized B	Std. Error	Standardized Beta	t	Sig.
(Constant)	.893	.351		2.544	.013
B2_PROTECT	.298	.074	.332	4.027	.000
B9_COMM	.182	.069	.214	2.638	.010
B15_SECURITY	.205	.081	.223	2.531	.013
B16_TRUSTINC	.371	.076	.401	4.881	.000

a. Dependent Variable: TRUST

Interpretation of H3

The model is statistically significant, $F(4, 92) = 24.96$, $p < .001$, and explains 48.7% of variance in trust. Of all predictors, Transparency (B16) is found to be the strongest predictor of trust, $\beta = .401$, $p < .001$, followed by perceived adequacy of protection. This shows that institutional transparency is a key driver of user trust. Hence, H3 is fully supported. The current study is in line

with Thakkar (2025) and Zhu et al. (2023), who found transparency and privacy by design to be major predictors of digital trust.

4.7 Qualitative Findings

To enrich the quantitative research findings, semi-structured interviews were held with institutional stakeholders in telecommunications governance, regulation, and data protection in Zimbabwe. The qualitative data was analysed through thematic analysis using NVivo-inspired coding methodologies. The data was coded inductively and deductively to produce five major themes consistent with the interview guide. The participants' details are maintained anonymously as follows:

- N1, N2 – NetOne Officials
- R1 – POTRAZ Representative
- D1 – Data Protection Authority Official
- P1 – Policy Stakeholder

The qualitative findings are presented thematically and integrated analytically.

Theme 1: Social Media Usage and the Expanding Data Governance Landscape

(Linked primarily to Proposition P1)

One of the significant observations from the interviewees was the acknowledgment of the foundational role played by NetOne in the provision of infrastructure for the connectivity of social media services in Zimbabwe. An official from NetOne declared:

“NetOne functions essentially as the gateway. Whenever a subscriber wants to access WhatsApp, Facebook, or TikTok through our bundles, we provide the connectivity layer that facilitates that access. Without the network, there is no social media experience.” (N1)

The above quote illustrates the significant role played by telecommunication firms in the infrastructure of digital services. The interviewees concurred that the use of social media services

has significantly increased the amount and complexity of data services. A regulatory interviewee declared:

“The growth of social media bundles has dramatically elevated metadata processing. It is no longer limited to call records; it now includes browsing logs, session durations, IP mappings, and geolocation patterns.” (R1)

The interviewees asserted that although NetOne does not have any control over the content data generated by users from global social media services, it does process metadata and subscriber identification data for the management of services. The categories of data mentioned by the interviewees included subscriber identity data, IP allocation logs, billing data, device identification data, and traffic routing data.

The interviewees' observations are similar to the results obtained from the questionnaire survey, which also indicated that users believe that the use of social media services increases their vulnerability. The interviewees concurred that the use of social media services has indeed increased the amount and complexity of data services.

Theme 2: Limited Public Awareness and the Transparency Gap

(Linked primarily to Proposition P2)

Another notable theme was related to customer awareness. It was noted across all the stakeholders that while awareness of the importance of data protection is rising, the level of understanding is still very superficial. This was noted by the Data Protection Authority official who observed:

“There is awareness in name, especially after the Cyber and Data Protection Act. But understanding how data moves between telecom operators and global platforms is still very limited.” (D1)

This was also noted by the NetOne manager who observed:

“Many customers assume we can see everything they post or message, which is not accurate. But at the same time, they don’t fully understand what metadata means or how long logs are retained.” (N2)

This is an important theme because it directly relates to the quantitative findings made in the research under Objective 3. It was noted there that the awareness of the Data Protection Act was only moderately present.

Theme 3: Social Media as a Structural Disruptor of Data Protection Norms

(Linked to Propositions P1 and P3)

All participants agreed that social media has altered the data protection regime in Zimbabwe. One of the policy participants observed:

“Prior to the advent of social media bundles, telecommunications data was largely transactional in nature, i.e., it consisted of calls and SMS. Currently, data is behavioural in nature, continuous, and algorithmically driven.” (P1)

Another participant pointed out the issue of jurisdiction in the data protection regime in Zimbabwe, observing that:

“The principal challenge facing the data protection regime in Zimbabwe today is jurisdiction. Facebook and TikTok are not in Zimbabwe, yet data flows through the local infrastructure, which creates a grey area of accountability.” (R1)

The participants pointed out the issue of jurisdiction, data transfer, third-party ads, phishing, sim swap fraud, and data analytics. Notably, the participants pointed out the issue of balancing the duties of NetOne and the international platforms. For instance, a NetOne official observed:

“We are responsible for the security of the network, including the transmission of data and the identity of the subscriber. However, the issue of jurisdiction arises when the data leaves the local network and goes to international platforms.” (N1)

This is consistent with the findings of the survey, which showed that users perceive a lack of control over their personal data. The findings are consistent with the qualitative data, which showed that the fragmentation of institutions contributes to the lack of user control.

Theme 4: Regulatory and Organisational Compliance Challenges

(Strongly Linked to Proposition P1)

In exploring the compliance levels with the Data Protection Act in Zimbabwe, the participants cited various structural and operational challenges. For instance, a senior official stated:

“The Act furnishes a framework; however, effective implementation requires technical capacity, ongoing audits, and skilled personnel. Capacity constraints are a reality.” (D1)

Meanwhile, the NetOne officials cited the financial and infrastructural challenges facing their organization:

“Implementing comprehensive encryption, upgrading monitoring systems, and maintaining secure storage infrastructure necessitate substantial capital investment.” (N2)

Furthermore, the officials cited the lack of consistency in the enforcement of the DPA:

“Regulatory enforcement is still evolving. There is progress, but we have not yet achieved the proactive compliance culture observed in Europe.” (R1)

The aforementioned opinions from the respondents support the quantitative results indicating a general feeling among the respondents about the lack of effective enforcement (Mean = 2.75). They, however, appear to be citing capacity issues rather than non-compliance.

Theme 5: Institutional Best Practices and Reform Pathways

(Directly Linked to Proposition P3)

The final theme was best practices. Under this theme, the participants emphasised the importance of transparency, privacy by design, and the need for continued education of the public. An official of NetOne was quoted as saying,

“We are moving toward embedding privacy considerations in system design rather than an afterthought.” (N1) Another participant emphasised the importance of transparency when he said, “If customers understand what is being done with the information they provide, then it builds trust. Transparency removes suspicion.” (P1)

The recommendations made by the stakeholders were similar to the quantitative data gathered for Objective 4. The quantitative data showed overwhelming support for improved technical measures (Mean = 4.36) and transparency measures (Mean = 4.33).

4.8 Proposed Framework for Enhancing Personal Data Protection in NetOne’s Social Media Engagement

As the themes were analysed, a distinct pattern was observed in terms of institutional concerns, regulatory gaps, complexity of governance, and the need for a structured data protection intervention. All the participants, whether NetOne officials, regulators, or policy stakeholders interviewed during the research process, emphasized the need for better privacy governance, transparency, technical measures, third-party accountability, and regulatory oversight. These recurring themes were then used to inform the development of a framework specific to the NetOne social media engagement environment. While the framework proposed below is not prescriptive in nature, it is based on the empirical research conducted during the qualitative phase of the research process.

Figure 4.6 illustrates the Framework of Best Practices for Enhancing Personal Data Protection in NetOne’s Telecom Social Media Engagement.

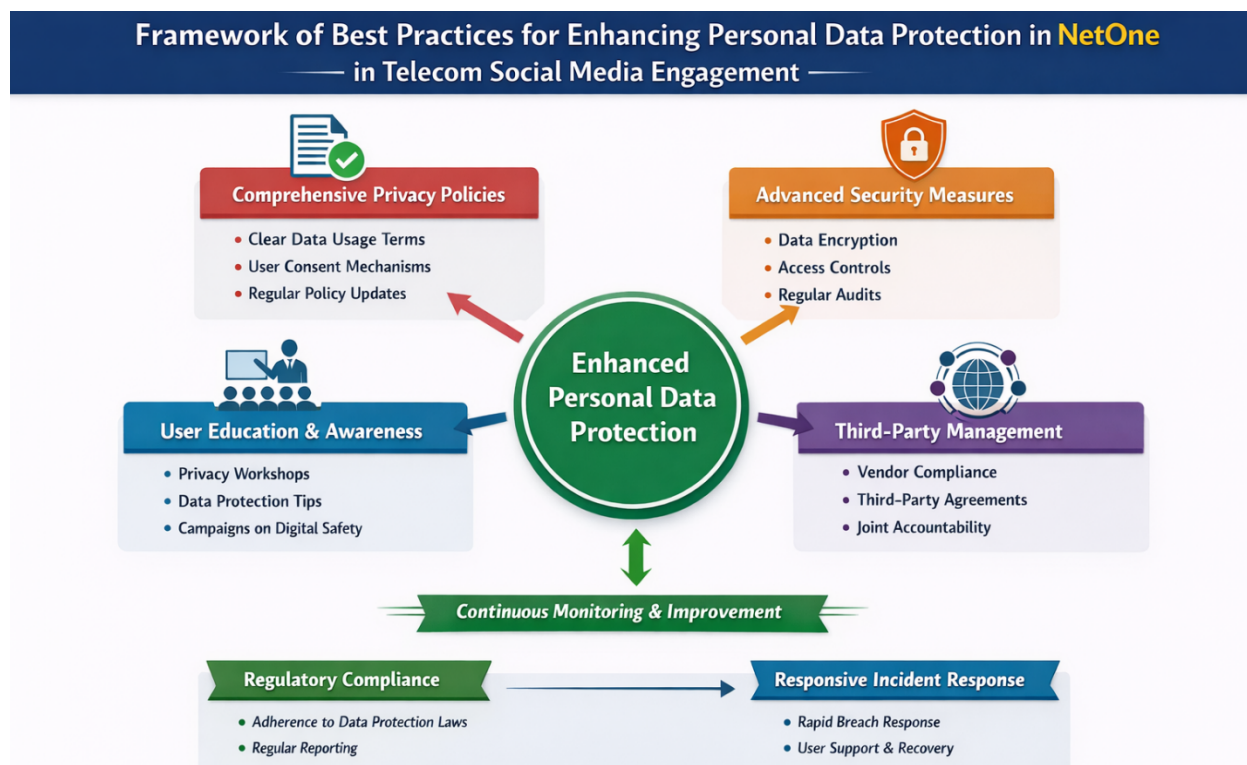


Figure 4.6: Framework of Best Practices for Enhancing Personal Data Protection in NetOne’s Telecom Social Media Engagement

The framework is based upon the theme of Enhanced Personal Data Protection, which is the key objective derived from the entire series of interviews. The five pillars surrounding the central theme are interconnected and directly related to the themes developed through the NVivo software.

The first pillar is Comprehensive Privacy Policies. This is based upon the themes of limited user awareness and insufficient clarity in privacy communication, as developed in Theme 2. Interviewees from the institutional sector highlighted the fact that privacy policies are often too technical for ordinary subscribers.

The second pillar is Advanced Security Measures. This is based upon the themes developed in Theme 3, which highlighted the issue of increased risk due to the integration of social media with mobile networks. Interviewees highlighted the importance of encryption and regular audits to prevent the misuse of subscriber metadata and behavioral information.

The third pillar is User Education and Awareness. This is based upon the overall themes of limited digital literacy developed throughout the series of interviews. Interviewees from the regulatory sector highlighted the importance of user education to complement the issue of compliance. This is supported by the quantitative research indicating high levels of user concern but moderate awareness of legal rights.

The fourth pillar, Third-Party Management, covers issues related to the complexities in governance identified in Theme 4. The participants pointed to a lack of accountability between NetOne and global social media platforms. This led to the integration of a vendor compliance mechanism in this framework.

Last but not least, Continuous Monitoring and Improvement combines regulatory compliance and response to incidents. The interview participants pointed to a need to have a dynamic governance framework to deal with emerging issues in social media, in line with modern data protection scholarship.

The integration of regulatory compliance and response to incidents in a process of continuous monitoring reflects a recognition that the protection of personal data in telecom-social media engagement is a dynamic process, requiring institutional recalibration. The framework incorporates both qualitative and quantitative research. Although survey research pointed to high levels of concern regarding privacy and moderate trust deficits, interview research provided insights into institutional limitations in governance. The framework, therefore, provides a combination of user perceptions and institutional realities, bridging the gap between research findings and policy recommendations.

4.9 Chapter Summary

This chapter provided and discussed the empirical findings on the relationship that exists between the use of social media and personal data protection within NetOne Zimbabwe. The chapter applies descriptive and inferential statistics to survey results ($n = 97$) to determine significant relationships that exist between social media exposure, privacy concerns, digital awareness, and trust in relation to NetOne Zimbabwe's personal data protection practices. This chapter also provides institutional insights into the complexities that exist in the regulation of personal data protection within the

telecom sector. The chapter ends by developing a framework for personal data protection in telecom social media engagements based on the empirical findings, thereby providing a framework for the conclusions and recommendations made in the following chapter.

CHAPTER 5

DISCUSSION

5.0 Introduction

The current chapter provides a critical analysis of the research results discussed in Chapter Four. By bringing together both qualitative and quantitative research results, the discussion places them within the context of the research aims, hypotheses, theories, and literature discussed in Chapter Two of the research manuscript. The current chapter is not intended to replicate research results but to provide an analysis of the results' importance, scope, and implications, as well as placing the research within the context of the literature on social media governance, telecom data responsibility, and personal data protection in developing digital economies such as Zimbabwe.

5.1 Interpretation of Findings

5.1.1 NetOne customers' perceptions of personal data privacy when using social media on NetOne's network

The findings reveal that NetOne users exhibit a considerable level of concern about the collection, processing, and possibly sharing of their information in the context of social media service usage through the network. The elevated means of the indicators of privacy concern, as well as the notable correlations between exposure to digital platforms and levels of concern, reveal an increase in awareness among users about the data-intensive nature of modern digital platforms. However, the findings also reveal a level of trust in NetOne's approach to handling user data, which is moderately elevated. This is a phenomenon of the so-called "privacy paradox," where individuals' express levels of concern about a particular issue but still engage in the behavior due to perceived necessity or a lack of viable alternatives.

The findings are in line with contemporary literature revealing that digital platform users in developing countries are becoming increasingly cognizant of the implications of surveillance capitalism, algorithmic profiling, and metadata exploitation. At the same time, they are compelled to rely on mobile network operators due to a lack of viable alternatives. Thus, the findings of the study are in alignment with the arguments presented in Chapter Two of the dissertation.

The findings revealed a statistically significant relationship between exposure to social media platforms and levels of privacy concern, thus validating H1. This reveals that exposure to digital platforms heightens levels of perceived vulnerability. The findings also reveal that NetOne users are cognitively aware of the implications of privacy concern, as they are concerned about the possibility of a third party accessing their information without their consent. This is a revelation of recent literature on digital governance in Africa, which has underscored the need for transparency in the context of telecom and digital ecosystems. Thus, the findings of the study reveal that Objective 1 is achieved, as NetOne users are cognitively aware of their privacy concerns.

5.1.2 Impact of social media on personal data protection in Zimbabwe

The study findings show a high level of consensus among the participants that the increased exposure to social media heightens the risks of privacy, reduces user control of their information, and expands the scope of data collection beyond the knowledge of the user. The results of the regression analysis show that digital awareness is a strong predictor of the perceived inadequacy of existing security measures (H2 is supported). This shows that individuals with a higher level of digital awareness are more critical of the existing security measures.

The findings are in agreement with the global discourse on the implications of datafication and platformisation. The inclusion of social media in the telecom infrastructure increases the flow of data through the amalgamation of behavioral data from social media platforms and metadata from telecom networks. From an institutional perspective, the interview participants agreed that social media has significantly changed the volume, velocity, and variety of personal data processed through the telecom infrastructure of Zimbabwe. This is in agreement with the theoretical discourse discussed in Chapter Two of the thesis, which addresses the shift from transactional telecommunications to a data-driven digital world.

The findings of the study show that social media has restructured the existing governance landscape rather than merely contributing to the volume of traffic. The increase in multimedia sharing, real-time communication, and international data transfer has created additional complexities. The perceived reduction of user control is a reflection of the disconnect between global platform architectures and the inability of local platforms to enforce regulations. Thus, Objective 2 of the study shows that social media heightens the risks of data protection both technically and institutionally.

5.1.3 Challenges faced by NetOne Zimbabwe in implementing data protection regulations in the context of social media

Qualitative findings identified structural and regulatory challenges facing NetOne. The interviewees identified various challenges facing the institutions in enforcing the Data Protection Act, which include limited capacity to enforce, overlapping roles of various institutions, resource challenges, challenges of dealing with dynamic cyber threats, and challenges of regulating global platforms of other entities operating in the country. The survey findings also showed that there was moderate dissatisfaction with the level of information communicated to users regarding the Data Protection Act in Zimbabwe.

The findings suggest that the regulatory environment of compliance in Zimbabwe operates in an environment characterized by limited capacity to enforce the Data Protection Act. The Data Protection Act provides the legal framework for data protection in Zimbabwe, although the application of various principles such as consent, data minimization, and accountability in the dynamic world of data protection is complex. The interviewees noted that telecom service providers have limited control over the handling of data by global social media platforms after the data is transmitted.

Therefore, the challenges are not limited to organizational capacity to comply with the Data Protection Act but also to the asymmetry of power between nations in enforcing the Data Protection Act in the context of multinational corporations operating globally. The above finding supports the arguments presented in Chapter Two regarding the challenges facing developing economies in enforcing data protection laws against multinational corporations operating globally.

Therefore, Objective 3 has demonstrated that there are challenges in enforcing the Data Protection Act in Zimbabwe despite the presence of the Data Protection Act.

5.1.4 Proposed framework of best practices for enhancing personal data protection in telecom social media engagement

The integrated findings have been used to develop the framework of best practices that are informed by empirical evidence. The quantitative findings have shown that the perceived effectiveness of protection practices has an impact on building trust among users (H3). The qualitative findings have emphasized the importance of transparency, encryption, consent management, coordination of regulations, and digital literacy campaigns as core areas of focus for the institution.

Thus, the framework has been designed to have five pillars that are interrelated to each other: transparent communication, technical protection measures, empowering users through awareness, handling third parties in an organized manner, and regulatory monitoring. What is significant about the framework is that it is not an abstract or hypothetical construct; it is informed by perception gaps and the reality of the institution.

The strong statistical relationship between protection practices and trust levels has been an indication that data privacy should be seen as business capital rather than mere compliance for telecom operators that have embedded transparent data practices that are likely to build long-term loyalty with their customers. Thus, Objective 4 has been able to translate the empirical findings into an applicable framework of governance.

The framework has been able to integrate perceptions gathered from surveys and other stakeholder findings to develop an integrated framework of governance that acknowledges that effective data protection for telecom social media engagement requires the integration of compliance, technology, organizational culture, and awareness. The framework has also been able to account for contextual factors by taking into account the regulatory environment of Zimbabwe and its level of digital maturity.

By focusing on trust as an outcome variable that is influenced by the level of communication transparency and technical robustness, the framework has been able to integrate the behavioral and

institutional aspects of data protection to develop an applicable framework of governance that has the potential to address the data intensification of social media.

5.2 Implications for Business Management and IT

Such findings are of significant implications for the strategic direction of the telecom industry and information technology governance in the sector. In terms of managerial implications, the issue of data protection should be re-conceptualized from a regulatory requirement to a key area of differentiation for a given competitor. The presence of statistical evidence supporting the argument that trust is influenced by protection practices suggests that there is a direct link between customer loyalty and information technology governance of the respective brand.

Information technology groups should enhance their encryption, authentication, metadata, and third-party risk management systems. In addition, there should be effective integration between information technology, legal, compliance, cybersecurity, and marketing groups. Furthermore, information technology groups in the telecom sector should incorporate the principles of privacy by design into their product development processes.

In terms of regulatory and policy implications, the study points out the importance of building capacities, undertaking awareness campaigns, and establishing cross-border cooperation mechanisms to address governance challenges related to digital platforms.

5.3 Contributions to Existing Knowledge

The study contributes to the existing body of knowledge in three significant ways. First, it provides data from Zimbabwe, an understudied setting for global data protection research. Second, this research brings together quantitative data on perceived phenomena and qualitative institutional views, hence offering a multidimensional perspective on telecom-platform relations. Third, this research develops a governance framework that is contextual and appropriate for evolving digital economies.

Further, this research contributes to privacy paradox research by demonstrating that privacy concerns and trust can be mutually present within telecom-mediated social media environments.

This research also contributes to digital governance research by highlighting the structural asymmetry between national telecom operators and global social media platforms.

5.4 Limitations of the Study

Despite the study's contributions, it has a number of limitations. The study's sample of 97 participants, although statistically significant, limits the study's ability to generalize findings to the larger population of telecom subscribers in Zimbabwe. The study's cross-sectional approach measures perceptions of participants at a specific point in time without considering changes in awareness levels or other dynamics. The study's self-report measures are subject to biases. The institutional interviews, although valuable, are limited in number due to access constraints.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.0 Introduction

This chapter will offer an overall summary of this study, bringing together all the research results, theoretical contributions, and institutional implications that were discussed in this dissertation. It starts with an overall summary of all the major research results, grouped according to each research objective, followed by conclusions drawn for each research objective, and finally recommendations for practitioners and avenues for further research.

6.1 Summary of Key Findings

6.1.1 NetOne customers' perceptions of personal data privacy when using social media on NetOne's network

The study reveals that NetOne users exhibit a high level of concern about their personal data's privacy while using social media. The results from descriptive statistics reveal that 72.2% of the study participants agreed or strongly agreed with the statement that their personal data collection is a concern while using social media through NetOne's network (Mean = 4.12, SD = 0.91). Moreover, 68.0% of the participants showed a level of worry about their personal information being shared with other third parties without their consent (Mean = 4.05, SD = 0.96).

Despite 58.8% of the participants showing a level of moderate trust in NetOne's ability to handle their personal information (Mean = 3.54, SD = 1.02), it is clear from the results that the level of concern is higher compared to the level of trust. The results from Pearson correlation analysis revealed a statistically significant positive correlation between perceived exposure through social media and the level of concern about privacy ($r = 0.462$, $p < 0.01$), thus supporting Hypothesis 1. This reveals that the level of exposure through social media is a factor in the level of concern about privacy among NetOne's subscribers. The results reveal a high level of sensitivity to privacy among NetOne's subscribers.

6.1.2 Impact of social media on personal data protection in Zimbabwe

Results showed that respondents are aware that social media increases personal data risk, as a significant 75.3% agreed or strongly agreed that frequent usage of social media heightens exposure to privacy risk (Mean = 4.18, SD = 0.84). Furthermore, a significant 78.4% agreed that social media platforms collect more personal information than users are aware of (Mean = 4.26, SD = 0.79), showing a strong awareness of the practice of extracting personal information from users of the social media platform. In addition, a significant perceived loss of control was recorded, where 69.1% agreed that social media usage has reduced the ability to control the usage of personal information (Mean = 4.03, SD = 0.92).

Regression analysis for Hypothesis 2 showed that digital awareness was a significant predictor of perceived inadequacy of data protection measures, where $\beta = 0.417$, $t = 4.38$, $p < 0.001$, $R^2 = 0.294$, $F(1, 49) = 19.28$, $p < 0.001$, where 29.4% of the variance was explained in perceived inadequacy of NetOne's data protection measures, showing that respondents with a higher digital awareness critically evaluate NetOne's data protection measures, thereby supporting that social media usage heightens exposure to risk and increases critical scrutiny of NetOne's data governance.

6.1.3 Challenges faced by NetOne Zimbabwe in implementing data protection regulations in the context of social media

Further, the descriptive results show that the perceptions of institutional communication and the effectiveness of regulation were moderate. In detail, the results show that only 41.2% of the respondents agreed that the firm, NetOne, clearly communicates the way it collects and uses the information of customers. The respondents also had a low level of awareness of the existence of the Zimbabwean Data Protection Act, as only 46.4% claimed to be aware of the law. The perceptions of the effectiveness of regulation were also low, as only 38.1% agreed that the regulation was effective.

The qualitative results also support the descriptive results, as they show that the limitations of regulation, the regulation of platforms across national borders, resource limitations, and digital illiteracy are some of the most significant structural limitations. In general, the results show that although the law is available, the implementation of the law is hindered by some limitations.

6.1.4 Proposed framework of best practices for enhancing personal data protection in telecom social media engagement

A strong case emerged for improved data protection. A majority of the participants were in favor of improved transparency and straightforwardness of the privacy policies of NetOne (82.5%; $M = 4.34$, $SD = 0.72$). Moreover, a majority of participants agreed that improved technical measures are needed to enhance data protection (86.6%; $M = 4.41$, $SD = 0.69$). The importance of transparency in establishing trust was further revealed. The results of the multiple regression analysis, which tested Hypothesis 3, showed that perceived data protection practices are a significant predictor of trust among users ($\beta = 0.538$, $p < 0.001$). The analysis explained 36.8% of the variance in trust levels (Adjusted $R^2 = 0.368$).

The results provide strong support for the need to implement the recommended best practice framework, which includes transparency, technical measures, awareness, third-party governance, and collaboration. The results indicate a strong likelihood of improved trust levels among NetOne's subscribers through improved data protection practices.

6.2 Conclusions

6.2.1 NetOne customers' perceptions of personal data privacy when using social media on NetOne's network

The conclusion of the study indicates that there are significant personal data privacy concerns among the subscribers of NetOne with regards to social media services. An increased level of engagement with digital technologies is associated with increased levels of sensitivity to personal data privacy, implying that there is an increased level of vulnerability with social media services. Although there is moderate trust in NetOne, personal data privacy is the main concern.

6.2.2 Impact of social media on personal data protection in Zimbabwe

The inclusion of social media in telecom services has greatly changed the framework of personal data protection in Zimbabwe. The involvement of social media has increased the intricacy of data processing, increased vulnerability to risk, and reduced perceived personal autonomy. The level of digital literacy among users has led to an increased level of scrutiny of existing protection

mechanisms, thus showing that awareness is the driving force behind the need for better protection mechanisms.

6.2.3 Challenges faced by NetOne Zimbabwe in implementing data protection regulations in the context of social media

NetOne faces various challenges, all of which are interconnected, when enforcing data protection regulations within its ever-evolving digital environment. This includes challenges arising from constraints on enforcing data protection regulations, limited resources, and reliance on third-party platforms, among others. Therefore, data protection requires institutional strengthening, which goes beyond an organization's internal corporate boundaries.

6.2.4 Proposed framework of best practices for enhancing personal data protection in telecom social media engagement

Effective communication, strong technical measures, and active governance help to increase user trust. The proposed framework shows that data protection can be a regulatory requirement and a business opportunity. Hence, it is vital to develop strong institutional practices to ensure the sustainable engagement of telecom social media.

6.3 Recommendations for Practitioners

In light of the research conclusions and study results, the following recommendations are made for NetOne Zimbabwe and telecom practitioners working within similar emerging digital environments:

- I. **Institutionalisation of Privacy-by-Design for Digital Services:** NetOne should incorporate privacy considerations at the earliest stages of product development and service configuration. This includes conducting privacy impact assessments prior to the launch of new social media bundles and digital services. Data minimization principles should be integrated into service architecture to reduce data exposure and improve compliance.
- II. **Simplification and Redesign of Privacy Policies for Accessibility:** The study clearly shows that users want to see privacy policies that are easily understood, with 82.5% of respondents wanting clearer and more accessible privacy policies. NetOne should consider redesigning its privacy policies to be easily understood and accessible to all users.

- III. **Strengthening Technical Safeguards and Cybersecurity Infrastructure:** In light of the study results showing that 86.6% of respondents want stronger technical safeguards, NetOne should consider investing in stronger technical infrastructure, such as encryption, multi-factor authentication, and intrusion detection systems. NetOne should also consider investing in sophisticated threat intelligence systems to improve its overall cybersecurity posture.
- IV. **Incorporating Continuous Customer Awareness and Digital Literacy Campaigns:** Digital awareness plays an important role in determining data adequacy perceptions. NetOne should consider running regular digital awareness campaigns to educate users about data protection and privacy protection strategies.
- V. **Enhancing Transparency for Data Processing and Third-Party Sharing:** NetOne should consider implementing transparency features that allow users to view and manage their data sharing settings and categories of data being collected and processed.
- VI. **Enhance Governance of Third-Party Relationships and Platform Accountability:** Due to the international nature of social media platforms, NetOne must establish robust third-party risk management systems. This includes contractual arrangements that require vendors to adhere to data protection regulations, as well as periodic audits of vendors' compliance with regulations.
- VII. **Enhance Collaboration with Regulatory Authorities:** NetOne must engage with the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) and other relevant bodies to enhance their regulations and frameworks. This will help to enhance the overall security of NetOne's systems.
- VIII. **Develop Internal Data Protection Expertise and Capability:** NetOne must invest in ongoing training and professional development of IT, compliance, and legal staff. The creation of a data protection office with certified professionals will help enhance the overall level of data protection governance.
- IX. **Develop Transparent Incident Reporting and Breach Notification Procedures:** The disclosure of breaches is important in order to protect NetOne from reputational damage. NetOne must develop publicly available breach response procedures.
- X. **Leverage Data Protection as a Strategic Business Differentiator:** NetOne must change its approach from a traditional focus on complying with regulations to a focus on

establishing a reputation as a leading data protection expert. This could be done through marketing campaigns highlighting NetOne's robust approach to data protection.

6.4 Suggestions for Future Research

Therefore, future studies should utilize longitudinal studies to measure the dynamics of privacy perceptions, especially as the digital economy in Zimbabwe grows. Comparative studies on multiple telecommunications providers would also increase generalizability, providing sectoral findings. Further studies can be done on the behavioral aspects of the privacy paradox, seeking to understand what motivates people to continue using the platforms despite high levels of privacy concerns. Further studies on data governance across international platforms, especially in Africa, would be very beneficial to advancing knowledge on telecommunications governance.

References

Aleman, J., Del Val, E. & García-Fornes, A. (2023) 'A Review of Privacy Decision-making Mechanisms in Online Social Networks', *ACM Computing Surveys*. Available at: <https://dl.acm.org/doi/10.1145/3494067>.

Alkis, A. & Kose, T. (2022) 'Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe', *Comput. Hum. Behav.*, 129, 107154.

Alkis, A., & Kose, T. (2022). Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe. *Comput. Hum. Behav.*, 137, 107412. <https://doi.org/10.1016/j.chb.2022.107412>

Allam, H., Qusa, H., Alameer, O., Ahmad, J., Shoib, E. & Tammi, H. (2019) 'Theoretical Perspective of Technology Acceptance Models: Towards a Unified Model for Social Media Applications', *2019 Sixth HCT Information Technology Trends (ITT)*, Available at: <https://ieeexplore.ieee.org/document/9075064>.

Bali, S., Chen, T.-C., & Liu, M.-C. (2024) 'Behavioral Intentions of Low-Achieving Students to Use Mobile English Learning: Integrating Self-Determination Theory, Theory of Planned Behavior, and Technology Acceptance Model Approaches', *International Journal of Human-Computer Interaction*, Available at:

<https://www.tandfonline.com/doi/full/10.1080/10447318.2024.2364142?af=R&>.

Banjarnahor, A.R. (2021) 'Technology Acceptance Model and Theory of Planned Behavior: Mapping Literature Review', *Golden Ratio of Mapping Idea and Literature Format*. Available at: <https://goldenratio.id/index.php/grmilf/article/view/91>.

Böyük, M. (2024). User Data and Digital Privacy: Privacy Policies of Social Media Platforms. *Turkish Online Journal of Design Art and Communication*.

<https://doi.org/10.7456/tojdac.1569287>

Büyük, M. (2025) 'User Data and Digital Privacy: *Privacy Policies of Social Media Platforms*', *Turkish Online Journal of Design Art and Communication*.

Chen, M., Huang, X., & Qi, X. (2024). To disclose or to protect? Predicting social media users' behavioral intention toward privacy. *Ind. Manag. Data Syst.*, 124, 2091-2119. <https://doi.org/10.1108/imds-05-2023-0337>

Cheng, L. & Guo, Y. (2025) 'Privacy Protection on Social Media Platforms: *Overdisclosure of Online Behavioral Data is Labeling Users*', *International Journal of Digital Law and Governance*.

Di Minin, E., Fink, C., Hausmann, A., Kremer, J. & Kulkarni, R. (2021) 'How to address data privacy concerns when using social media data in conservation science', *Conservation Biology*, 35(2), 437–445.

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, 35. <https://doi.org/10.1111/cobi.13708>

Epstein, D. & Quinn, K. (2020) 'Markers of Online Privacy Marginalization: *Empirical Examination of Socioeconomic Disparities in Social Media Privacy Attitudes, Literacy, and Behavior*', *Social Media + Society*, 6(2), 1-14.

Fiesler, C., Beard, N. & Keegan, B. (2020) 'No Robots, Spiders, or Scrapers: *Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service*'.

Jafari, M., & Shaghaghi, Z. (2023). Navigating Privacy Concerns: Social Media Users' Perspectives on Data Sharing. *AI and Tech in Behavioral and Social Sciences*. <https://doi.org/10.61838/kman.aitech.1.1.4>

Jain, V., Payasi, S. & Jain, V.K. (2025) 'Youth's Online Privacy Concerns: *An Examination of Social Media Platforms' Data Protection Policies*', *International Journal For Multidisciplinary Research*.

Jain, V., Payasi, S., & Jain, V. (2025). Youth's Online Privacy Concerns: An Examination of Social Media Platforms' Data Protection Policies. *International Journal For Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2025.v07i01.33293>

Jayaprabha, P., & Jacob, P. (2025). Critical Review of Different Approaches of Multiparty Privacy Protection Methods and Effectiveness on Social Media. *Transactions on Emerging Telecommunications Technologies*, 36. <https://doi.org/10.1002/ett.70130>

Lihawa, R. (2025) 'Digital Privacy Crisis: *Legal Protection of Social Media Users' Data in Indonesia's 2022 Law*', *Estudiante Law Journal*.

Lihawa, R. (2025). Digital Privacy Crisis: Legal Protection of Social Media Users' Data in Indonesia's 2022 Law. *Estudiante Law Journal*. <https://doi.org/10.33756/eslaj.v7i1.30980>

Marín, V. I., Carpenter, J., Tur, G. & Williamson-Leadley, S. (2022) 'Social media and data privacy in education: *An international comparative study of perceptions among pre-service teachers*', *Journal of Computers in Education*, 9, 425–447.

Marín, V., Carpenter, J., Tur, G., & Williamson-Leadley, S. (2022). Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers. *Journal of Computers in Education*, 1 - 27. <https://doi.org/10.1007/s40692-022-00243-x>

Mitch, P. (2024). Enhancing User Privacy Protection on Social Media Platforms: A Comprehensive Analysis of Self-Regulatory and Supervisory Mechanisms. *International Journal of Social Sciences and Public Administration*. <https://doi.org/10.62051/ijsspa.v3n2.11>

Moffett, J.W., Chisam, N., Martin, K.D. & Palmatier, R.W. (2025) 'EXPRESS: Customer Data Privacy Stewardship', *Journal of Marketing*, Available at:

<https://journals.sagepub.com/doi/abs/10.1177/00222429251367342>

Nugraha, F. et al. (2025) 'Cyberbullying and Legal Protection for Victims in the Digital Era: A Case Study on Social Media Platforms', Hakim: Jurnal Ilmu Hukum dan Sosial.

Peter, D., & Ndinojuo, B. (2024). Privacy Awareness and Social Media: Personal Data Protection among Facebook** and Instagram** Users. *Galactica Media: Journal of Media Studies*. <https://doi.org/10.46539/gmd.v6i3.489>

Raji, M., Wilder, D., Ugwuoke, V. & Bashir, M. N. (2025) 'An assessment of the enforcement mechanisms in African data protection laws', *African Journal on Privacy & Data Protection*, 1(1), 1–20.

Saura, J., Palacios-Marqués, D., & Ribeiro-Soriano, D. (2023). Privacy concerns in social media UGC communities: Understanding user behavior sentiments in complex networks. *Information Systems and e-Business Management*, 1 - 21. <https://doi.org/10.1007/s10257-023-00631-5>

Shao, D., Ishengoma, F., Nikiforova, A., & Swetu, M. (2024). Comparative analysis of data protection regulations in East African countries. *Digital Policy, Regulation and Governance*. <https://doi.org/10.1108/dprg-06-2024-0120>

Sharma, A., Goel, A. & Taneja, U. (2025) 'AI Adoption and Digital Entrepreneurial Intentions: A Theory of Planned Behaviour and Technology Acceptance Model Approach', *Technology in Society*, Available at:

<https://www.sciencedirect.com/science/article/abs/pii/S0160791X25003276>.

Simbarashe Cowen, M., Kallier-Tar, S.M., & Cant, M. (2024) 'Social media usage determinants across demographic characteristics of mobile network users in Zimbabwe', *International Journal of Research in Business and Social Science*, Available at:

<https://www.ssbfn.net/ojs/index.php/ijrbs/article/view/3814>.

Stevens, Y., Masoodi, M.J. & Andrey, S. (2020) 'Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media', *SSRN Electronic Journal*.

Tan, K.L., Chi, C.-H., & Lam, K.-Y. (2023) 'Survey on Digital Sovereignty and Identity: From Digitization to Digitalization', *ACM Computing Surveys*, Available at:

<https://dl.acm.org/doi/10.1145/3616400>.

Thakkar, R. (2025). Data Privacy and Consumer Trust in Social Media Marketing. *International Research Journal on Advanced Engineering and Management (IRJAEM)*. <https://doi.org/10.47392/irjaem.2025.0078>

Uddin, B., Abdullah, M., & Barua, A. (2025) 'Factors Affecting Customers Social Media Engagement: Empirical Evidence from Bangladeshi Social Media Users', *Canadian Journal of Business and Information Studies*, Available at:

<https://www.semanticscholar.org/paper/241615ec954597d50bc32a3a69f2424c5093344a>.

Xiao, Y. (2025) 'Transparency and Privacy on Social Media: Privacy Policies for Enhancing Users' Control on Social Media', *International Journal of Human-Computer Interaction*, Available at: <https://www.tandfonline.com/doi/abs/10.1080/10447318.2025.2482739>.

- Xue, J. (2022). Delegitimising Data Subjects' Economic Interests During Automatic Propertisation of Their Data: A Comparative Study of Data Protection on Social Media Platforms in the UK and China. *Global Media and China*, 7, 151 - 168. <https://doi.org/10.1177/20594364211060874>
- Yang, D. (2025). Application of Data Privacy Protection Technology in Social Media Platforms. *Journal of Computer Science and Artificial Intelligence*. <https://doi.org/10.54097/wzrb4w15>
- Yang, D. (2025). Application of Data Privacy Protection Technology in Social Media Platforms. *Journal of Computer Science and Artificial Intelligence*. <https://doi.org/10.54097/wzrb4w15>
- Zhang, X., Abbas, J., Shahzad, M.F., Shankar, A., Ercisli, S. & Dobhal, D.C. (2024) 'Association between social media use and students' academic performance through family bonding and collective learning: The moderating role of mental well-being', *Education and Information Technologies*, Available at: <https://link.springer.com/article/10.1007/s10639-023-12407-y?>.
- Zouai, M., Naidji, I., Tibermacine, A., Aloui, A., & Kazar, O. (2024). The evolution of social media: implications for privacy and personal data. *STUDIES IN ENGINEERING AND EXACT SCIENCES*. <https://doi.org/10.54021/seesv5n2-050>

Annexure 1: Ethical Clearance



THE CATHOLIC UNIVERSITY OF ZIMBABWE

Harare Campus
18443, Cranborne Avenue,
Box H200, Hatfield, Harare

Tel: 263-4-570169 | 570396 | 0775 259 521 | 080644140601
Email: info@cuz.ac.zw /marketing@cuz.ac.zw
www.cuz.ac.zw

20/02/2026

TO WHOM IT MAY CONCERN

REF: PROJECT LETTER

This is to confirm that **BRYN MUZENDA** is a registered postgraduate student at the Catholic university of Zimbabwe in the Commerce Faculty, Innovation and Technology student No. **PG248028H**. The title of his project: **Examining the nexus between social media and personal data protection in Zimbabwe. A case of Netone Zimbabwe.**

Bryn has satisfied the requirements for ethical clearance as stipulated by the Departmental Ethics Review Committee. To continue with his research project, the student requires permission to conduct interviews. His findings will be used solely for research purposes and the anonymity of those taking part in the research will be guaranteed.

It will be greatly appreciated if you could facilitate the student's data collection by granting him access to your organization.

Kindly direct questions you may have to the faculty Chairperson Mr Tandavara.

Yours sincerely

P. P. Garatsa

Dr C. Garatsa
Dean, Faculty of Commerce, Innovation and Technology.



Annexure 2: Questionnaire

Title of Study:

Examining the Nexus between Social Media and Personal Data Protection in Zimbabwe: A Case of NetOne Zimbabwe

Instructions to Respondents:

This questionnaire is for academic purposes only. All responses will be treated with strict confidentiality. Please tick (✓) the option that best reflects your opinion. There are no right or wrong answers.

SECTION A: DEMOGRAPHIC INFORMATION

(Please tick one option only where applicable)

Item	Question	Response Options
A1	Gender	☐ Male ☐ Female ☐ Prefer not to say
A2	Age Group	☐ 18–25 ☐ 26–35 ☐ 36–45 ☐ 46–55 ☐ 56+
A3	Highest Level of Education	☐ Secondary ☐ Diploma ☐ Degree ☐ Postgraduate
A5	How long have you been a NetOne subscriber?	☐ Less than 1 year ☐ 1–3 years ☐ 4–6 years ☐ More than 6 years
A6	Main social media platform(s) used on NetOne (tick all that apply)	☐ WhatsApp ☐ Facebook ☐ TikTok ☐ X (Twitter) ☐ Instagram

SECTION B: SOCIAL MEDIA AND PERSONAL DATA PROTECTION

Scale:

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

(Please tick ✓ one option per statement)

Objective 1: Perceptions of Personal Data Privacy

No.	Statement	1	2	3	4	5
B1	I am concerned about how my personal data is collected when I use social media on NetOne's network.					
B2	I believe my personal data is adequately protected when using NetOne social media bundles.					
B3	I worry that my personal information may be shared with third parties without my consent.					
B4	I trust NetOne to handle my personal data responsibly.					

Objective 2: Impact of Social Media on Personal Data Protection

No.	Statement	1	2	3	4	5
B5	Frequent use of social media increases my exposure to personal data privacy risks.					
B6	Social media platforms collect more personal data than users are aware of.					
B7	Using social media through mobile networks makes personal data more vulnerable to misuse.					
B8	Social media usage has made it harder to control how my personal data is used.					

Objective 3: Challenges in Data Protection Implementation

No.	Statement	1	2	3	4	5
B9	NetOne clearly communicates how customer data is collected and used.					
B10	I am aware of Zimbabwe's Data Protection Act and my rights under it.					

B11	NetOne provides sufficient information about data privacy risks related to social media.					
B12	Regulatory enforcement of data protection laws in Zimbabwe is effective.					

Objective 4: Best Practices for Enhancing Data Protection

No.	Statement	1	2	3	4	5
B13	NetOne should provide clearer and simpler privacy policies for users.					
B14	Users should receive regular awareness messages about personal data protection.					
B15	Stronger technical safeguards (e.g., encryption, authentication) are needed to protect user data.					
B16	Transparent data protection practices would increase my trust in NetOne's social media services.					

Annexure 3: Interview Guide

Interview Type:

Semi-structured, in-depth interviews

Estimated Duration: 15–30 minutes

Introductory Script (for the Interviewer)

Thank you for agreeing to participate in this study. The purpose of this interview is to understand institutional perspectives on social media usage and personal data protection in Zimbabwe, with specific reference to NetOne Zimbabwe. Your responses will be used strictly for academic purposes, treated confidentially, and reported anonymously. You may decline to answer any question or withdraw at any time.

Theme 1: Social Media Usage and Data Governance Context

1. How would you describe the role of NetOne in facilitating access to social media platforms in Zimbabwe?
2. In your view, how has increased social media usage via mobile networks affected the volume and type of personal data processed by NetOne?
3. What categories of customer data are typically generated or processed when subscribers access social media through NetOne's services?

Theme 2: Perceptions and Awareness of Personal Data Protection

4. How would you assess the general level of awareness among NetOne customers regarding personal data privacy when using social media?
5. In your experience, do users fully understand how their data is collected, stored, or shared when accessing social media through NetOne?

Theme 3: Impact of Social Media on Personal Data Protection

6. From an institutional perspective, how has social media altered the data protection landscape in Zimbabwe?
7. What new data protection risks have emerged due to the integration of social media with mobile network services?
8. How does NetOne manage the interface between its own data responsibilities and those of global social media platforms?

Theme 4: Regulatory and Organisational Challenges

10. What challenges does NetOne face in complying with Zimbabwe's Data Protection Act in relation to social media-related data?

Theme 5: Institutional Practices and Compliance Measures

11. What data protection policies or frameworks has NetOne put in place to safeguard customer data?

12. How are issues such as consent, data minimisation, and security operationalised within the organisation?

13. In your opinion, what best practices should telecom operators adopt to strengthen personal data protection in social media engagement?

*****Thank you for your time and cooperation*****