DATA PRIVACY MANAGEMENT BEHAVIOUR OF SOCIAL MEDIA USERS IN SOUTH AFRICA

by

IEREFAAN BATCHELOR

208006818

Thesis submitted in partial fulfilment of the requirements for the degree

Master of Information and Communication Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Dr E. Francke

Cape Town

Date submitted (7 February 2025)

DECLARATION

I, Ierefaan Batchelor, declare that the contents of this thesis represent my unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it expresses my opinions and not necessarily those of the Cape Peninsula University of Technology.

7 February 2025

Signed **Date**

ABSTRACT

Privacy at its core is the right to be let alone and ascribes the breach thereof to constitute a crime with the potential award of damages to the victim. In South Africa, the Bill of Rights within the Constitution of the Republic of South Africa, 1996, affords privacy protection to every person.

The South African population, which amounted to 62,027,503 people in the census conducted in 2022, represents diverse groups and unique communities speaking a multitude of languages. Smartphone and telecommunications industries continually experience rampant growth, thereby lowering costs and removing barriers to entry. This extends the capability of accessing the internet beyond traditional personal computers.

The convenience of access to mobile devices coupled with the social value aspect of social media platforms function as a significant driver in the popularity of the platforms for South African social media users. The South African social media user population is estimated at twenty-six (26) million users as of January 2024. The rapid proliferation of innovative technologies has further intensified privacy concerns due to new opportunities for surveillance, tracking, detection and watching people. The Cambridge Analytica privacy breach included the Facebook personal information of eighty-seven (87) million users used to profile and tailor advertisements to solicit votes for the intended political candidate. Similarly, several social media platforms may be subject to similar risks and practices.

Data breaches are an eventuality that must be pre-empted by both private and public organisations through the stringent implementation of information security measures and awareness programmes for staff and clients. Stolen personal information can be used for identity theft and fraudulent financial transactions, resulting in personal losses, reputational harm and bad credit ratings for many people. The data privacy behaviour of individuals exposes them as prime candidates for data theft and breach. Their level of exposure links to their data privacy decisions. The privacy paradox relates to disparate behaviour exhibited by users for their general privacy compared to their social media data privacy practice. Moreover, erratic privacy practice is the result of dissimilarities in demography, technical aptitude, general usage and the need for social recognition. Social media users' attitudes toward data privacy may impact their data privacy practices.

Al-Rabeeah and Saeed's combined theory contends that Communication Privacy Management (CPM) and the Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user's cultural influences. The authors believe that embedded culture and beliefs have the potential to affect users' behaviour.

The research problem relates to social computing and human-computer interaction (HCI) within the Information and Communication Technology (ICT) sector. Examining the human aspect of the data privacy management behaviour of social media users may provide critical insight into the potential for privacy breaches and vulnerability to malicious attacks. An improved understanding of data privacy behaviour has the potential to yield results that could aid data privacy education and prevention efforts. Research involving CPM and TPB in the social media context is sparse and deserves attention. Several studies have been conducted on this problem globally. However, very few studies were in the South African context.

In light of these facts, the researcher believes that there is research value in understanding the data privacy management behaviour of adult social media users in South Africa. The study is a mono-qualitative interpretivist study. The purpose of this study is to better understand the data privacy management behaviour of adult social media users residing in South Africa, specifically what factors inform the decisions that users make.

The aim of the study was to determine the data privacy behaviour of adult social media users residing in South Africa. The researcher explored the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms. The study recruited participants through social media platforms to participate in a survey and garnered responses from ninety-five (95) respondents. The data analysis employed in the study consisted of thematic analysis. The researcher used the collected data to reveal any themes or patterns that could be interpreted.

ACKNOWLEDGEMENTS

I wish to thank:

- My supervisor, Dr Errol Francke, for his unwavering backing and guidance in the conduct of this study.
- My wife, Rezahna Batchelor, for her support, sacrifice and understanding during my study duration.
- My family for their assistance and patience.
- My friends for their contributions.
- My fellow students who provided guidance and encouragement.
- My employer for affording me the flexibility to pursue my studies.
- The supportive Faculty of Informatics and Design.

DEDICATION

I would like to dedicate this work to my dearly departed father-in-law, who believed in the value of perseverance for the sake of education, self-improvement and growth.

For Cassiem Bowers

GLOSSARY

Terms	Definition
Data subject	A data subject is described as a person to whom the personal information relates.
Digital divide	The unequal distribution of access to information and communication technology due to historical social inequity.
Information owner	An information owner is the person that the private data is wholly owned and controlled by.
Privacy paradox	It entails different behaviours regarding general privacy compared to social media privacy practices. A person may state their privacy stance and completely upend it in certain situations.
Smartphone	A mobile device that can operate as both a mobile telephone and the functions related to a computer.
Social media	The information and communication technology platforms allow for the formulation of social networks to share and interact.

Acronyms/Abbreviations	Explanation
CPM	Communication Privacy Management
ICT	Information and Communication Technology
TPB	Theory of Planned Behaviour

TABLE OF CONTENTS

DECLARATION i

ABSTRACT ii

ACKNOWLEDGEMENTS iv

DEDICATION v

GLOSSARY vi

LIST OF FIGURES xiv

LIST OF TABLES xvii

CHAPTER 1: INTRODUCTION 1

1.1 Introduction and Background 1

1.1.1 Introduction 1

1.1.2 Background 2

1.2 Research Problem 4

1.3 Research Aim and Objectives 6

1.3.1 Aim 6

1.3.2 Objectives 6

1.4 Research Questions 6

1.4.1 Research Question (RQ) 6

1.4.2 Sub-research Questions (SRQ) 6

1.5 Design, Methodology, Adoption of Theoretical Framework and Ethics 6

1.5.1 Design 6

1.5.2 Research Methodology 7

1.5.3 Adoption of Theoretical Framework 8

1.5.4 Ethics 12

1.6 Delineation 12

1.6.1 In-scope 13

1.6.2 Out-of-scope 13

1.7 Outcomes, Contribution, Significance 13

1.7.1 Outcomes 13

1.7.2 Contribution 14

1.7.3 Significance 14

1.8 Clarification of basic terms 15

1.9 Summary 15

1.10 Keywords 15

CHAPTER 2: LITERATURE REVIEW 16

2.1 Introduction 16

2.2 Definition of privacy 19

2.3 Purpose of privacy 21

2.4 Privacy and the rise of technology 22

2.4.1 Technology footprint and growth 22

2.4.2 Value of privacy 23

2.4.3 Technology and privacy connection 23

2.4.4 Medical applications 24

2.4.5 IoT 24

2.4.6 Biometrics implementation 25

2.4.7 Government use cases 25

2.5 Social media use and privacy 26

2.5.1 Social media popularity 26

2.5.2 Social media registration process 27

2.5.3 Influencers and disingenuous user profiles 28
2.5.4 Risk potential 28
2.5.5 Peer pressure 29
2.5.6 Privacy calculus 29
2.5.7 Privacy paradox 29
2.5.8 Privacy Fatigue 30
2.6 Governance in social media 31
2.6.1 Terms of service 32
2.6.2 Privacy policy 33
2.6.3 Legal liability 41
2.7 Privacy breaches 41
2.7.1 Financial sector breach 42
2.7.2 Government surveillance 43
2.7.3 Technology wearables 43
2.7.4 Mobile phones 44
2.8 Privacy breaches in social media 45
2.8.1 Facebook 45
2.8.2 Google 47
2.8.3 Google Maps 48
2.8.4 Third-party profiling of social media accounts 48
2.9 Human behaviour in data privacy 48
2.10 Adoption of theory 49
2.11 Research opportunity 52
2.11.1 Research gap 52
2.11.2 Linkage to research objectives 52
2.12 Conclusion 53

CHAPTER 3: METHODOLOGY 55

3.1 Introduction 55

3.2 Research objectives 57

3.2.1 Aim 57

3.2.2 Objective 57

3.2.3 Research Questions 58

3.3 Theoretical framework 59

3.4 Research approach 61

3.4.1 Qualitative research 62

3.4.2 Quantitative research 63

3.4.3 Mixed method research 64

3.4.4 Selection of research approach 65

3.5 Research method 66

3.6 Research design 67

3.6.1 Population 67

3.6.2 Sampling 68

3.6.3 Recruitment of study participants 70

3.7 Data collection 70

3.7.1 Data collection instrument 70

3.7.2 Survey formulation 71

3.7.3 Selection of appropriate data collection medium 73

3.7.4 Process for data collection 73

3.8 Data analysis 74

3.8.1 Data preparation 74

3.8.2 Thematic Analysis 74

3.9 Validity and Reliability (or Trustworthiness) 76

3.10 Ethical considerations 77

3.10.1 Phase 1: Ethics before the study 78

3.10.2 Phase 2: Ethics at the outset of the study 79

3.10.3 Phase 3: Ethics during the data gathering phase 79

3.10.4 Phase 4: Ethics during the analysis phase 79

3.10.5 Phase 5: Ethics during the concluding phase 80

3.11 Limitations and Delimitations 80

3.12 Data Management 81

3.13 Conclusion 83

3.13.1 Research objectives 83

3.13.2 Theoretical framework 84

3.13.3 Research approach 84

3.13.4 Research method, design and data collection 84

3.13.5 Data analysis 86

3.13.6 Validity and reliability 86

3.13.7 Ethical considerations 86

CHAPTER 4: RESULTS 88

4.1 Introduction 88

4.2 Background of study 92

4.3 Research objectives 94

4.3.1 Aim 94

4.3.2 Objectives 94

4.4 Data collection 94

4.4.1 Surveys for data collection 94

4.4.2 Composition of survey participants 96
4.5 Theory 109
4.6 Analysis 110
4.6.1 Getting started 110
4.6.2 Data analysis software tools 111
4.6.3 Start data prep 111
4.6.4 Thematic analysis 113
4.7 Data presentation of findings 127
4.7.1 Sub-research question 1 129
4.7.2 Sub-research question 2 140
4.7.3 Sub-research question 3 153
4.8 Conclusion 159
CHAPTER 5: DISCUSSION 164
5.1 Introduction 164
5.2 Research objectives 166
5.2.1 Aim 166
5.2.2 Objective 166
5.3 Research synopsis 167
5.4 Theory 168
5.5 Discussion 169
5.5.1 Sub-research question 1 171
5.5.2 Sub-research question 2 191
5.5.3 Sub-research question 3 204
5.6 Conclusion 211
5.6.1 Aim and objectives 212

5.6.2 Themes 213
5.6.3 Theory 213
5.6.4 Discussion 214
CHAPTER 6: CONCLUSION 218
6.1 Introduction 218
6.2 Summary of the analysis 221
6.3 Discussion of findings 224
6.3.1 Sub-research question 1 225
6.3.2 Sub-research question 2 226
6.3.3 Sub-research question 3 227
6.3.4 Unexpected findings 227
6.4 Implications 228
6.5 Limitations 229
6.6 Recommendations 231
6.7 Contribution ..... Error! Bookmark not defined.
6.8 Conclusion 232
REFERENCES 234
APPENDICES 244
APPENDIX A: SURVEY QUESTIONNAIRE 244
APPENDIX B: INDIVIDUAL CONSENT 256
APPENDIX C: ETHICAL CLEARANCE 259
APPENDIX D: TURNITIN REPORT 261
APPENDIX E: EDITING CERTIFICATE 262

LIST OF FIGURES

Figure 1-1: Social media utilisation in South Africa (Kemp, 2024) 2

Figure 1-2: South African social media user age and gender distribution (Adapted from www.statista.com) 7

Figure 2-1: Study outline (Adapted from research proposal, 2022) 16

Figure 2-2: Outline of literature review (Adapted from research proposal, 2022) 18

Figure 2-3: Social media usage (Adapted from research proposal, 2022) 28

Figure 2-4: Social media usage and potential privacy breaches (Adapted from research proposal, 2022) 45

Figure 2-5: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017) 51

Figure 3-1: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017) 61

Figure 3-2: South African social media user age and gender distribution (Adapted from www.statista.com, 2021) 68

Figure 3-3: Thematic analysis process (Adapted from Saunders et al., 2023) 74

Figure 4-1: Problem statement (Adapted from research proposal, 2022) 89

Figure 4-2: South African population proportions per province (South Africa, 2022) 92

Figure 4-3: Proportions of languages (South Africa, 2022) 92

Figure 4-4: South African social media user age and gender distribution (Adapted from www.statista.com, 2021) 93

Figure 4-5: Google Forms survey (Google Forms, 2024) 95

Figure 4-6: Google Forms survey minimum age exclusion handler (Google Forms, 2024) 96

Figure 4-7: Age groups of participants (Google Forms, 2024) 97

Figure 4-8: Gender of participants (Google Forms, 2024) 97

Figure 4-9: Highest level of education of participants (Google Forms, 2024) 98

Figure 4-10: Employment status of participants (Google Forms, 2024) 98

Figure 4-11: Residence city of participants (Google Forms, 2024) 99

Figure 4-12: Languages spoken and read by participants (Google Forms, 2024)..... 99

Figure 4-13: Mother-tongue of participants (Google Forms, 2024) 100

Figure 4-14: Province where participants spent most of their childhood (Google Forms, 2024).. 100

Figure 4-15: City where participants spent most of their childhood (Google Forms, 2024) 101

Figure 4-16: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017) .. 109

Figure 4-17: Thematic analysis approach (Adapted from Saunders et al., 2023) 110

Figure 4-18: Data heading manipulation for import into ATLAS.ti 112

Figure 4-19: Importing .csv format survey into ATLAS.ti..... 112

Figure 4-20: Survey import question selections in ATLAS.ti 113

Figure 4-21: Documents in ATLAS.ti 114

Figure 4-22: Document groups in ATLAS.ti 115

Figure 4-23: Codification of the raw data in ATLAS.ti 117

Figure 4-24: Codes and categories in ATLAS.ti 117

Figure 4-25: Smart codes in ATLAS.ti 118

Figure 4-26: Adding codes to code groups in ATLAS.ti 119

Figure 4-27: Conceptual framework – combined CPM & TPB 128

Figure 4-28: Code - Terms of Service (ATLAS.ti, 2024) 130

Figure 4-29: Code - Registration vs Usage Purpose (Adapted from ATLAS.ti, 2024) 136

Figure 4-30: Code - Data ownership (ATLAS.ti, 2024) 138

Figure 4-31: Theme 1: Data privacy threat perception word cloud (ATLAS.ti, 2024) 139

Figure 4-32: Code - Data upload benefit vs language (ATLAS.ti, 2024) 144

Figure 4-33: Code - Data risk perception (ATLAS.ti, 2024) 147

Figure 4-34: Code - Data privacy importance perception (ATLAS.ti, 2024) 149

Figure 4-35: Code - Data Trust Perception (ATLAS.ti, 2024) 150

Figure 4-36: Know someone who experienced a breach (ATLAS.ti, 2024)..... 154

Figure 4-37: Theme 3: Behaviour word cloud (ATLAS.ti, 2024)..... 156

Figure 4-38: Breach attitude and behaviour (ATLAS.ti., 2024) 156

Figure 4-39: Breach attitude and behaviour with Smart Groups (ATLAS.ti., 2024) 158

Figure 4-40: Findings (Adapted from Analysis section, 2024)..... 161

Figure 5-1: Problem statement (Adapted from research proposal, 2022) 164

Figure 5-2: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017) 168

Figure 5-3: Findings (Adapted from Analysis section, 2024) 170

Figure 6-1: Findings (Adapted from Analysis section, 2024) 220

Figure 6-2: Social media platform utilisation (Adapted from research proposal, 2022) 221

Figure 6-3: Privacy behaviour workflow (Adapted from research proposal, 2022) 222

Figure 6-4: Integrated framework (Adapted from thesis, 2024)..... 222

LIST OF TABLES

Table 1-1: Summary of theoretical frameworks (Adapted from Petronio and Child, 2020; Al-Rabeeah and Saeed, 2017)..... 9

Table 1-2: Related work..... 10

Table 1-3: Contributions of the study..... 14

Table 1-4: Clarification of basic terms..... 15

Table 2-1: Research question and Sub-research questions (Adapted from research proposal, 2022)..... 17

Table 2-2: Terms of service and Privacy policy summary for social media platforms (Adapted from social media platforms, 2024)..... 35

Table 2-3 Components of combined CPM and TPB theories..... 50

Table 3-1: Research question and Sub-research questions (Adapted from research proposal, 2022)..... 56

Table 3-2 Components of combined CPM and TPB theories..... 60

Table 3-3: Alternative research designs (Creswell & Creswell, 2018)..... 62

Table 4-1: Research questions and theme linkages..... 89

Table 4-2: Composition of the study participants (Adapted from Google Forms, 2024)..... 102

Table 4-3: Theme 1 - Data privacy management (Adapted from ATLAS.ti, 2024)..... 120

Table 4-4: Theme 2 - Social media utilisation and threat perception (Adapted from ATLAS.ti, 2024)..... 123

Table 4-5: Theme 3 – Behaviour (Adapted from ATLAS.ti, 2024)..... 126

Table 4-6: Terms of Service vs Language..... 132

Table 4-7: Terms of Service vs Age Group..... 133

Table 4-8: Terms of Service vs Gender and Age Group..... 135

Table 4-9: Breach attitude (ATLAS.ti., 2024) 157

Table 4-10: Breach behaviour (ATLAS.ti., 2024) 157

Table 4-11: Research questions and theme linkages 162

Table 5-1: Research questions and theme linkages 165

Table 5-2: Components of combined CPM and TPB theories 169

Table 5-3: Finding for Legal component 173

Table 5-4: Finding for Emotion component 176

Table 5-5: Finding for Culture component 177

Table 5-6: Finding for Gender component 179

Table 5-7: Finding for Motivation component 180

Table 5-8: Finding for Context component 181

Table 5-9: Finding for Attitude component 182

Table 5-10: Finding for Subject Norm component 185

Table 5-11: Finding for Behavioural Control Component 187

Table 5-12: Finding for Boundary Permeability Component 188

Table 5-13: Finding for Boundary Linkage Component 189

Table 5-14: Finding for Boundary Ownership Component 190

Table 5-15: Finding for Legal component 193

Table 5-16: Finding for Culture component 197

Table 5-17: Finding for Motivation component 199

Table 5-18: Finding for Attitude component 202

Table 5-19: Finding for Boundary Permeability Component 203

Table 5-20: Finding for Boundary Ownership Component 204

Table 5-21: Finding for Culture component 206

Table 5-22: Finding for Gender component 207

Table 5-23: Finding for Motivation component 208

Table 5-24: Finding for Attitude component 210

Table 5-25: Finding for Boundary Permeability Component 211

Table 5-26: Components of combined CPM and TPB theories 214

Table 6-1: Research questions and theme linkages 223

Table 6-2: Components of combined CPM and TPB theories 225

Table 6-3: Contributions of the study ..... **Error! Bookmark not defined.**

CHAPTER 1: INTRODUCTION

1.1 Introduction and Background

1.1.1 Introduction

Jamalova and Constantinovits (2020) assert that the smartphone and telecommunications industries are some of the fastest-growing spheres of business. They further argue that the rapid growth of the smartphone market lowers the cost of entry and extends the capability of accessing the internet beyond traditional personal computers. BenRhouma et al. (2022) attribute the convenience of access to mobile devices coupled with the social value aspect of social media platforms as a significant driver in the popularity of the platforms for South African social media users. Furthermore, the authors conclude that this convenient method for users to connect, share and interact contributes to the growth of the social media base (BenRhouma et al., 2022). BenRhouma et al. (2022) assert that the value offered by social media to the sizeable South African social media base inadvertently attracts malicious actors intent on committing identity fraud, hacking to use or sell personal information, surveillance and cyberbullying.

The purpose of this study is to better understand the data privacy management behaviour, including the privacy threat awareness, of adult social media users residing in South Africa, specifically what factors inform the decisions that users make. Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Al-Rabeeah and Saeed (2017) contend that Communication Privacy Management (CPM) and the Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user's cultural influences. The authors believe that embedded culture and beliefs have the potential to affect users' behaviour (Al-Rabeeah & Saeed, 2017).

This chapter is organised into ten sections. Section One (1) presents the Introduction and Background, in which the researcher introduces the research and provides a background to contextualise the research study. The next section, Section Two (2), on the Research Problem, explains why it is a researchable problem and the implications if not attended to. The Section Three (3). Objectives and Section Four (4). Research Questions establish the drivers for the proposed research by relaying the intent of the research. Section Five (5). Design, Methodology and Ethics describe the design and methodological steps to undertake in Section Six (6). Delineation outlining the scope of the research study. Section Seven (7). Outcomes, Contribution, and Significance state the intended contribution to the body of knowledge and social assistance that may delivered. Section Eight (8). Clarification of Basic Terms defines terms used in the research proposal. Lastly, the research proposal provides the Nine (9). Summary and Then (10). Keywords.

1.1.2 Background

Kshetri and DeFranco (2020:4) boldly ask the question: “Is privacy dead?” On the surface, this sharply contrasts with earlier notions of privacy in the social computing domain. The authors state that most people value their privacy but generally lose control of their personal information with the widespread processing of information technology corporations and governmental entities (Kshetri & DeFranco, 2020). Becker (2019) describes privacy fundamentally as the right to be left alone and ascribes the breach thereof to constitute a crime with the potential award of damages to the victim. In South Africa, the Bill of Rights within the Constitution of the Republic of South Africa, 1996, affords privacy protection to every person (Kandeh et al., 2018).

Kshetri and DeFranco (2020) describe social computing as an assortment of information technologies connected to the internet to facilitate interaction, social connection and sharing. According to Hollenbaugh (2019), social media platforms are valued by a multitude of users. The burgeoning popularity of social media platforms is a prime example of a user’s social need to connect, share and interact (Hollenbaugh, 2019). Kemp (2024) reports in Figure 1-1 that South Africa has a social media population of approximately twenty-six (26) million social media users as of January 2024, thereby constituting 42,8% of the total population in the country. Beigi and Liu (2020) state that Facebook utilisation by South African social media users revealed some disturbing data privacy trends.

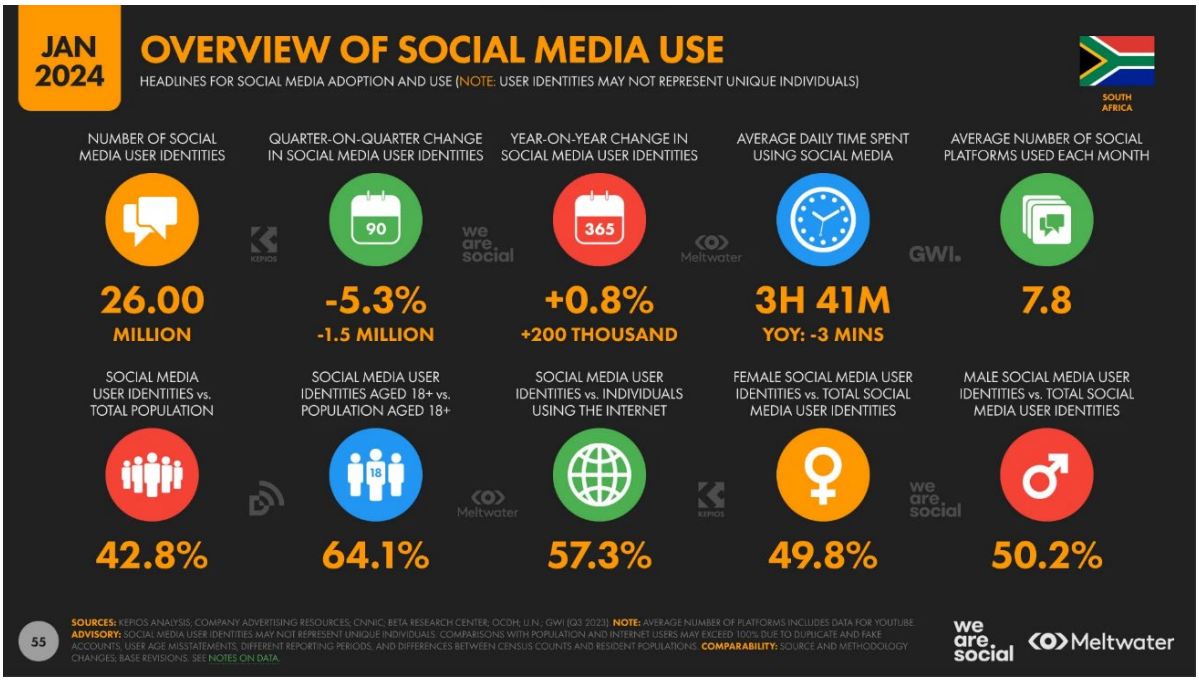


Figure 1-1: Social media utilisation in South Africa (Kemp, 2024)

Nyoni and Velempini (2018) and Arzoglou et al. (2023) claim that the rapid proliferation of innovative technologies and platforms further intensifies privacy concerns due to opportunities for surveillance, tracking, detection, and watching people. Al-Rabeeah and Saeed (2017) assert that privacy is a key consideration for social media users with the potential for breach that can be categorised as either self-inflicted, where the user places themself in a compromising situation or via a third party-inflicted privacy attack (Al-Rabeeah & Saeed, 2017). Zuboff (2019) states that the Facebook social media platform allows Facebook and governments to profile or track users with the aims of economic gains and national security, respectively. Hu et al. (2019) and Qureshi et al. (2020) state that cyber harassment pertains to incessant behaviour targeted toward a person with the intent to cause the person heightened feelings of distress and fear of physical injury. The author argues that cyber harassment is usually the precursor to threats of violence and the posting of untruths of the person on social media. The author adds that perpetrators sometimes attempt to impersonate their victim and seek out their victim's personal information to reveal online (Hu et al., 2019; Qureshi et al., 2020). Messing et al. (2020) explain that technology-based stalking is the evolution of physical stalking to the technological realm and allows a perpetrator to monitor the movements of their victim.

Ali (2023) provides an account of $8.8 billion lost to swindles in 2022, signalling a 30% increase in attacks. The author provides examples of the attacks below:

1. Electronic mail from a social media platform to facilitate a phishing attack;
2. Fraudulent LinkedIn offers of employment with an upfront salary payment;
3. Use of fake Facebook and Instagram user accounts based on a user's friend or relative that solicits payments;
4. Solicitation of personal information via Instagram and TikTok; and
5. Scams where the bad actor poses as a customer service representative to source payments.

According to Malinga (2024) and Mzekandaba (2024) privacy breaches in South Africa occur frequently and manifest increasing year-on-year. Numerous examples of the most notable privacy breaches in South Africa acknowledged include:

1. Experian breach affected 24 million South African individuals and 800,000 businesses (Hosken, 2020);
2. A Facebook breach affecting 14.3 million South African users' publicly available personal data was web-scraped and uploaded online for anyone to access Delport (2021);
3. TransUnion ransomware attack by the N4ughtySecTU hacking group impacted the personal information of 54 million South Africans in 2022 (Mzekandaba, 2023);
4. Hi-Fi Corp and Incredible group of companies experienced a breach in June 2023, impacting the records of 500,000 South African customers (Illidge, 2024b);

5. The OneDayOnly ransomware data breach by the KillSec hacking group in South Africa (Illidge, 2024b) and
6. The Liberty Holdings' electronic mail repository breach (Malinga, 2024).

Beigi and Liu (2020) and Hajli et al. (2021) conclude that data breaches are an eventuality that must be pre-empted by organisations through the stringent implementation of information security measures and awareness programmes for staff and clients. The eventuality links to privacy management behaviours, perceptions and approaches (Beigi & Liu, 2020; Hajli *et al.*, 2021). Hajli et al. (2021) concede that stolen personal information can be used for identity theft and fraudulent financial transactions, resulting in personal losses, reputational harm and bad credit ratings for many people.

The research problem relates to social computing and human-computer interaction (HCI) within the Information and Communication Technology (ICT) sector. The proposed study envisages the detection of meaningful data privacy attitudes for adult social media users residing in South Africa. Moreover, the researcher will attempt to confirm the awareness of data privacy threats and potential barriers to data privacy management. The aim is to reveal deeper meaning using the theoretical lens for the combined CPM and TPB theories. The researcher will further attempt to differentiate this qualitative study from similar studies by considering influences like culture, language, gender and age within the research study context whilst aspiring to add to the body of knowledge through the creation of new knowledge or new insights into old problems (Joubert *et al.*, 2020).

1.2 Research Problem

Hollenbaugh (2019) and Alwafi and Fakieh (2024) state that social media platforms like Facebook are valued by a multitude of users. The burgeoning growth and popularity of social media platforms are a prime example of a user's social need to connect, share and interact. The behaviour of social media users around the management of data privacy is a challenge given the potential for breaches that can be categorised as either self-inflicted, where the user places themself in a compromising situation or via a third-party-inflicted privacy attack (Al-Rabeeah & Saeed, 2017). Generally, social media users register for various social media platforms. During the registration process, they capture significant amounts of biographical personal information. Furthermore, during the period of use of social media, the user may add other personal information, including financial information (individual or business), medical information, and personal opinions or views. Zuboff (2019) mentions that the user's behaviour on the social media platform can also be tracked by the social media service provider to tailor social media posts and marketing opportunities for the user.

According to Beigi and Liu (2020), the value offered by social media platforms has unintentionally drawn bad actors to it due to the richness of the personal data available. The bad actors set out to obtain the personal data with the intent of committing identity fraud, hacking to use or sell personal information, surveillance and cyberbullying after the tactical gathering of the social media users' personal information. Moreover, service providers share social media users' personal information with or without their consent. This is observed in the 2014 example where Facebook committed a privacy breach when releasing secondary data to Cambridge Analytica (Ayaburi & Treku, 2020). Beigi and Liu (2020), Hajli et al. (2021) and Tsou et al. (2021) acknowledge a concerning trend where service providers share their big data with other entities for further analysis. The data shared is usually not anonymised to protect the personal information of social media users. This financial or nefarious-driven allure for social media service providers and bad actors, respectively, creates a real-world problem for social media users. The potential consequences entail financial harm, reputational harm, personal harm or data breaches (Beigi & Liu, 2020; Hajli et al., 2021; Tsou et al., 2021).

Bandara et al. (2021), Chen et al. (2021) and Arzoglou et al. (2023) introduce the privacy paradox involving disparate behaviour by users for general privacy compared to social media data privacy practice. Erratic privacy practice is a result of dissimilarities in demography, technical aptitude, general usage and the need for social recognition. Social media users' attitudes toward data privacy may impact their data privacy practices. Examining the human aspect of the data privacy management behaviour of social media users may provide critical insight into the potential for privacy breaches and vulnerability to malicious attacks (Bandara et al., 2021). Chen et al. (2021)contend that an improved understanding of data privacy behaviour has the potential to yield results that could aid data privacy education and prevention efforts.

The implications of increased frequency and veracity of data privacy attacks mean that social media users may fall prey to one or more forms of data privacy breach. A breach has the potential to upend the life of the affected social media user personally, financially or criminally. This matter urgently requires a deeper understanding of what drives the user behaviour that leads to a breach. Perhaps a study on the data privacy behaviour of social media users would assist in resolving the identified problem and formulating new ways of addressing this problem via more effective awareness initiatives.

1.3 Research Aim and Objectives

1.3.1 Aim

The aim of the study is to determine the data privacy behaviour of adult users of social media residing in South Africa whilst interacting on social media platforms. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

1.3.2 Objectives

1. To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.
2. To determine the data privacy threat perception of adult social media users residing in South Africa.
3. To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

1.4 Research Questions

1.4.1 Research Question (RQ)

What is the data privacy management behaviour of adult social media users?

1.4.2 Sub-research Questions (SRQ)

1. How do adult social media users manage their privacy when interacting on a social media platform?
2. What is the perceived privacy threat awareness level of adult social media users?
3. What are the behavioural barriers to privacy management implementation for adult social media users?

1.5 Design, Methodology, Adoption of Theoretical Framework and Ethics

1.5.1 Design

Babbie (2016) and Biggs et al. (2022) describe a paradigm as a perspective of the social system. He presents this as a way of looking at the world by considering various actors, their environment

and their roles in the phenomenon being studied (Babbie, 2016). The study is a mono-qualitative interpretivist study. Furthermore, this study is exploratory in nature, where the researcher will attempt to explore through investigation how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy. Biggs et al. (2022) that quantitative research leans more toward a numerical disposition, whereas qualitative research delves into a description through words. Braun et al. (2021) state that a qualitative study is best suited for the capturing of authentic perceptions, practices, experiences, behaviours, attitudes and general outlook. This qualitative study allows the researcher to delve into the social construct of the study to acquire a comprehensive understanding of the adult social media user and insight into the social media users' experience in the natural setting.

1.5.2 Research Methodology

The research methodology entails a survey study. According to Blaxter et al. (2006), Braun et al. (2021) and Biggs et al. (2022), the survey study is used to capture the natural perception, practices, experiences, behaviour, attitudes and general outlook of people. Thus, this methodology is well suited to the study of adult social media users' treatment or management of their data privacy. The study presents a level of complexity that the survey study can manage well and produce a source of data on which to base analysis. In contrast, the analysis of data may prove difficult. The survey study provides a holistic and rich set of data that may hamper analysis since the researcher may grapple with knowing what data to keep and discard. The empirical study will utilise data observed directly from respondents via survey. The survey will be used to collect data relating to intangible aspects like feelings, thoughts and opinions (Braun et al., 2021).

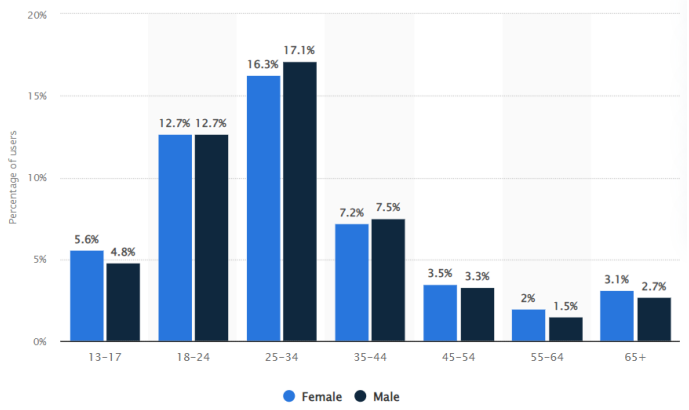


Figure 1-2: South African social media user age and gender distribution (Adapted from www.statista.com)

White (2009), Braun et al. (2021) and Biggs et al. (2022) emphasise the significance of the research population of interest as it contributes to the scope of the research study. For example, the researcher limited the research population to all adult social media users residing in South Africa. A sample of the population transacting on several popular social media platforms like Facebook, Instagram, and X will be selected from the Western Cape. A child is legally defined as a person under 18 years of age, inferring that an adult is any person who is 18 years of age or older (South Africa, 2008). Children have been eliminated from the research population due to the necessity of ethical affordance. Kemp (2021) asserts that the South African social media population consists of twenty-five (25) million social media users as of January 2021 and constitutes 41,9% of the total population. Statista (2021) illustrated the age and gender distribution of the population in Figure 1-2. The population spans generations and may be able to assess differentiated attitudes to data privacy over the generations.

White (2009) and Joubert *et al.* (2020) note that it is necessary to explicitly delineate the geographical span of the research study. The researcher resides in the Western Cape in South Africa and will conduct the research within the borders of South Africa. Joubert *et al.* (2020) reinforce the sentiment, as mentioned earlier, by noting that the span must be determined.

Blaxter et al. (2006) and Biggs et al. (2022) introduce the sampling technique concept consisting of probability and non-probability sampling. The researcher employs survey data collection methods. Non-probability sampling, given that the researcher cannot foresee the compilation of the survey's participants. The researcher used the survey data in a manner similar to interviews, where the survey data used to qualitatively generate the prevalent data privacy behaviour patterns.

1.5.3 Adoption of Theoretical Framework

Communication Privacy Management (CPM) and the Theory of Planned Behaviour (TPB) have previously been used in ICT studies, notably in IEEE Explore and the International Journal of Advanced Computer Science and Applications. The related work in Table 1-1 serves to support the researcher's selection of the theory for this study.

Table 1-1: Summary of theoretical frameworks
(Adapted from Petronio and Child, 2020; Al-Rabeeah and Saeed, 2017)

FRAMEWORK	DESCRIPTION
Communication Privacy Management (CPM):	Petronio and Child (2020) contend that Communication Privacy Management (CPM) pertains to privacy decisions influenced by the user's cultural influences. The authors believe that the embedded culture and beliefs could affect the behaviour of users (Petronio & Child, 2020). Al-Rabeeah and Saeed (2017) explain that CPM assists in understanding the way an individual organises their logic for data privacy protection.
Theory of Planned Behaviour (TPB):	Al-Rabeeah and Saeed (2017) describe the Theory of Planned Behaviour (TPB) as the interconnection between an individual's belief structure and their behaviour. The authors state that the theory can forecast a decision when inserting a specific action. Barth and de Jong (2017) and McNealy and Mullis (2019) explain that the behaviour of an individual is determined by their predetermined belief system. This includes their perceptions of the intended outcome, norms and reward despite the associated risk (Barth & de Jong, 2017; McNealy & Mullis, 2019).

Table 1-2 provides a summary of related data privacy work. The researcher explored vast quantities of academic literature to inform the theory selection. Al-Rabeeah and Saeed (2017) propose a data privacy model that amalgamates CPM and TPB. Moreover, the authors recommend further studies where this combined theory can be applied to validate their findings (Al-Rabeeah & Saeed, 2017).

The researcher aims to reveal deeper meaning using the combined CPM and TPB theories as the theoretical lens for the study. The researcher will attempt to differentiate this qualitative study from similar studies by considering influences like culture, language, gender and age within the context of the research study.

Table 1-2: Related work

AUTHORS	YEAR & COUNTRY	PAPER TITLE	SUMMARY	METHODS	FINDINGS	GAP/S
Al-Rabeeah, A.A.N. & Saeed, F.	2017; Malaysia	Data privacy model for social media platforms	The authors contend that data privacy is problematic in social media. They intend to propose a Data Privacy Model.	• Survey • Non-probability sampling • Quantitative study • Thematic analysis	The authors propose a data privacy model consisting of an amalgam of Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB).	• Limited to Malaysian respondents. • The study focuses on the data privacy model. • The survey limits responses. • Application of the combined theories to a study.
Han, K., Jung, H., Jang, J.Y. & Lee, D.	2018; Korea	Understanding users' privacy attitudes through subjective and objective assessments: An Instagram case study	The authors investigate the privacy attitudes of Instagram end-users. The study considers the literature and compares privacy attitudes.	• Public Instagram data • Sample = 271 participants • Criteria = Instagram users over 18 who must have shared over 5 pieces of private data. • Survey • Quantitative study	Observed changes in respondent attitudes to privacy between pre-test and post-test. The authors noted that "hometown, education, religion, political views, relationship status, profile photo, favourites/likes, emotions/sentiment and sexual orientation" are the most important when safeguarding privacy.	• Limited to Instagram. • Limited to Korea. • Authors identified future work: • Looking into additional privacy items via literature review. • Deep learning techniques for extracting knowledge from an image. • The survey limits responses.
Nyoni, P. & Velempini, M.	2018; South Africa	Privacy and user awareness on Facebook	The authors allude that Facebook users store a wealth of personal information on social media platforms. The authors intend to investigate the data privacy attitudes of	• Mixed methods approach: – Online observation of Facebook users – Cloning simulation Survey • Convenience sampling • Sample = 357 participants	Personal information can be easily accessed by anyone, given that much of it is publicly available on the Facebook social media platform. Moreover, users are prone to theft of their personal information due to a lack of knowledge on methods to protect themselves.	• Limited to a specific pool of Facebook users that had liked the North-West University's (NWU's) Facebook page. • The survey limits responses. • Inclusion of a more diverse group of participants, e.g. no university education

AUTHORS	YEAR & COUNTRY	PAPER TITLE	SUMMARY	METHODS	FINDINGS	GAP/S
			Facebook users and whether their data privacy attitudes place them at risk of breach.	• Population = 5701 North-West University (NWU) Facebook users		

1.5.4 Ethics

Kumar (2011) speaks about the importance of obtaining informed consent before gathering data for research. The components of the data gathering must be explicitly stated to the potential participants so that they may decide whether or not to participate. The researcher will explain the purpose of the study and explicitly state that participants must provide written consent for the researcher to proceed. For example, the researcher must conduct this research in a responsible manner that will ensure that the participants are afforded anonymity and confidentiality. The researcher must safeguard the information provided by the participants and must anonymise the participants when making reference to them in the study. Moreover, provision must be made for the rights of the approached participants to refuse participation, allow for withdrawal and inform the participants of the details of the consent. Assurance must be provided that data is only stored and retained in the location, on the medium and for the duration required for the research. Access to the data must further be strictly limited to the researcher and the Higher Degrees Committee (HDC) or University where required. The data will be protected with either physical or electronic safeguards to prevent unauthorised access. The requirements of the Protection of Personal Information Act: Act 4 of 2013 will be applied, and the personal information in the research will be safeguarded.

The researcher must ensure that the University is protected. Furthermore, research conducted in an open-source environment remains the property of the University. The researcher must adhere to the University's licensing mechanism when intending to publish the research. All research from documents must be credited for their contribution by referencing the research in the body of the text and the reference or bibliography section. The researcher must read the University's Plagiarism Policy, understand their ethical responsibilities and rigidly conform by applying it to their work.

1.6 Delineation

The study employs a qualitative study using surveys to examine the data privacy behaviour of adult social media users. Biggs et al. (2022) ascribes that quantitative research leans more toward a numerical disposition, whereas qualitative research delves into a description through words. Babbie (2016) and Braun et al. (2021) state that a qualitative study is best suited for the capturing of authentic perceptions, practices, experiences, behaviours, attitudes and general outlook. This qualitative study will allow the researcher to delve into the social construct of the study to acquire a comprehensive understanding of the adult social media user and insight into the social media users' experience in the natural setting.

Children are excluded from the study in lieu of the ethical affordances necessary for inclusion. Moreover, the study will be conducted within the confines of South Africa. The study is delineated to

the confines of South Africa as the researcher resides in the Western Cape, which would be manageable for the size, complexity, and time constraints of the study. The study's limitation to South Africa is to understand the influence of diverse cultures and communities on data privacy management.

In Appendix C, the researcher was granted ethical clearance between 22 September 2022 – 30 June 2025. Therefore, the research must conclude by 30 June 2025.

1.6.1 In-scope

The study is limited to the following parameters:

- Data privacy behaviour of adult social media users
- The research population will be limited to adult social media users 18 years of age and older residing in South Africa
- The study will be conducted within the confines of South Africa
- Combined CPM and TPB theories will be employed
- Influence of participants' age, language, education and community

1.6.2 Out-of-scope

The study is limited to the parameters outlined in section 1.6.1. The study excludes the following:

- Social media users under 18 years of age
- Legislation and policy instruments for managing data privacy
- Information security
- Cyber security
- Encryption and decryption

1.7 Outcomes, Contribution, Significance

1.7.1 Outcomes

White (2009) and Wisse and Roeland (2022) attest that researchers have, in some part, an influence through their research. For example, the study attempted to better understand the data privacy management behaviour of adult social media users. The study attempted to detect any meaningful data privacy behaviour for adult social media users. The researcher selected adult social media users to participate in the research study. The researcher increased the data privacy awareness of the social media user.

1.7.2 Contribution

White (2009) and Wisse and Roeland (2022) suggest that postgraduate students must try to distribute their research widely. For example, several associations are listed that arrange special conferences where researchers can share their work with their peers. The researcher made the contributions listed in Table 1-3.

Table 1-3: Contributions of the study

THEORETICAL CONTRIBUTION	METHODOLOGICAL CONTRIBUTION	PRACTICAL CONTRIBUTION
• The revelation of the influence of personal beliefs, culture and language on data privacy behaviour may add to the theoretical contribution.	• The peer-reviewed results of the study may bolster data privacy management frameworks.	• The practical contribution may be realised from an improvement in the data privacy awareness and behaviour of respondents. • Improved comprehension of this phenomenon may add to the practical contributions via data privacy management training and awareness efforts.

1.7.3 Significance

Creswell and Creswell (2018) and Nind (2023) explain that the significance section in a research proposal is intended to demonstrate the importance of the problem.

Firstly, the proposed research intends to first clarify whether data privacy management on social media is a problem.

Secondly, it provides an opportunity for the researcher to compare the research study to similar studies previously conducted.

Thirdly, it allows the researcher to establish whether the CPM and TPB theory elements influence the data privacy management behaviour of adult social media users.

Lastly, if the aforementioned is confirmed, the research findings could be utilised to tailor data privacy management awareness campaigns or assist with initiatives to improve data privacy practices, thereby reducing opportunities for identity theft, fraud and direct marketing. Similarly, the findings from the study could assist with driving improvement in information security design on social media platforms.

1.8 Clarification of basic terms

Table 1-4: Clarification of basic terms

TERM	DEFINITION
Data subject	A data subject is described as a person to whom the personal information relates.
Privacy paradox	It entails different behaviours regarding general privacy compared to social media privacy practices. A person may state their privacy stance and completely upend it in certain situations.
Social media	It is the information and communication technology platforms that allow for the formulation of social networks to share and interact.

1.9 Summary

Millard and Bascerano (2016) describe privacy at its core as the right to be let alone and ascribe the breach thereof to constitute a crime with the potential award of damages to the victim. In South Africa, the Bill of Rights within the Constitution of the Republic of South Africa, 1996, affords privacy protection to every person. Nyoni and Velempini (2018) and Arzoglou et al. (2023) tendered that the rapid proliferation of innovative technologies has further intensified privacy concerns due to new opportunities for surveillance, tracking, detection and watching people. Kshetri and DeFranco (2020) note that the Cambridge Analytica privacy breach included the Facebook personal information of eighty-seven (87) million users that was used to profile and tailor advertisements to solicit votes for the intended political candidate. Similarly, numerous other social media platforms may be subject to similar risks and practices (Kshetri & DeFranco, 2020).

Beigi and Liu (2020) are of the opinion that data breaches are an eventuality that must be pre-empted by both private and public organisations through the stringent implementation of information security measures and awareness programmes for staff and clients. The authors concede that stolen personal information can be used for identity theft and fraudulent financial transactions, resulting in personal losses, reputational harm and bad credit ratings for many people (Beigi & Liu, 2020).

1.10 Keywords

Data privacy; Facebook; Instagram; privacy behaviour, social media; Twitter

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The chapter is organised into Twelve (12) sections. Section One (1) provides the introduction where the researcher opens the literature review. Sections Two (2) and Three (3) outline the definition and purpose of privacy, respectively. Section Four (4) delves into the rise of technology, and Section Five (5) considers social media in the context of privacy. Section Six (6) reviews the governance framework in social media. Sections Seven (7) and Eight (8) span the privacy breaches experienced by users and entities. Section Nine (9) investigates the human behavioural aspect, whilst Section Ten (10) considers the theoretical framework. Section Eleven (11) describes the research gap, and Section Twelve (12) closes the chapter with a conclusion.

Figure 2-1: Study outline (Adapted from research proposal, 2022)

The study is exploratory in nature, considering how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy. The researcher intends to use the embedded culture and beliefs of participants as a lens to improve the understanding of the behaviour of users' data privacy interactions on social media platforms. The study's title, aim, objectives, research question and sub-research questions are illustrated in Figure 2-1 above for easy reference. These research objectives set the scene for the section 3. Methodology, 4. Results and 5. Discussion that follows. The keywords for the study are found in section 1.10 above and are also provided below for ease of reference.

Predominantly, peer-reviewed journal articles and books are used by the researcher to formulate this literature review. These are acquired by the researcher utilising the Cape Peninsula University of Technology's (CPUT's) online library search engine with the keywords mentioned earlier. The main intention of the literature review is to use authentic and vetted empirical information to better understand the problem and the associated research gaps by essentially standing on the shoulders of proven academics. Newspaper articles, magazine articles and internet webpages are also used in the literature review to provide statistical data and authentic accounts of privacy issues, data breaches and problems associated with the utilisation of social media platforms.

Table 2-1: Research question and Sub-research questions
(Adapted from research proposal, 2022)

NATURE	RESEARCH QUESTIONS	RESEARCH OBJECTIVES
Research Question **(RQ)**	What is the data privacy management behaviour of adult social media users?	
Sub-Research Question 1 **(SRQ1)**	How do adult social media users manage their privacy when interacting on a social media platform?	To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.
Sub-Research Question 2 **(SRQ2)**	What is the perceived privacy threat awareness level of adult social media users?	To determine the data privacy threat perception of adult social media users residing in South Africa.

Sub-Research Question 3 **(SRQ3)**	What are the behavioural barriers to privacy management implementation for adult social media users?	To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

The literature resources are imported into Mendeley. This is a software application that supports researchers in managing their reference material. The researcher uses Mendeley to read, identify passages of interesting text that potentially could be used for the literature review and assist with the provisional in-text referencing. The number of literature sources is vast, amounting to 103. All sources are cited in this body of text and the reference table using the CPUT Harvard referencing method as prescribed by CPUT dated 5 August 2024.

The sub-headings for Chapter 2, illustrated in Figure 2-2, are formulated using the research title's focal points. The researcher will structure the chapter using the available literature to form a cohesive flow for the reader. The box outlines and arrows coloured in blue, green and pink depict the relevance of the three (3) focal points of the research title, namely: "Privacy", "Behaviour", and "Social Media Users".

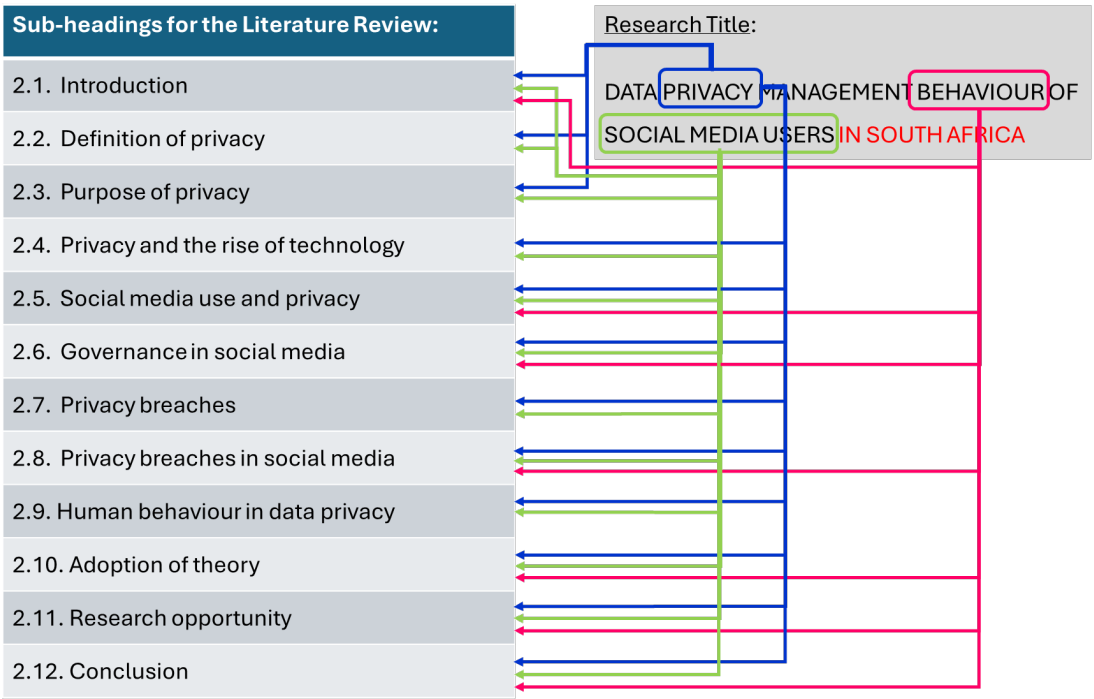


Figure 2-2: Outline of literature review (Adapted from research proposal, 2022)

The study attempts to determine the data privacy management behaviour of social media users residing in South Africa. According to Statistics South Africa (2024), as of Census 2022, the country has a diverse population of 62,027,503 people. Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Petronio and Child (2020) and Al-Rabeeah and Saeed (2017) contend that the Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user's cultural influences. McNealy and Mullis (2019:111) add that research involving CPM in the "social media context" is sparse and deserves attention.

Beigi and Liu (2020) are of the opinion that the abundance and scale of private data available on social media primes the platforms for exploitation by bad actors. This sets the stage for opportunities for identity fraud, hacking to use or sell personal information, surveillance and cyberbullying (Beigi & Liu, 2020).

The researcher will conduct a study that will explore how adult social media users residing in South Africa interact on social media platforms, specifically their treatment or management of their data privacy. The researcher intends to use embedded culture and beliefs as a lens to improve the understanding of user behaviour.

This chapter describes the problem to establish this as a researchable problem. The goal is facilitated by the formulated research aim and objectives directing the research questions of the study by clarifying the definition of privacy, understanding the progression of technology and the associated privacy challenges, social media use cases, potential for negative social media outcomes, social media governance, and applicable behavioural theories like Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB).

The literature review commences in the next section by defining the concept of privacy. It is necessary to clearly and explicitly relay this definition to ensure that the reader fully comprehends the parameters and context thereof.

2.2 Definition of privacy

According to Lacity and Coon (2024), the task of defining privacy is often taken for granted and construed as a simple undertaking. Lacity and Coon (2024) mentions that many have attempted to adequately define privacy using traditional means. The authors propose the use of an approach that takes the context into account, as this has a significant effect on whether

something is considered private. They further describe privacy as the ability to control what and to whom information can be released (Lacity & Coon, 2024). Millard and Bascerano (2016) and Hajli et al. (2021) submit the definition that privacy entails the right to be disremembered and the right to confidentiality, void of interference in a personal capacity. They add that privacy involves the concealment of personal information from persons not privy to the information and that disclosure must be driven by consent (Millard & Bascerano, 2016). Lacity and Coon (2024) contend that the administration, including restrictions, of privacy is fundamental to managing the probability of negative privacy outcomes. Becker (2019:308) tenders the privacy definition as “the right to be left alone”. The author adds that a person is entitled to a private space free of interference (Becker, 2019). Becker (2019) explains that empirical research on privacy rights has been extended in that the data subject owns their destiny. Therefore, the data subject manages their own privacy and chart their privacy course. The author describes privacy autonomy as data subjects exposing their data and consuming it by a third party. When the third party knows the difference between right and wrong, they may continue to consume the individual’s data. The choice of the data subject to persist with this behaviour means that they actively make this privacy choice (Becker, 2019).

Lacity and Coon (2024) posits that privacy can be understood in one of three (3) ways. The first way that privacy can be understood is by protecting information. The authors describe an example where someone’s personal insights are exposed without their knowledge or explicit consent (Lacity & Coon, 2024). Lacity and Coon (2024) present the notion of physical privacy where the physical property of an individual or group is trespassed and thereby contravenes their privacy. The second understanding relates to tranquillity, where the individual or group can construct a serene environment if there is no privacy breach. Lastly, the authors explain that privacy encompasses the flexibility of an individual to manage their privacy (Lacity & Coon, 2024).

Al-Rabeeah and Saeed (2017) state that the law makes privacy provisions, vesting the authority for the release of information with the owner and concession of ownership when information is placed in the public domain by the owner. They elaborate on privacy as the ownership of private moments or incidences hinged on consent for publication or sharing (Al-Rabeeah & Saeed, 2017). Becker (2019) contends that the notion of privacy is upended by scientific works by Nissenbaum. Becker (2019), asserts that an individual does not automatically have a right to privacy. For example, a person and social confidant are in a public setting. They are essentially in a private interaction within the public setting. Should someone insert themself in the interaction, they would contravene the privacy rule (Becker, 2019). Lacity

and Coon (2024:26) asserts that information in the “public domain” remains open for anyone to consume and reuse. For example, it would constitute a breach if the affected person were an ordinary person with a reasonable expectation of privacy. In stark contrast, information for an affected person in public office or necessary for court proceedings is not protected by the right to privacy for their public office duties. Al-Rabeeah and Saeed (2017) report that verbal versus written exchanges of private information are not treated the same way, with verbal privacy offences often conceded as freedom of speech (Al-Rabeeah & Saeed, 2017). Lacity and Coon (2024:26) reinforce this sentiment by explaining that a doctor and patient professional relationship is constrained by the rules of the “private domain”. The setting requires the necessary privacy protocols to be strictly upheld to safeguard the professional relationship and the patient's medical history (Lacity & Coon, 2024).

Lacity and Coon (2024) asserts that the context in which privacy is construed is crucial. The authors explain that privacy is defined differently from the philosophical, system, sociology and architectural perspective (Lacity & Coon, 2024).

The definition of privacy, as proposed by Becker (2019), brings some social dimensions into the fray. However, the definition by Hajli et al. (2021) and Lacity and Coon (2024) lack appropriately defined dimensions for the social media context. It is important to draw in new aspects that impact privacy to ensure that the definitions keep pace with developments and newly established contexts. Therefore, the definition and explanations provided by Becker (2019) shall be used for the purposes of this study. In the social media context, this amounts to the social media user taking responsibility for their data privacy management decisions and affording themselves sufficient protections to safeguard their data.

The next section supplements the definition of privacy by touching on the purpose and need for privacy. This section elicits some use cases to realise how privacy impacts people and entities.

2.3 Purpose of privacy

The purpose of privacy is to protect the individual and potential fallout. Instances of negative fallout could relate to breaches of personal information, medical information, commercial information, financial information, civil liberties or contravention of the law.

Lacity and Coon (2024:29), explains that an individual intrinsically has “The Right to Privacy”. The authors add that individuals are provided the necessary safeguards to give effect to this

via the law. Moreover, privacy is cited for providing information security safeguards against personal information and “identity theft” (Lacity & Coon, 2024:35). Schubert and Barrett (2024) note that the safeguarding of personal information is fundamental to data privacy management. Moreover, the protection of sensitive classes of information, like medical information, requires enhanced safety mechanisms (Schubert & Barrett, 2024).

Lacity and Coon (2024:36) alludes that privacy can be exempted from certain scenarios. The authors contend that it is necessary to exempt privacy rules to facilitate openness and “transparency” for government entities. These principles should evoke accountability and circumvent immoral acts to foster good governance. The authors add that openness and “transparency” could fail entities where officials must relay information for which they do not have the competence. This act could again place the entity at risk (Lacity & Coon, 2024). Kuşkonmaz (2021) concludes that the United States of America (USA) directed legislation to protect against domestic terrorism and egregious criminal activity. The legislation affords the USA’s authorities the right to circumvent any privacy directions in the name of national security and justice. These exemptions allow the USA’s authorities to monitor, track and collect data on people under these auspices. The relaxation of the data privacy prescripts further allows for the cross-agency sharing of data to perform their function (Kuşkonmaz, 2021).

Lacity and Coon (2024) heed the potential dangers that technology imposes. The authors describe an example where the rampant rise of digital videography and photography available through new technologies could negatively impact the privacy of individuals. Breaches of information have the potential to cause significant harm. This could manifest in emotional, reputational and physical harm to an individual. Alternatively, this could manifest in economic losses for an individual or organisation. Schubert and Barrett (2024) attribute extortionate levels of economic losses to privacy breaches, with an average data loss amounting to $4.35 million.

Privacy and the rise of technology are discussed in the next section. The intricacies of privacy in the digital age are explained amidst the rise of technology.

2.4 Privacy and the rise of technology

2.4.1 Technology footprint and growth

Statistics SA (2019) reported internet penetration in South African households, signalling growth from 41.30% to 61.83% between 2013 and 2017, respectively. The growth of

households using or having access to the Internet achieved a net growth of 20.53% over the four years (Statistics SA, 2019). According to Statistics SA (2019), in 2017, 13.8 million people (25.8% of the population) lived in extreme poverty. Despite these facts depicting the extreme digital divide and poverty in South Africa, widespread mobile device adoption is frequently connecting more people to the internet (Statistics SA, 2019). Jamalova and Constantinovits (2020) describe the smartphone and telecommunications industry as experiencing rapid growth due to the lowered cost of entry for smartphones and extending the capability to access the internet beyond traditional computers. Despite these facts depicting the extreme digital divide and poverty in South Africa, widespread mobile device adoption is frequently connecting more people to the internet (Statistics SA, 2019).

2.4.2 Value of privacy

According to Kshetri and DeFranco (2020), a sample of the population in the USA was polled, and it was revealed that more than 90% of the participants felt that their data was important. The authors relay that despite the participants' sentiments, very little protection can be afforded to the data due to rampant technological innovation where data repositories are scaling at pace (Kshetri & DeFranco, 2020).

The statement by Kshetri and DeFranco (2020) relays a serious concern where users' outlooks do not match their practice. Furthermore, this represents a problem as the technology evolves at a phenomenal pace that the protections cannot keep up with. Much needs to be done to better understand the factors that lead to this user practice.

2.4.3 Technology and privacy connection

Kandeh et al. (2018) and Hammons and Kovac (2019) believe that privacy and technology cannot be considered in isolation. They further cite that technological advancement and development such as the internet-of-things (IoT), social media, data management, mobile devices, geographical positioning system (GPS) location services and electronic government information services highlight the import of information privacy protection enforcement as key drivers to rapidly address data protection (Kandeh et al., 2018). Becker (2019) argues that a data subject's autonomy is severely diminished with the technology propagating various industries. These are evident in CCTV camera systems that watch people and automated number plate recognition (ANPR) systems. The monitoring capability is extended to the internet and social media platforms where the government and social media platforms can track people (Becker, 2019).

The subsequent sections provide a view of the implementation of technology that is overlaid with privacy considerations. This list is not exhaustive but attempts to provide a sense of how these two (2) aspects connect to each other.

2.4.4 Medical applications

Fazeldehkordi et al. (2019) describe data privacy in the medical field. They depict medical devices, sensors, equipment, systems, networks, and the internet converge, aiming to provide enhanced healthcare that is beneficial to patients and medical practitioners. For example, a heart disease patient utilising a pacemaker can share relevant data over the IoT. The patient's medical practitioner can monitor and diagnose the patient remotely. Alternatively, if distress is detected, the medical practitioner can send emergency medical services to assist to stabilise and transport the patient to a hospital.

In contrast to the immense value of this technology, it is at risk of attack and unauthorised access, highlighting the need for sound (Fazeldehkordi et al., 2019). Knight (2023) tenders another risk relating to the monetisation of medical data. The author notes an uptick with this practice where a user's medical data is captured by third parties, either a business entity or bad actor, to use for commercial purposes or nefarious activities, respectively (Knight, 2023).

2.4.5 IoT

Ochoa et al. (2019) expand on the IoT and smart cities by explaining that common items and environments are linked through the internet. It uses the data collected to improve the quality of life in smart cities. For example, the smart city is a system that collects real-time data using sensors and mobile devices throughout the city. The authors identify a problem with license plate recognition systems, citing that the data collected, including the captured license plate or number plate, the surrounding area, GPS coordinates, date and the time the image was captured for all motor vehicles. This includes motor vehicles used in crime and the vehicles of law-abiding citizens. It is also important to safeguard the personal information of suspected criminals as criminal proceedings may be in progress, and the unauthorised release of information linking a person to an alleged crime, whether innocent or guilty, may tarnish the reputation and social standing of the person (Ochoa et al., 2019).

Farnell et al. (2024) discuss the immense value that IoT delivers with the constant feed of sensor data. It allows the relevant authorities to monitor the health of a smart city and respond accordingly as alarms and alerts sound. Whilst IoT technology drives efficiency and

effectiveness, it is important to remain alert of potential bad actors that might attempt to exploit the system by breaching the feed to gather personal information (Farnell et al., 2024).

Nemmaoui et al. (2023) contend that technology service providers should ensure that there are governance statements like Terms of Service and Privacy Policy implemented for IoT. The authors further state that these governance statements have the potential to impact the choices that users make. However, it is concerning that the trends reveal that governance statements feature low on the user's priorities and often are not assimilated (Nemmaoui et al., 2023).

2.4.6 Biometrics implementation

Kasim et al. (2021:1) discuss privacy concerns in the implementation of biometric systems at airports. The authors outline that biometric systems constitute the processing of "faces, fingerprints, voices, signatures, and irises". They add that "less common methods that are also in use are palm print, hand geometry, vein pattern, retina, and gait recognition" (Kasim et al., 2021:1). Kasim et al. (2021) attributes a good uptake of the biometric systems in airports that is likely linked to the trade of users' private information for processing ease of use and efficiency.

2.4.7 Government use cases

Mzekandaba (2023) reports that the implementation of technologies like Automated Number Plate Recognition (ANPR), In-vehicle Cameras (IVC) and Body Worn Cameras (BWC) in Cape Town, South Africa, on 30 August 2023 enhanced the government's capability to monitor and track members of the public. Adams (2023) adds that this was further supplemented by the Western Cape Government's provincial traffic implementation of their instance of ANPR and IVC. Nemakonde (2024) discloses that, similarly, the South African Police Service (SAPS) has vowed to follow suit with the uptake of this technology to improve policing efforts. Nene (2024) states that the City of Cape Town recently procured the services of the "eye in the sky". The authors add that the technology consists of a human-crewed aircraft fitted with a powerful sensor to conduct surveillance for policing operations (Nene, 2024). BenRhouma et al. (2022) assert that the rapid proliferation of new technologies has further intensified privacy concerns due to new opportunities for surveillance, tracking, detection and watching people. These new technologies place increasing demands on authorities to safeguard privacy with law, policy, process and regulation (BenRhouma et al., 2022).

The privacy concessions afforded under government surveillance raised by BenRhouma et al. (2022) are concerning. Often, users do not know that they are being watched in the first place. Additionally, the practice must be strengthened to ensure that the government does not abuse its authority.

The next section on social media use and privacy detail the utilisation scale in South Africa. It further provides insight into the good and bad potential of social media for users.

2.5 Social media use and privacy

Kemp (2024) reports in Figure 1-1 that South Africa has a social media population of approximately twenty-six (26) million social media users as of January 2024, thereby constituting 42,8% of the country's total population. The platforms are valuable and often draw a lot of attention. Some of the attention is ill-intentioned and places users at risk (Beigi & Liu, 2020).

The next sections explore this and outline some notable considerations.

2.5.1 Social media popularity

BenRhouma et al. (2022) attribute the convenience of access to mobile devices coupled with the social value aspect of social media platforms as a significant driver in the popularity of the platforms for South African social media users. BenRhouma et al. (2022:118) state that the "smartphone" is firmly entrenched as a necessity that people cannot live without. The authors add that the rapid adoption of the "smartphone" led to its acclaim as the most valued technology instrument today. The instrument is considered highly valuable as it can fulfil a multitude of use cases. For example, a user can use a smartphone to make telephone calls, send text messages, take photographs, record videos, watch online content, make payments and interact on social media (BenRhouma et al., 2022). Liu et al. (2022) conclude that this convenient method for users to connect, share and interact contributes to the growth of the social media base. Alwafi and Fakieh (2024) claim that social media is used by a significant proportion of the global population in various cases. According to Hollenbaugh (2019) and Alwafi and Fakieh (2024), social media platforms like Facebook are valued by a multitude of users. The burgeoning popularity of the platform is a prime example of a user's social need to connect, share and interact. Kshetri and DeFranco (2020) describe social computing as an assortment of information technologies connected to the internet to facilitate interaction, social connection and sharing.

Botim (2024); Facebook (2024); Instagram (2024); LinkedIn (2024); Snapchat (2024); Strava (2024); Telegram (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) terms of service statements prescribe that a potential user must register to use the respective social media platform. The generic user registration process and platform utilisation scenario are depicted in Figure 2-3.

2.5.2 Social media registration process

Figure 2-3 encapsulates the basic steps of a registration process scenario with Step 1. Register, Step 2. Connect and Step 3. Share. The registration process encompasses a once-off capturing of the potential user's biographic information and contact details in Step 1. Moreover, Step 1 obligates the potential user to accept the Terms of Service, also referred to as Terms of Use for select platforms, to commence usage of the solution. Failure to accept the Terms of Service means that the potential user would need to opt-out and be unable to use the solution. Step 2 entails the registered user initiating interaction on the social media platform by seeking people, groups and things of interest. Lastly, Step 3 pertains to the users' interactions on the social media platform, where they can create posts, share content, and state opinions within the confines of the governance structure. Terms of Service and Privacy Policy for respective social media platforms are occasionally updated and circulated to users for information and acceptance.

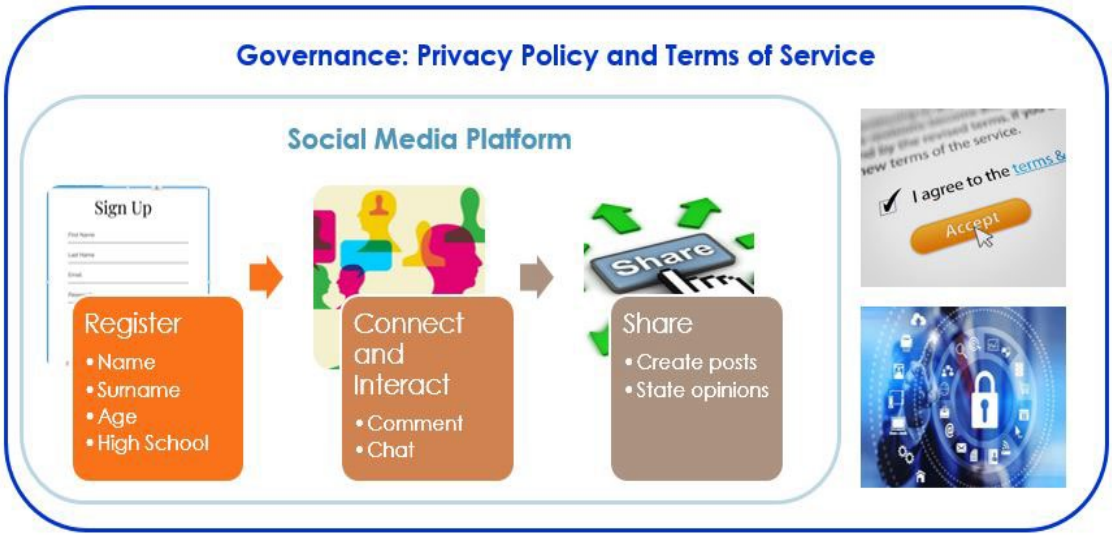


Figure 2-3: Social media usage (Adapted from research proposal, 2022)

2.5.3 Influencers and disingenuous user profiles

According to Arzoglou et al. (2023), social media platforms have given rise to an evolution in the way that humans connect, forging an asynchronous medium between individuals, groups and communities. The authors conclude that social media users adopt an online persona. This persona may authentically emulate the user or may be an inflated portrayal of how a user would like to be perceived. The latter may be ascribed to exaggerating their persona through possessions and experiences to draw attention and likes. A need for a social media persona to build a brand may be linked to securing popularity or financial gain. Moreover, these users may ascribe to reworking the photographs and media to cast an image of perfection (Arzoglou et al., 2023). Arzoglou et al. (2023) present that data privacy is a key consideration with the immense volumes of data that pervades social media platforms.

2.5.4 Risk potential

Arzoglou et al. (2023) assert that privacy is a key consideration for social media users with the potential for breach that can be categorised as either self-inflicted, where the user places themself in a compromising situation or via a third party-inflicted privacy attack (Arzoglou et al., 2023). Beigi and Liu (2020) and Kshetri and DeFranco (2020) assert that the value offered by social media to the sizeable South African social media base inadvertently attracts malicious actors intent on committing identity fraud, hacking to use or sell personal information, surveillance and cyberbullying. The authors state that Facebook utilisation by South African

social media users reveals some disturbing data privacy trends (Beigi & Liu, 2020; Kshetri & DeFranco, 2020). Beigi and Liu (2020) are of the opinion that the scale and abundance of private data available on social media primes the platforms for exploitation by bad actors.

2.5.5 Peer pressure

Arzoglou et al. (2023) tenders that individuals may succumb to peer pressure. The authors advance that an individual may be encouraged to join a social media platform for the sake of inclusivity and to satisfy the fear of missing out. Additionally, the authors state that an individual may join a social media platform to stop or circumvent ridicule by their peers. In both scenarios, the user may not stay true to their regular data privacy decision-making logic and may not fully comprehend the risks of the new platform (Arzoglou et al., 2023).

2.5.6 Privacy calculus

Lacity and Coon (2024) posits that there is significant value attributed to privacy. The authors explain that good privacy logic can be overturned through the offering of incentives to an individual in exchange for something. An example is where a user is offered as mapping service in exchange for their live location tracking. The service provider can use the location tracking for themselves to monetise or for sale to third parties (Lacity & Coon, 2024).

Abdelaziz et al. (2019) allude that the Google Corporation provides its Gmail electronic mail service at no cost to the public and electronically sniffs through users' electronic mail to discover marketing opportunities. Terms of Service statements do refer to this act, but users are quick to concede their privacy. Users often skip the opportunity to read the Terms of Service or apply wholesale acceptance of the terms to use a free product, application or service (Abdelaziz et al., 2019).

Arzoglou et al. (2023) explain the concept of privacy calculus. The authors describe this concept as involving a user's conscious exploration of a gratuitous product or service in exchange for something of value to the service provider. A user weighs up the associated data privacy threat of sharing personal information against the value of a free product or service (Arzoglou et al., 2023).

2.5.7 Privacy paradox

Bandara et al. (2021), Chen et al. (2021) and Arzoglou et al. (2023) introduce the privacy paradox involving disparate behaviour by users for general privacy compared to social media

data privacy practice. Arzoglou et al. (2023) describe the privacy paradox concept. The authors contend that when tested, social media users express a strong desire to protect their data, especially what is shared, with whom it is shared, when it is shared and how it is shared. Moreover, the how of sharing extends to the medium and the duration the data will be shared. When the authors evaluate the outlook exhibited against the results of data privacy behaviour observation, the outcome is highly contradictory. This mismatch between outlook and behaviour is referred to as the privacy paradox (Arzoglou et al., 2023).

Han et al. (2018) attribute erratic data privacy practices to dissimilarities in demography, technical aptitude, general usage and the need for social recognition. The authors explain that people provide the impression of expressing privacy concerns yet do very little to protect themselves. Their approach to privacy management uses a basic risk aversion algorithm to answer the question of whether the reward or benefit is worth the risk. The authors allude that the relevant person's knowledge and bias drive the decision-making process. The knowledge and bias are shaped by the person's demography, culture, belief system, upbringing and community (Han et al., 2018).

Bandara et al. (2021), Chen et al. (2021), and Arzoglou et al. (2023) present the privacy paradox. The studies conducted to arrive at these findings are limited to the contexts where these studies were conducted. This means that the views cannot appropriately be generalised to the South African context, given the diverse demographics, culture and communities.

2.5.8 Privacy Fatigue

Alwafi and Fakieh (2024:1) present the concept of "privacy fatigue". The authors outline that "privacy fatigue" elicits overwhelming feelings of tiredness, annoyance and frustration from the constant implementation of "Information Privacy Awareness (IPA)". IPA pertains to the social media user remaining vigilant of data privacy threats and applying the necessary precautions against the bombardment of targeted marketing whilst slowly wearing the user down until fatigue (Alwafi & Fakieh, 2024).

The idea of privacy fatigue by Alwafi and Fakieh (2024) is interesting. However, the South African context consists of diverse demographics, cultures and communities. It should be considered in the South African context as these arguments may not be generalisable.

The next section on governance in social media describes the legal instruments for social media and data privacy management in South Africa. This section is extremely important as it provides a baseline for these tools that will be used in subsequent parts of the study.

2.6 Governance in social media

Social media service providers include a Terms of Service, also known as Terms of Use, and Privacy Policy sections on the platform describing the rights of the service provider and the rights of the user. Botim (2024); Facebook (2024); Instagram (2024); LinkedIn (2024); Snapchat (2024); Strava (2024); Telegram (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) states their terms of service statements on their respective websites and applications.

In general, the Terms of Service are stated to provide coverage for the service provider. Moreover, social media service providers have a statutory obligation to compile and implement a Privacy Policy to safeguard the privacy of users. Lastly, social media service providers publish other policies and guidelines for themselves and third parties that operate on their platform.

In short, the purpose of the Terms of Service is to:

- Protect the social media platform.
- Determine the code of conduct.
- Mitigate liability claims.
- Safeguard the social media platform against disputes between third parties, i.e. other users and entities.
- Manage the expectations of the user.
- Stipulate the condition that the user accepts the social media platform's Privacy Policy.

Nemmaoui et al. (2023) and Hanlon and Jones (2023) convey that a Terms of Service, Privacy Policy and Terms and Conditions statements constitute legal agreements between the user and the service provider. The overall concept of these legal agreements is well-intentioned but is structured and written in a way that the user battles to grasp. This leads to users accepting the conditions that either do not understand them or do not read them. The authors estimate that more than 90% of technology users accept the conditions without knowing what they consented to (Nemmaoui et al., 2023; Hanlon & Jones, 2023).

The Terms of Service and Privacy Policy for several social media service providers are reviewed in the sections that follow.

2.6.1 Terms of service

Botim (2024); Facebook (2024); Instagram (2024); LinkedIn (2024); Snapchat (2024); Strava (2024); Telegram (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) necessitates a user registering for the platform to accept and comply with the conditions prescribed by the Terms of Service. Becker (2019) states that modern online platforms like social media service providers require a user to accept their Terms of Service to use the platform. The author adds that numerous concessions are entrenched within the Terms of Service. This allows the social media service provider to target users for marketing, track user utilisation behaviour, permit studies, and share user data with third parties (Becker, 2019). Kuenzler (2022) states that individuals have the final say in which social media platforms they opt to use. The author relays that individuals have far more power to affect change in the Terms of Service of social media platforms than they realise, especially where the user is the creative talent for the platform, uploading content and driving interest on the platform. Should users remain steadfast in their demands for change, the respective social media platform would comply. The assertion is rooted in the business model of social media platforms, where the user is ultimately the data provider (Kuenzler, 2022).

Botim (2024); Facebook (2024); Instagram (2024); Snapchat (2024); Strava (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) Terms of Service prescribes a minimum age for users. This is generally stated as a minimum of 13 years or older. LinkedIn (2024) and Telegram (2024) have a minimum age for users of 16 and 18 years of age, respectively. Exceptions are made where a parent or guardian of a child under the minimum age can assent to the minor using the social media platform under their supervision. A parent or guardian consenting to this accepts liability for potential negative outcomes. Additionally, the Terms of Service stipulates different minimum ages for users in specific countries. Hanlon and Jones (2023:2) recognise the minimum age requirement as the “age of digital consent” for the Terms of Service.

English is the most prevalent language used for the Terms of Service. A few other languages are available, but this is severely limited. This fact is problematic as it does not encourage other language groups to read the Terms of Service. This decision is peculiar as there are so

many solutions available to automatically translate the Terms of Service. Furthermore, it presents exclusionary practices and may lead to ill-informed users.

Botim (2024); Facebook (2024); Instagram (2024); LinkedIn (2024); Snapchat (2024); Strava (2024); Telegram (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) Terms of Service generally conveys that the user retains ownership of the data and content they upload. The user essentially waives their right to privacy for the uploaded content unless their privacy settings stipulate differently. The social media platforms' Terms of Service allow them to utilise the data and content as they deem fit without infringing on intellectual property rights. The social media platform affords themselves the right to store, copy, share and reuse uploaded content. Moreover, social media platforms reserve the right to market products and services to users. This may manifest as recommendations or targeted advertisements. A social media platform can track user behaviour or platform usage. These metrics can either be used by the social media service provider to inform marketing endeavours or shared with third parties like platform affiliates and advertisers. It further uses this data to target connections with other users. Lastly, the social media platforms collect user data for the purposes of the Law.

Obar and Oeldorf-Hirsch (2022) state that more than 75% of adults over the age of 50 years are inclined to completely ignore the Terms of Service without opening or reading it. The authors add that many users open the Terms of Service but spend less than an average of one (1) minute on it (Obar & Oeldorf-Hirsch, 2022). Yerby and Vaughn (2022) contend that the Terms of Service and Privacy Policy documents of social media platforms are lengthy and aim to obfuscate the information for the reader

A summary of the Terms of Service is provided in Table 2-2.

2.6.2 Privacy policy

Botim (2024); Facebook (2024); Instagram (2024); LinkedIn (2024); Snapchat (2024); Strava (2024); Telegram (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) prescribe their respective Privacy Policy statements. The Privacy Policy statements of the social media platforms listed in Table 2-2 obligate a user to accept and comply with the conditions prescribed by the Privacy Policy of the social media platform. This is assented to when the user accepts the Terms of Service upon registration. The Privacy Policy statements further outline the rights of the social media service providers in the overall

management and handling of the data. A user's right to privacy is relayed in the policy, including the protection and recourse options afforded to them.

Nemmaoui et al. (2023) note that the Privacy Policy is a legislative prescript imposed on social media service providers and other entities. The authors explain that the Privacy Policy conforms to the law of the country where the service provider offers their service and relays how the personal information of users will be processed (Nemmaoui et al., 2023).

English is the most prevalent language used in the Privacy Policy. A few other languages are available, but this is severely limited. This fact is problematic as it does not encourage other language groups to read the Privacy Policy. This decision is peculiar as there are so many solutions available to automatically translate the Privacy Policy. Furthermore, it presents exclusionary practices and may lead to ill-informed users.

A summary of the Terms of Service and Privacy Policy are combined per social media platform in Table 2-2. The sentiments have been extracted from the social media platforms in a bid to have an enhanced understanding thereof and against which to evaluate the data collected in the study.

Table 2-2: Terms of service and Privacy policy summary for social media platforms (Adapted from social media platforms, 2024)

PLATFORM	PLATFORM OWNER	TERMS OF SERVICE IN OFFICIAL SOUTH AFRICAN LANGUAGES	DATA OWNER: POST UPLOAD	USER AGE RESTRICTIONS	PERMISSIONS CEDED BY THE USER TO THE PLATFORM	REFERENCE	DATE ACCESSED
Facebook Terms of service	Meta	English; Afrikaans	User	>= 13 years old	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it. • Right to store, copy, share and reuse uploaded content • Right to market • Waiver right to privacy for the uploaded content • User behaviour or platform usage tracking in respect of viewing advertised content may be shared with advertisers • Targeted connections with other users and advertisers across Meta platforms • Collect user data for the purposes of the Law	Facebook (2024)Facebook (2024)Facebook (2024)Facebook (2024)	15/04/2024
X (aka Twitter)	X Corp	English	User	>= 13 years old	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it. • Right to store, copy, share and reuse uploaded content	X (2024)X (2024)X (2024)X (2024)	

PLATFORM	PLATFORM OWNER	TERMS OF SERVICE IN OFFICIAL SOUTH AFRICAN LANGUAGES	DATA OWNER: POST UPLOAD	USER AGE RESTRICTIONS	PERMISSIONS CEDED BY THE USER TO THE PLATFORM	REFERENCE	DATE ACCESSED
					• Shared or uploaded content affords other users the same rights mentioned above • Waiver right to privacy for the uploaded content • Right to market		
Instagram	Meta	English	User	>= 13 years old	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it. • Right to store, copy, share and reuse uploaded content • Right to market • Waiver right to privacy for the uploaded content • User behaviour or platform usage tracking with respect to viewing advertised content may be shared with advertisers. • Targeted connections with other users and advertisers across Meta platforms • Collect user data for the purposes of the Law	Instagram (2024)Instagram (2024)Instagram (2024)Instagram (2024)	
TikTok Terms of service	TikTok Pte. Ltd.	English	User	>= 13 years old, with exceptions for certain areas	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it	TikTok (2024)TikTok (2024)TikTok	

PLATFORM	PLATFORM OWNER	TERMS OF SERVICE IN OFFICIAL SOUTH AFRICAN LANGUAGES	DATA OWNER: POST UPLOAD	USER AGE RESTRICTIONS	PERMISSIONS CEDED BY THE USER TO THE PLATFORM	REFERENCE	DATE ACCESSED
					• Right to store, copy, share and reuse uploaded content • Right to market • Waiver right to privacy for the uploaded content • Disclosure of identity to a third party where they have upheld claims of intellectual property theft • The user chooses whether to post privately or publicly	(2024)TikTok (2024)	
WeChat (Utilisation internationally) Weixin (utilisation in China)	WeChat International Pte. Ltd. Or Tencent International Services Europe BV	English	User	>= 13 years old	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it. • Right to store, copy, share and reuse uploaded content • Right to market • Waiver right to privacy for the uploaded content • Affiliate companies and third parties afforded the concessions as mentioned earlier. • Option to view third-party content, products and services via the WeChat platform subject to the third party's respective terns of use	WeChat (2024)WeChat (2024)WeChat (2024)WeChat (2024)	

PLATFORM	PLATFORM OWNER	TERMS OF SERVICE IN OFFICIAL SOUTH AFRICAN LANGUAGES	DATA OWNER: POST UPLOAD	USER AGE RESTRICTIONS	PERMISSIONS CEDED BY THE USER TO THE PLATFORM	REFERENCE	DATE ACCESSED
SnapChat	Snap Inc.	English	User	>= 13 years old (unless your applicable legislation stipulates differently)	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it • Right to store, copy, share and reuse uploaded content • Content categorised as Public can be shared with third parties. • Right to market • Store select personal information on the user necessary for user account registration and payment where applicable. • Device permissions, where applicable	Snapchat (2024)Snapchat (2024)Snapchat (2024)Snapchat (2024)	
LinkedIn	LinkedIn Corporation © 2024	English	User	>= 16 years old	• Right to market/suggest • Right to store, copy, share and reuse uploaded content • Share posts and media are available to other users to view, use, copy or share	LinkedIn (2024)LinkedIn (2024)LinkedIn (2024)LinkedIn (2024)	
YouTube	Google LLC		User	>= 13 years old	• Subjects the user to their advertising policies where a user advertises on the platform	YouTube (2024)YouTube (2024)YouTube	

PLATFORM	PLATFORM OWNER	TERMS OF SERVICE IN OFFICIAL SOUTH AFRICAN LANGUAGES	DATA OWNER: POST UPLOAD	USER AGE RESTRICTIONS	PERMISSIONS CEDED BY THE USER TO THE PLATFORM	REFERENCE	DATE ACCESSED
					• Right to market	(2024)YouTube (2024)	
WhatsApp Terms of service	WhatsApp LLC (part of Meta Companies)	English	User	>= 13 years old	• Allow for analysis of user use of the platform • Assess the efficacy of business transactions and marketing • Share information with and receive from Meta Companies	WhatsApp (2024)WhatsApp (2024)WhatsApp (2024)WhatsApp (2024)	
Telegram	Telegram Group Inc.	English	User	>= 18 years old	• Targeted connections with other users and advertisers	Telegram (2024)Telegram (2024)Telegram (2024)Telegram (2024)	
Other: Strava	Strava Inc.	English	User	>= 13 years old	• Ownership is relinquished, in part, when uploaded, and the platform is permitted to use it. • The platform can use user behaviour or platform usage tracking to make recommendations. • Targeted connections with other users • The main purpose of the app is to “Live Track” a user whilst they are participating in sport or	Strava (2024)Strava (2024)Strava (2024)Strava (2024)	

PLATFORM	PLATFORM OWNER	TERMS OF SERVICE IN OFFICIAL SOUTH AFRICAN LANGUAGES	DATA OWNER: POST UPLOAD	USER AGE RESTRICTIONS	PERMISSIONS CEDED BY THE USER TO THE PLATFORM	REFERENCE	DATE ACCESSED
					exercise; therefore, the user's location services are enabled whilst using the app to plot their course, speed, sensor feeds and other metrics.		
Other: Botim	Algento DMCC	English	User	Legal age of maturity in the jurisdiction where you are resident under the applicable laws	• Right to store, copy, share and reuse uploaded content • Waiver right to privacy for the uploaded content • Right to access user contacts stored on the user's device • User behaviour or platform usage tracking can be used by the platform to make recommendations • Right to market	Botim (2024)Botim (2024)Botim (2024)Botim (2024)	

2.6.3 Legal liability

Nemmaoui et al. (2023) and Hanlon and Jones (2023) convey that a Terms of Service, Privacy Policy and Terms and Conditions statements constitute legal agreements between the user and the service provider.

Botim (2024); Facebook (2024); Instagram (2024); LinkedIn (2024); Snapchat (2024); Strava (2024); Telegram (2024); TikTok (2024); WeChat (2024); WhatsApp (2024); X (2024); YouTube (2024) ascribe their Terms of Service and Private Policy as the legal instruments to address certain contravention of the rules of the platform. Additionally, the service providers share the instances in which they would be legally compelled to share the user's data with a policing authority, subject to due process.

Illidge (2024) reports that legal liability in respect of defamation in South Africa can be enforced from the minimum age of seven (7) years of age. An incumbent can be sued for defamatory remarks submitted via social media platforms. Additionally, where a child is above twelve (12) years of age, and an allegation is lodged at the South African Police Services (SAPS), the child can be taken into custody and legally processed as the law provides (Illidge, 2024a).

The abovementioned section on governance in social media describes the legal instruments for social media and data privacy management in South Africa. It explicitly outlines the protections afforded to users and the social media platforms. The next section on privacy breaches highlights the failures of these legal instruments and users' ability to ingest the legal information.

2.7 Privacy breaches

According to Zuboff (2019), the 9/11 terror attacks in the United States of America on 11 September 2001 led to significant changes in the surveillance of the country. This tragic incident culminated in the formulation of numerous government agencies tasked with increased surveillance activities with far more power and autonomy. These activities included facial recognition, monitoring of financial transactions, electronic mail accounts, and mobile phones, including listening to mobile phone calls, text messaging, accessing geolocation information and monitoring social media in the name of national security. Kshetri and DeFranco (2020) and Hajli et al. (2021) share that several governments and large technology companies continually monitor and track people using various media to gather pieces of

personal information to exploit financial and political opportunities at the expense of the data subjects.

According to Malinga (2024) and Mzekandaba (2024, privacy breaches in South Africa occur frequently and are manifesting increases year-on-year. Numerous examples of the most notable privacy breaches in South Africa acknowledged include:

1. Experian breach affected 24 million South African individuals and 800,000 businesses (Hosken, 2020);
2. A Facebook breach affecting 14.3 million South African users' publicly available personal data was web-scraped and uploaded online for anyone to access Delport (2021);
3. TransUnion ransomware attack by the N4ughtySecTU hacking group impacted the personal information of 54 million South Africans in 2022 (Mzekandaba, 2023);
4. Hi-Fi Corp and Incredible group of companies experienced a breach in June 2023, impacting the records of 500,000 South African customers (Illidge, 2024b);
5. The OneDayOnly ransomware data breach by the KillSec hacking group in South Africa (Illidge, 2024b) and
6. The Liberty Holdings' electronic mail repository breach (Malinga, 2024).

Kshetri and DeFranco (2020) acknowledge that technology service providers assert that they have acquired consent to harvest users' data. The authors state that service providers predominantly do not have the rights to harvest the data, and cases where users consented, would have been facilitated by ill-informed users (Kshetri & DeFranco, 2020).

2.7.1 Financial sector breach

Hosken (2020) describes that the latest large-scale privacy breach realised the exposure of the sensitive information of approximately twenty-four (24) million South Africans and 800,000 businesses held by Experian. The company, Experian, is a credit bureau housing millions of records, including mobile phone numbers, identity numbers, addresses, electronic mail addresses, banking details, work details, salary details, and every financial transaction ever entered by every person on the database. Hosken (2020) cautioned that the breach could represent approximately ninety per cent of the working South African population and could result in fraudulent financial transactions using the leaked information.

Moodley (2022) reported the Transunion breach in March 2022. Transunion is an international credit bureau housing millions of consumers' personal information. The breach allowed access to the personal information of approximately fifty-four (54) million South Africans. Thorne (2024) discusses the outlook of privacy breaches in South Africa. The authors note an incremental escalation in technology-related crime. Losses amounting to more than twenty million rand (R20,000,000) between 1 January 2024 and 30 June 2024 show a 14% surge in damages. "Ransomware" incidents account for a significant portion of these transgressions. However, a peculiar breach type involving the accidental release of personal information to the wrong party has garnered the attention of privacy breach specialists due to the rise in damage claims from affected parties. As a result, South Africa is placed fourteenth internationally for damage claims, amassing fifty million rand (R50,000,000) (Thorne, 2024).

2.7.2 Government surveillance

Kshetri and DeFranco (2020) discuss the tracking of a group of people by the Chinese government. The authors explain that CCTV camera networks in China can record and apply "facial recognition" software in real-time to keep track of their movements. Unethical behaviour is portrayed in these acts as there is bias embedded in the artificial intelligence to seek out this group of people (Kshetri & DeFranco, 2020).

2.7.3 Technology wearables

Fyke et al. (2019) allude to the fact that many people use mobile phones and wearable devices. These devices continuously collect copious amounts of data and frequently connect to other devices and wireless networks to synchronise the data with users' accounts. This is useful for users but lends itself to potential abuse by large technology corporations, governments or malicious actors. The devices have the functionality to plot movements inadvertently using an array of motion sensors within a user's home, place of work or public spaces. This might be of interest to a malicious actor intending to map the layout of a sensitive building or to identify an individual's movement patterns.

According to Shokri et al. (2011) and Primault et al. (2019), GPS or location-based services on a mobile device combined with a mobile device application allow for useful functionality for the voluntary live tracking of friends and family, navigation services and weather forecasting services. However, other parties can use the technology to track a person and analyse their movements. A practical example illustrates that certain persons could be identified as from the Muslim religion based on their lack of movement at certain times of the day. As a result of

9/11, the Muslim community fell victim to oppression and was branded as terrorists. Muslims observe religious prayers at least five times a day, during which the person is in a fixed position for several minutes. The times of prayer differ by geographical position or city, and prayer times constantly shift from one day to the next as they are linked to sunrise and sunset. Prayer timetables are freely available for all to access on the internet. These pauses in movement could also be overlaid with known places of worship or mosques. Therefore, a party tracking various persons using their GPS and sufficient background knowledge could easily establish which persons are Muslim for purposes of targeted surveillance. The authors propose the use of Location Privacy Protection Mechanisms (LPPM) to mask the GPS coordinates (Shokri et al., 2011; Primault et al., 2019).

Fung et al. (2010) and Tsou et al. (2021) present the concept of Privacy-Preserving Data Publishing (PPDP). This concept describes the process of responsibly sharing data whilst sufficiently ensuring the preservation of privacy through efforts to facilitate the anonymisation of the data. (Fung et al., 2010; Tsou et al., 2021). Tsou et al. (2021) suggest that people's data privacy must be achieved with information usability remaining intact after the anonymisation efforts.

2.7.4 Mobile phones

Kshetri and DeFranco (2020) mention that the major smart phone manufacturers may have been complicit in data breaches entailing user tracking. The authors add that the tracking method did not require the user to provide consent to the tracking. Moreover, the user's smartphone does not need to be enabled for GPS tracking so that manufacturers can access the tracking information (Kshetri & DeFranco, 2020). BenRhouma et al. (2022) allege that a smartphone factory reset does not remove all the information on the device. This means that an individual with the required technical skill can retrieve information remnants after the factory reset, including social media data. The authors contend that devices sold on the used phone market and accessible through other circumstances would allow someone to retrieve the data. The retrieved data could be sufficient to initiate illicit activities like identity theft or hacking of the user's accounts (BenRhouma et al., 2022).

The abovementioned section on privacy breaches casts the general concerns in South Africa and globally. The next section narrows the focus of privacy breaches by highlighting specific instances of the failures in social media.

2.8 Privacy breaches in social media

Gilbert (2018) mentions that social media breaches constitute more than 4.5 billion records affected between 1 January 2018 and 30 June 2018. Anti-Phishing Working Group (2024) reports that phishing attacks realised 963,994 and 877,536 victims for quarters one (1) and two (2), respectively. The report acknowledges that social media platforms account for a significant proportion of the total phishing attacks at 32,9% for the second quarter of 2024 (Anti-Phishing Working Group, 2024).

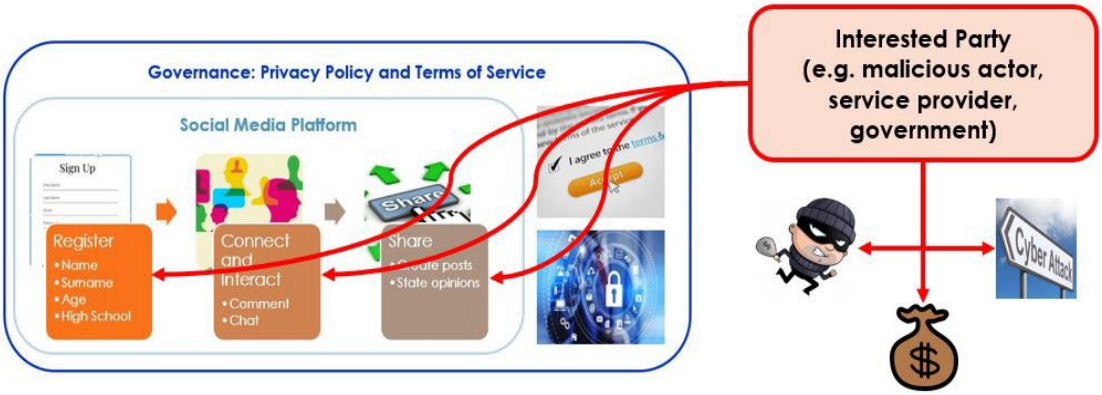


Figure 2-4: Social media usage and potential privacy breaches (Adapted from research proposal, 2022)

Section 2.5 describes the social media registration process and the platform utilisation scenario. Figure 2-4 adds to this by depicting how an interested party can exploit the personal data captured at each step of the process to monetise, launch a cyber-attack or steal the personal data. According to Beigi and Liu (2020), publishers of social media data have a significant responsibility to safeguard the privacy of users. The authors note that this can be achieved through the sanitisation of the data prior to release for publication.

The next sections explore some high-profile and some lessor known social media platform breaches.

2.8.1 Facebook

Hu et al. (2019) and Qureshi et al. (2020) state that cyber harassment pertains to incessant behaviour targeted toward a person with the intent to cause the person heightened feelings of

distress and fear of physical injury. Hu et al. (2019) and Qureshi et al. (2020) argue that cyber harassment is usually the precursor to threats of violence and the posting of untruths of the person on social media. The author states that perpetrators may attempt to impersonate their victim and seek out their victim's personal information to reveal online (Hu et al., 2019); (Qureshi et al., 2020). According to Messing et al. (2020), technology-based stalking is the evolution of physical stalking to the technological realm and allows a perpetrator to monitor the movements of their victim.

Delport (2024) examines the Facebook breach, where the personal data of at least 530 million users was exposed. The author confirms that 14.3 million South Africans are impacted by this breach (Delport, 2024).

Zuboff (2019) states that the Facebook social media platform allows Facebook and governments to profile or track users for the aims of economic gains and national security, respectively.

According to Ayaburi and Treku (2020),Facebook users' privacy concerns were realised with the data privacy breach involving the London-based business Cambridge Analytica in 2014. Kshetri and DeFranco (2020) note that the Cambridge Analytica incident includes the personal information of eighty-seven (87) million users to profile and tailor advertisements to solicit votes for the intended political candidate. The authors contend that Facebook is guilty of infringement of the data privacy of their users as the organisation's privacy statement conveys this commitment. The personal information of users was shared, void of their consent, for the use of profiling users (Ayaburi & Treku, 2020; Kshetri & DeFranco, 2020).

Kshetri and DeFranco (2020:4) report that Facebook received a significant financial penalty in an unrelated incident. The social media platform was found to have contravened privacy laws with its artificial intelligence algorithm that detected the identity of an individual based on their facial characteristics in uploaded photographs and videos. This activity was declared self-serving for the social media platform as it was engineered to harvest data about individuals' movements and associations for financial gain. The authors argue whether "facial recognition" is deemed appropriate when it is linked to a purpose like the greater good. For example, a child is kidnapped by an assailant, and their face is captured by closed-circuit television (CCTV) cameras operated by a city's policing authorities. The usage of CCTV footage and facial recognition would benefit the policing endeavour to recover the victim (Kshetri & DeFranco, 2020).

Kuenzler (2022) reports that the Düsseldorf Higher Regional Court (HRC) found Facebook guilty of contravening its Terms of Service. The social media platform coerced users to consent to the assimilation of their third-party data with their Facebook data. The users had to accept the bundled consent to use the Facebook platform (Kuenzler, 2022).

Knight (2023:751) reports that landmark legal decisions on women's rights in numerous states of the United States of America (USA) realised the ban on abortions. The act of abortion in any of these states criminalises it and means that anyone involved in it would face prosecution. The author states that several allegations were lodged with the courts alleging that Facebook contravened privacy laws, including the "Health Insurance Portability and Accountability (HIPAA) prescripts. HIPAA affords a person the "right to medical privacy". The lawsuits describe that Facebook, including the Meta parent organisation, embedded monitoring mechanisms on the websites for any of any potential health entities capable of abortions. This blatant privacy violation means that a potential online visitor of one of these websites could be flagged as seeking an abortion, thereby initiating a legal process to apprehend these individuals (Knight, 2023).

2.8.2 Google

Abdelaziz et al. (2019) believe that the Google Corporation provides its Gmail electronic mail service at no cost to the public and electronically sniffs through users' electronic mail to discover marketing opportunities. The authors contend that the Terms of Service do refer to this act but that users are quick to concede their privacy. Users often skip the opportunity to read the Terms of Service or apply wholesale acceptance of the terms to use a free product, application or service (Abdelaziz et al., 2019).

Kshetri and DeFranco (2020) revealed that Google also illegally accessed patients' medical records. The data encompassed medical facility visits, medical tests and medical practitioner records. The medical records were perused by Google's employees (Kshetri & DeFranco, 2020).

Boukoros and Katzenbeisser (2017) and Kshetri and DeFranco (2020) detail the modern convenience of technology by autonomously tailoring user preferences based on the tracking of the user's historical interactions with an application through the recording and analysis of the microdata to learn about the user's preferences and interests. This allows the application to profile the user and make recommendations on items of interest under the auspices of the user application experience improvement. However, it allows a company to better market

goods and services to users. This highlights that the microdata generated poses a significant risk to user privacy (Boukoros & Katzenbeisser, 2017) Kshetri & DeFranco, 2020).

2.8.3 Google Maps

Kshetri and DeFranco (2020:6) state that the Google Corporation conducts a diverse pool of business ventures. The company has developed numerous offerings. However, “Google Street View” contravened numerous privacy rules when it captured imagery. The problem does not necessarily lie with the initial capturing. It is the post-capturing activity where Google processes the imagery to reveal data that could be consumed by their business customers, such as insurance providers (Kshetri & DeFranco, 2020).

2.8.4 Third-party profiling of social media accounts

Espinosa and Xiao (2020) state that Twitter social media accounts can easily be profiled for monetisation. They describe a modern direct marketing data gathering exercise using Twitter by identifying the gender from the Twitter user’s first name, a profile description, pictures and inferences of the gender of the user through personal pronoun usage in posts. Furthermore, the authors explained that Twitter has a simple privacy setting where an account is set to private or public. The default setting is public, and users who are ignorant of the privacy settings will continue to operate their user accounts as public (Espinosa & Xiao, 2020).

After exploring the instances of social media breaches, the next section considers the human aspect of data privacy management. This section delves into the general outlook of users and how culture, community and belief systems shape this outlook.

2.9 Human behaviour in data privacy

Lacity and Coon (2024) contrasts on acceptable behaviour in public versus private. The authors appraise private behaviour and establish that the outlook of an individual is moulded during the early development years. Impressionable minors are groomed by elders and the community on acceptable behaviour and how to behave in various contexts. These learnings during childhood persist into adulthood, shaping the behaviours applied in a multitude of contexts (Lacity & Coon, 2024).

According to Bandara et al. (2021), people provide the impression of expressing privacy concerns yet do very little to protect themselves. The authors describe an approach to privacy management using a basic risk aversion algorithm to answer the question of whether the

reward or benefit is worth the risk. The relevant person considers the risk of accessing the internet and using social media against the potential breach of their privacy. The authors allude that the relevant person's knowledge and bias drive the decision-making process. The knowledge and bias are shaped by the person's demography, culture, belief system, upbringing and community (Bandara et al., 2021).

Al-Rabeeah and Saeed (2017) and Petronio and Child (2020) state that various genders view data privacy differently. The authors explain that women employ privacy logic independently, where each woman would determine their logic. This infers that no two women would necessarily apply identical privacy logic to achieve the outcome. Men are forecasted to follow a collective privacy logic. This implies that men are more consistent with repeatable results (Petronio & Child, 2020).

McNealy and Mullis (2019) state that culture delineates parameters by which data privacy is viewed and considered. The authors strongly contend that culture shapes the ground rules for data dissemination (McNealy & Mullis, 2019).

The next section transitions to the adoption of theory. This section considers the selection of the appropriate theories to better comprehend and cast deeper meaning for the research problem.

2.10 Adoption of theory

The study aims to determine the data privacy behaviour of adult social media users residing in South Africa. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms. Furthermore, the research objectives entail: 1. To explore the privacy management methods and techniques employed by adult social media users; 2. To determine the data privacy threat perception of adult social media users, and 3. To identify behavioural barriers to data privacy management implementation of adult social media. The aforementioned aim and objectives are fundamental to the theory and research decision selected for this study.

Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Petronio and Child (2020) contend that Communication Privacy Management (CPM) pertains to privacy decisions influenced by the user's cultural influences. The authors believe that the embedded culture and beliefs could

affect the behaviour of users (Petronio & Child, 2020). Al-Rabeeah and Saeed (2017) explain that CPM assists in understanding the way an individual organises their logic for data privacy protection. Al-Rabeeah and Saeed (2017) describe the Theory of Planned Behaviour (TPB) as the interconnection between an individual's belief structure and their behaviour. Barth and de Jong (2017) and McNealy and Mullis (2019) explain that the behaviour of an individual is determined by their predetermined belief system. This includes their perceptions of the intended outcome, norms and reward despite the associated risk (Barth & de Jong, 2017; McNealy & Mullis, 2019). McNealy and Mullis (2019:111) add that research involving CPM in the "social media context" is sparse and deserves attention. Several studies have been conducted on this problem globally. However, very few studies have been conducted in the South African context.

CPM and the TPB have previously been used in ICT studies, notably in IEEE Explore and the International Journal of Advanced Computer Science and Applications. The components depicted below provide the framework by which the data must be analysed and interpreted.

Table 2-3 Components of combined CPM and TPB theories

PRIVACY FACTORS CPM:	DECISION-MAKING MODEL TPB:	BOUNDARY COORDINATION OPERATION CPM:
• Legal • Emotion • Culture • Politics • Gender • Motivation • Context	• Attitude • Subjective norm • Behavioural control	• Boundary permeability • Boundary linkage • Boundary ownership

The Privacy Factors CPM are comprised of Legal, Emotion, Culture, Politics, Gender, Motivation and Context. According to Al-Rabeeah and Saeed (2017), the Legal, Culture and Politics aspects consider the implications of legislative mechanism, political decisions and the appetite for government legislation on the privacy management of users, respectively. Moreover, the Emotion component delves into the emotional reasoning of users whereas the Motivation component considers the drivers for users' privacy decision-making. The framework determines that the Genders aspect is representative of gender-specific

preferences. Lastly, according to the framework, the Context that the user finds themself in has an influence on the privacy decisions (Al-Rabeeah & Saeed, 2017).

Al-Rabeeah and Saeed (2017) describes the Decision-Making Model TPB as consisting of Attitude, Subjective norm and Behavioural control. Azad et al. (2023) states that the Decision-Making Model TPB components could be used to forecast the privacy decision-making of a user.

Boundary Coordination Operation CPM is comprised of Boundary permeability, Boundary linkage and Boundary ownership. McNealy and Mullis (2019) explain that the Boundary Coordination Operation CPM delineates the limits of the privacy decisions for these aspects. Boundary permeability relates to how narrowly or widely privacy decisions are applied. The latter two (2) aspects relate to the observation of sharing rules and understanding amongst the parties involved (McNealy & Mullis, 2019).

The combined Al-Rabeeah and Saeed (2017) CPM and TPB theory are illustrated in Figure 2-5 and consist of several components.

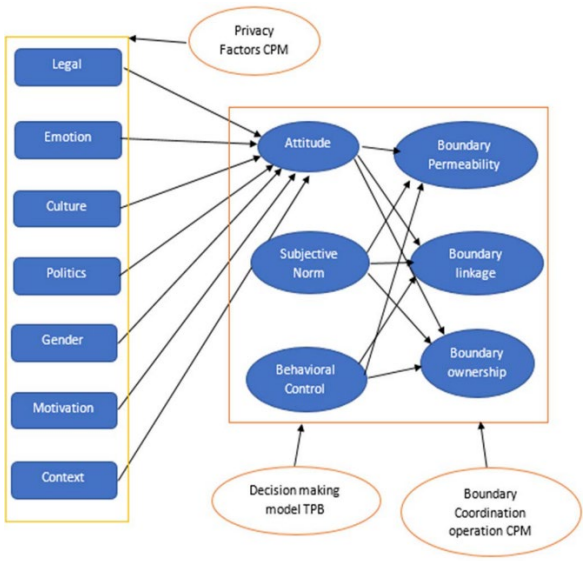


Figure 2-5: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017)

The next section discusses the opportunities for the research by highlighting the research gaps and the linkage to the research objectives of the study.

2.11 Research opportunity

2.11.1 Research gap

McNealy and Mullis (2019:111) add that research involving CPM in the “social media context” is sparse and deserves attention. Al-Rabeeah and Saeed (2017) recommend further study on privacy in light of the lack of studies conducted from a user’s perspective. The authors add that using CPM and TPB theory would be valuable in gaining a deep insight into the problem.

Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. It is acknowledged that the behaviour must be better understood by considering the impact of culture.

McNealy and Mullis (2019:111) add that research involving CPM in the “social media context” is sparse and deserves attention. The sentiment raised by the author resonates with the research objectives. A study employing a combined CPM and TPB theoretical framework study would be useful in better understanding the problem.

In respect to the context, South Africa is a diverse, multilingual, and culturally diverse ecosystem. The complexity of the culture necessitates a study to understand the problem. There are barely any studies conducted on data privacy, behaviour and social media in South Africa. Perhaps a study on the data privacy behaviour of social media users would assist in resolving the identified problem and formulating new ways of addressing this problem via more effective awareness initiatives. This may further the theoretical information. Moreover, it may inadvertently contribute to improved frameworks for designing awareness mechanisms and outcomes through the consciousness of cultural nuances.

2.11.2 Linkage to research objectives

The objectives of the research are: 1. To explore the privacy management methods and techniques employed by adult social media users; 2. To determine the data privacy threat perception of adult social media users, and 3. To identify behavioural barriers to data privacy management implementation of adult social media users. Each research objective discussed in 2.11.1 connects with a research gap.

The study aims to determine the data privacy behaviour of adult social media users residing in South Africa. Exploration of the reasons for the behaviour will allow the researcher to

develop a thorough understanding of the problem and contribute to the design of future data privacy awareness initiatives.

The next section provides the conclusion by providing a synopsis of this chapter.

2.12 Conclusion

A comprehensive literature review reveals that the concept of privacy has been around for several decades. However, after all this time, it is still evident that the concept has widely varied definitions describing it. Lacity and Coon (2024) defines privacy as the ability to control what is shared and with whom it is shared. Becker (2019:308) tenders the privacy definition as “the right to be left alone”. Furthermore, privacy is considered as physical privacy and the flexibility to manage your privacy.

Privacy takes its purpose in attempting to protect users against harm by devising safeguards against theft of personal information. This is driven by legislation, governance and procedure. The rise of technology is complicating the management of privacy. This relates to previously defined boundaries being redefined with technology upending what is possible and how things are done. It is crucial to embed good governance to ensure structure without stifling the technology. Internet and smartphone utilisation in South Africa are rising year-on-year despite the considerable digital divide (Statistics SA, 2019). A smartphone is considered a necessity, facilitating a low cost of entry to the internet and social media.

Kemp (2024) reports that South Africa has a social media population of approximately twenty-six (26) million social media users as of January 2024, constituting 42,8% of the total population in the country. This represents a considerable proportion of the population. The diverse, multilingual and varied cultural ecosystem comprising the South African population presents some interesting challenges when it comes to social media. The effect of language, gender, culture and community injects these users into a landscape with loads of potential. However, the same landscape is dotted with wolves waiting to pounce on unsuspecting victims through malicious attacks to rob them of their identity, personal information and finances.

Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Al-Rabeeah and Saeed (2017) and Petronio and Child (2020) contend that the Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user’s cultural

influences. McNealy and Mullis (2019:111) add that research involving CPM in the “social media context” is sparse and deserves attention.

The theoretical underpinnings are provided in this chapter. It has the potential to deepen comprehension of data privacy management behaviour using CPM and TPB in the South African context. Gaps are proposed in the literature review, where most literature has a Western, European or Middle East focus. Given South Africa’s unique identity, perhaps a study on the data privacy behaviour of social media users would assist in resolving the identified problem and formulating new ways of addressing this problem via more effective awareness initiatives.

CHAPTER 3: METHODOLOGY

3.1 Introduction

The methodology chapter is organised into 13 sections to address the Aim, Objectives, Research Question and Sub-research Questions (Table 3-1).

Section One (1) presents the Introduction, in which the researcher provides an overview of the proposed research study. Section Two (2) spans the Aim, Objective, Research question and Sub-research questions to establish the drivers for the research by relaying the intent of the study. Section Three (3) explains the application of the selected theories. Section Four (4) considers the research approach, and Section Five (5) discusses the research method. Section Six (6) relays the research design, and the data collection procedure is explained in Section Seven (7). Section Eight (8) spans the description of the data analysis, whereas Section Nine (9) considers the validity and reliability mechanisms of the study. Section Ten (10) describes the ethical considerations. The limitations and delineation of the study are sketched in Section Eleven (11). Section Twelve (12) outlines the data management, and Section Thirteen (13) delivers the conclusion for this chapter. This chapter provides the methodology that will be used to research the problem. The goal of the methodology is facilitated by the formulated research aim and objectives directing the research questions of the study to explore the data privacy behaviour of social media users in South Africa.

Table 3-1: Research question and Sub-research questions

(Adapted from research proposal, 2022)

NATURE	RESEARCH QUESTIONS	RESEARCH OBJECTIVES
Research Question **(RQ)**	What is the data privacy management behaviour of adult social media users?	
Sub-Research Question 1 **(SRQ1)**	How do adult social media users manage their privacy when interacting on a social media platform?	To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.
Sub-Research Question 2 **(SRQ2)**	What is the perceived privacy threat awareness level of adult social media users?	To determine the data privacy threat perception of adult social media users residing in South Africa.
Sub-Research Question 3 **(SRQ3)**	What are the behavioural barriers to privacy management implementation for adult social media users?	To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Al-Rabeeah and Saeed (2017) and Petronio and Child (2020) contend that the Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user's cultural influences. McNealy and Mullis (2019:111) add that research involving CPM in the "social media context" is sparse and deserves attention. Several studies have been conducted on this problem globally. However, very few studies have been conducted in the South African context.

The researcher will conduct a study that will explore through survey questionnaires how adult social media users residing in South Africa interact on social media platforms, specifically their treatment or management of their data privacy. The researcher intends to use embedded culture and beliefs as a lens to improve the understanding of user behaviour.

The research objectives in the next section outline the aim, objectives, research question and sub-research questions to stage the methodology chapter. These research objectives are fundamental to crafting a well-designed scientific study.

3.2 Research objectives

Hollenbaugh (2019) notes that millions of users globally value social media platforms, demonstrating the significant appeal of the technology. Al-Rabeeah and Saeed (2017) and Hollenbaugh (2019) contend that social media platforms' burgeoning growth and popularity are a prime example of a user's social need to connect, share and interact. User interaction and collaboration on social media platforms present a data privacy behaviour problem. The management of data privacy is a challenge given the potential for breaches that can be categorised as either self-inflicted, where the users place themselves in a compromising situation or via a third-party-inflicted privacy attack (Al-Rabeeah & Saeed, 2017). The implications of increased frequency and veracity of data privacy attacks mean that social media users may fall prey to one or more forms of data privacy breach.

The study is exploratory in nature, where the researcher will explore how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy. The Aim, Objectives, Research Question and Sub-research Questions below provide context to the study. The study is guided by the main and sub-research questions. It addresses the identified research problem in the study, which entails exploring data privacy management behaviours exhibited by adult social media users residing in South Africa. The research questions seek to understand whether the age, gender, language, culture and community of social media users influence their privacy management behaviour. This entails intangible aspects that can be described but not measured. The research objectives and questions will require the methodology to support the study.

3.2.1 Aim

The aim of the study is to determine the data privacy behaviour of adult social media users residing in South Africa. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

3.2.2 Objective

1. To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.

2. To determine the data privacy threat perception of adult social media users residing in South Africa.
3. To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

3.2.3 Research Questions

3.2.3.1 Research Question (RQ)

RQ: What is the data privacy management behaviour of adult social media users?

The research question addresses the identified research problem in the study. The primary purpose of the research is to explore the data privacy management behaviours exhibited by adult social media users residing in South Africa. Furthermore, the research question seeks to understand whether the culture of social media users influences their privacy management behaviour.

3.2.3.2 Sub-research Questions (SRQ)

SRQ1: How do adult social media users manage their privacy when interacting on a social media platform?

SRQ2: What is the perceived privacy threat awareness level of adult social media users?

SRQ3: What are the behavioural barriers to privacy management implementation for adult social media users?

Sub-research question 1 (SRQ1) explores the privacy management methods and techniques of adult social media users in South Africa. The main idea revolves around fully appreciating how the users use social media, what their beliefs are and how they interact on the social media platforms from a data privacy management perspective. Al-Rabeeah and Saeed (2017) and Bandara et al. (2021) view social media utilisation as problematic, given the potential for users to place themselves in harm's way or unwittingly fall prey to malicious attacks. Therefore, the researcher will attempt to better understand the interactions of social media users.

Sub-research question 2 (SRQ2) evaluates the perception of data privacy threats among adult social media users residing in South Africa. Beigi and Liu (2020) assert that social media platforms have become the hunting grounds for bad actors who harvest the wealth of personal

information that is freely available. The malicious actors can skilfully craft their attacks on social media users through a variety of means (Beigi & Liu, 2020). Moreover, Hajli et al. (2021) report concerning trends in social media companies exploiting user data, with or without consent, for a variety of use cases. The researcher will assess users' perceptions of data privacy threats to determine whether adequate data privacy management is implemented.

Sub-research question 3 (SRQ3) delves into the behavioural barriers to data privacy management of adult social media users. Bandara et al. (2021), Chen et al. (2021), and Arzoglou et al. (2023) discuss the privacy paradox where users exhibit erratic behaviour when managing their social media data privacy. The authors state that the erratic privacy practice is attributed to dissimilarities in demography, technical aptitude, general usage and the need for social recognition (Bandara et al., 2021). According to Chen et al. (2021), examining the human aspect of the data privacy management behaviour of users may provide clues to their weaknesses.

The Aim, Objectives, Research Question, and Sub-research Questions are fundamental to this study. These notions provide a structure and ensure that the researcher remains focussed on the study.

3.3 Theoretical framework

Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Petronio and Child (2020) and Al-Rabeeah and Saeed (2017) contend that the Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user's cultural influences. McNealy and Mullis (2019:111) add that research involving CPM in the "social media context" is sparse and deserves attention.

Creswell and Creswell (2018) and Biggs et al. (2022) note that researchers use theory to study the ethnic aspects of the community under observation. The authors add that the theory serves to better understand the social norms and habitual and cultural aspects of the participants so that they can appreciate the research problem holistically. Moreover, they state that researchers employ the theory as a lens using the demography, community and cultural context to create meaning (Creswell & Creswell, 2018; Biggs et al., 2022).

The study aims to determine the data privacy behaviour of adult social media users residing in South Africa. The researcher intends to explore the reasons for the behaviour to contribute

to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms. Furthermore, the research objectives entail: 1. To explore the privacy management methods and techniques employed by adult social media users; 2. To determine the data privacy threat perception of adult social media users, and 3. To identify behavioural barriers to data privacy management implementation of adult social media. The aforementioned aim and objectives are fundamental to the theory and research decision selected for this study.

The study is exploratory in nature, where the researcher will explore through survey questionnaires how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy. The researcher intends to use the combined Al-Rabeeah and Saeed (2017) CPM and TPB theory as a lens to better understand the data privacy management behaviour of users by applying the theoretical framework to the study's questionnaire formulation, analysis and discussion. The combined Al-Rabeeah and Saeed (2017) CPM and TPB theory are illustrated in Figure 3-1 and consist of several components. The components depicted below (Table 3-2) provide the framework by which the data must be analysed and interpreted.

Table 3-2 Components of combined CPM and TPB theories

COMBINED COMPONENTS	DECISION-MAKING MODEL TPB:	BOUNDARY COORDINATION OPERATION CPM:
• Legal • Emotion • Culture • Politics • Gender • Motivation • Context	• Attitude • Subjective norm • Behavioural control	• Boundary permeability • Boundary linkage • Boundary ownership

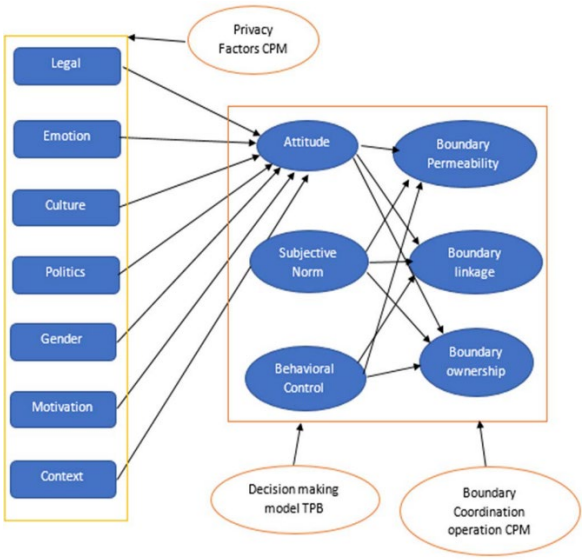


Figure 3-1: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017)

3.4 Research approach

Creswell and Creswell (2018) and Biggs et al. (2022) outline the research approach as consisting of qualitative, quantitative or mixed-method research. The authors distinguish between qualitative and quantitative research, which deals with intangible actions through words and evaluations through numbers (Creswell & Creswell, 2018). Creswell and Creswell (2018) and Biggs et al. (2022) add that the choice of research approach is a careful consideration that must be informed by the aim, objective and research questions of the study. Moreover, the epistemological, ontological and axiological assumptions influenced by the researcher's view of reality will have a clear influence on the crafting of the research approach and design (Creswell & Creswell, 2018)(Creswell & Creswell, 2018). Creswell and Creswell (2018) and Biggs et al. (2022) outline the array of research designs and their aptness to the relevant research approach in Table 3-3. These concepts will be discussed further hereunder.

Table 3-3: Alternative research designs (Creswell & Creswell, 2018)

Quantitative	Qualitative	Mixed Methods
• Experimental designs • Nonexperimental designs, such as surveys	• Narrative research • Phenomenology • Grounded theory • Ethnographies • Case study	• Convergent • Explanatory sequential • Exploratory sequential • Transformative, embedded, or multiphase

3.4.1 Qualitative research

Creswell and Creswell (2018) and Biggs et al. (2022) assert that the qualitative research approach is well suited for social research, where the researcher must delve into problems linked to the human condition. The research approach is a good fit for research problems where an evaluation of a condition or comprehension of intangible behaviour is needed. Data collection is facilitated using one or more data collection instruments that can record the results. The accumulated authentic results are analysed to create meaning using the specific inputs to develop generalised concepts that distinctly describe the problem (Creswell & Creswell, 2018). Creswell and Creswell (2018) and Biggs et al. (2022) present the research designs suited to qualitative research. These research designs will be discussed below.

Narrative research

According to Creswell and Creswell (2018) and Biggs et al. (2022), narrative research entails the researcher eliciting information from study participants in words. The solicitation of information can be facilitated through interviews where the researcher poses open-ended questions to obtain rich data for analysis. The researcher documents the research by rewriting the participants' accounts as a story whilst infusing the researcher's life experience (Creswell & Creswell, 2018).

Phenomenological research

Creswell and Creswell (2018:14) and Biggs et al. (2022) state that phenomenological research pertains to the collection of the participants' accounts of the research problem and results in an amalgamation of "philosophy and psychology" to document the issue.

Grounded theory research

Creswell and Creswell (2018) and Biggs et al. (2022) involve the formulation of theory using participants' views on the research problem. The authors suggest that the research would prove resource-intensive given the fact that multiple data gathering, iteration, and enhancement rounds are necessary (Creswell & Creswell, 2018).

Ethnographic research

Creswell and Creswell (2018) and Biggs et al. (2022) clarify that ethnographic research pertains to the monitoring of authentic actions and linguistics of a community. The authors add that the research would be carried out longitudinally by monitoring the participants in their community. Additionally, the research could necessitate the posing of questions to solicit authentic responses from participants, thereby allowing for rich and complex data (Creswell & Creswell, 2018).

Case study research

Creswell and Creswell (2018) and Biggs et al. (2022) propose that case study research allows the researcher to conduct a postmortem of the case to comprehensively understand the problem. The authors contend that the process could include multiple participants. Moreover, the postmortem is operated under strict conditions where the period and problem of interest are ringfenced to ensure consistency (Creswell & Creswell, 2018).

3.4.2 Quantitative research

Creswell and Creswell (2018) and Biggs et al. (2022) differentiate quantitative research from qualitative research. The authors explain that quantitative research is geared toward proving or disproving a hypothesis through the statistical analysis of numbers. This research approach is well-suited for a researcher with an affinity for statistical analysis. Management of bias in this approach is a notable concern that must be suitably addressed by the researcher (Creswell & Creswell, 2018). Creswell and Creswell (2018) present the research designs suited to quantitative research are discussed below.

Survey research

Creswell and Creswell (2018:13) and Biggs et al. (2022) describe survey research as a statistical analysis of "trends, attitudes, or opinions". The authors add that the study focusses

on a representative subset of the population that can be generalised. Whilst the items under interrogation are software intangible issues, the research employs a statistical format. The research can be facilitated using interviews or surveys over either a snapshot of time or an extended timeline (Creswell & Creswell, 2018).

Experimental research

Creswell and Creswell (2018) and Biggs et al. (2022) explain that experimental research utilises cause and effect. A pharmaceutical drug trial is an example of experimental research. The research tests the efficacy of a new blood pressure medication by using a test group and a control group. The test group receives the new medication, and the control group is provided a placebo. In this experimental research example, the outcome efficacy is evaluated using the inputs from the participants (Creswell & Creswell, 2018).

3.4.3 Mixed method research

Creswell and Creswell (2018) and Nind (2023) state that the mixed-method research approach consists of a combination of qualitative and quantitative research. The researcher must perform both research approaches independently in a single study. This approach is required where the researcher collects data relating to intangible behaviours like feelings or opinions to serve the one objective of the study and also collects numerical data to evaluate the formulated hypothesis for the other objective of the study. This approach is necessary, as the researcher cannot use either a mono-qualitative or mono-quantitative method to satisfy the study's needs prescribed by the aim, objectives, and research questions Creswell and Creswell (2018) present the research designs suited to qualitative research. These research designs are discussed below.

Convergent parallel mixed methods research

Creswell and Creswell (2018) state that convergent parallel mixed methods research allows for the simultaneous collection of qualitative and quantitative data via the respective data collection instruments. Moreover, the research approaches can converge for the interpretation of data to address any observed irregularities (Creswell & Creswell, 2018).

Explanatory sequential mixed methods research

Creswell and Creswell (2018) report that explanatory sequential mixed methods research allows for the consecutive collection of qualitative and quantitative data via the respective data

collection instruments. The researcher concludes and analyses the quantitative data in the first phase. The next phase of the qualitative research approach uses the learnings and enhancement derived from the first phase to drive improvement (Creswell & Creswell, 2018).

Exploratory sequential mixed methods research

According to Creswell and Creswell (2018), exploratory sequential mixed methods research is the inverse of explanatory sequential mixed methods research. This means that the qualitative and quantitative research approaches are switched around. Therefore, the first phase of qualitative research drives improvement in the subsequent quantitative research approach phase (Creswell & Creswell, 2018).

Transformative, embedded or multiphase research

Creswell and Creswell (2018) note that transformative, embedded or multiphase research allows for enhanced approaches to conduct the research. This allows for variants of the approaches, as mentioned earlier, to achieve successful research outcomes.

3.4.4 Selection of research approach

The researcher will conduct an inductive, mono-qualitative interpretivist study for a specific point in time. A mono-qualitative study is limited to the qualitative research approach.

Babbie (2016) and Braun et al. (2021) state that a qualitative study is best suited for the capturing of authentic perceptions, practices, experiences, behaviours, attitudes and general outlook. This qualitative study will allow the researcher to explore the social construct of the study to acquire a comprehensive understanding of the adult social media user and insight into the social media users' experience in the natural setting.

Babbie (2016) and Biggs et al. (2022) describe inductive theory as working from a narrow view of data collected from participants to reveal trends and deeper meaning. This could consist of several interviews to elicit information to understand the problem. It would be ideal if the interviews could pose open-ended questions to gather rich responses. This allows the researcher to analyse the data, develop themes and ultimately establish findings that can be generalised. Deductive theory is the inverse of inductive theory in that it reverses and engineers trends back to the actions or behaviours that determine them (Babbie, 2016). Saunders et al. (2019) complement this description by stating that the research using the

deductive approach focusses on testing the theory and attempting to understand the cause thereafter.

Babbie (2016:105) and Biggs et al. (2022) present the “time dimension” as consisting of either “cross-sectional” or “longitudinal” horizons. “Cross-sectional” studies focus on a specific plot on the timeline, whereas “longitudinal” studies span a longer section of time with periodic data collection (Babbie, 2016).

The qualitative research approach works well with the aim of determining the data privacy behaviour of adult users of social media. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

Quantitative and mixed-method approaches are not selected for this research. A quantitative study is numerically driven and well-suited to a researcher who has an affinity for statistical analysis. The researcher of this study is not well suited to statistical research. It would place demands on him with the added complexity and steep learning necessary for this approach. A mixed-method study is ideal for research where one approach, either qualitative or quantitative, would not satisfy the analysis. Moreover, this research approach would place a significant demand on the part-time researcher, whom he would not be able to meet.

Lastly, the researcher must understand the content of the respective social media platforms’ Terms of Service and Privacy Policy. The researcher will download copies of these documents and provide a synopsis thereof in section 2.6. The next section discusses the research method of the study.

3.5 Research method

The research methodology will entail a survey study. According to Blaxter et al. (2006) and Braun et al. (2021), the survey study is used to capture people's natural perceptions, practices, experiences, behaviours, attitudes, and general outlooks. Thus, this methodology is well suited to the study of adult social media users’ treatment or management of their data privacy. The study presents a level of complexity that the survey study can manage well and produce a source of data on which to base analysis. In contrast, the analysis of data may prove difficult. The survey study provides a holistic and rich set of data that may hamper analysis since the researcher may grapple with knowing what data to keep and discard. The empirical study will

utilise data observed directly from respondents via survey. The survey will be used to collect data relating to intangible aspects like feelings, thoughts and opinions (Braun et al., 2021).

The study aims to determine the data privacy behaviour of adult users of social media residing in South Africa whilst interacting on social media platforms. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms. The research choices are directly linked to the aim and objectives of the study.

The research design and data collection aspects are discussed in sections 3.6 and 3.7, respectively.

3.6 Research design

3.6.1 Population

White (2009) and Braun et al. (2021) emphasise the significance of the research population of interest as it contributes to the scope of the research study. Creswell and Creswell (2018) acknowledge that the population encompasses the complete group that the study sample is representative of. According to Statistics South Africa (2024), as of Census 2022, the country's population is estimated at 62,027,503 people. Statistics South Africa (2024) acknowledges that the South African population is comprised of numerous racial groups. Moreover, the languages used by the country's population are diverse at 24,4% speaking isiZulu, 16,3% speaking isiXhosa, 10,6% speaking Afrikaans, 10,0% speaking Sepedi, 8,7% speaking English, 8,3% speaking Setswana, 7,8% speaking Sesotho, 4,7% speaking Xitsonga, 2,8% speaking Siswati, 2,5% speaking Tshivenda, 2,1% speaking other languages, 1,7% speaking isiNdebele and less than 0,1% speaking Sign language (Statistics South Africa, 2024)(Statistics South Africa, 2024)(Statistics South Africa, 2024)(Statistics South Africa, 2024).

Kemp (2024) estimates the South African social media user population, as illustrated in Figure 3-2, to be around twenty-six (26) million users as of January 2024.

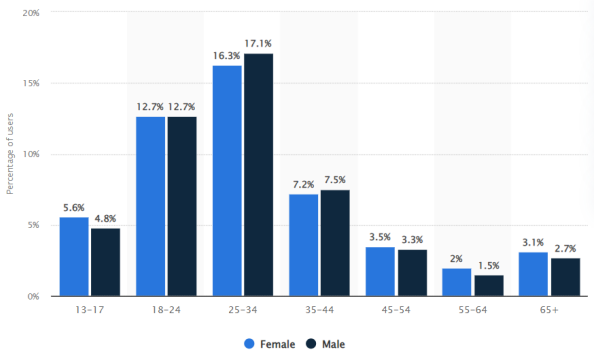


Figure 3-2: South African social media user age and gender distribution (Adapted from www.statista.com, 2021)

The study attempts to determine the data privacy management behaviour of social media users residing in South Africa. A child is legally defined as a person under 18 years of age, inferring that an adult is any person who is 18 years of age or older (South Africa, 2008). Children have been eliminated from the research population due to the necessity of ethical affordance.

3.6.2 Sampling

Creswell and Creswell (2018) and Biggs et al. (2022) report that the sample proportion is determined by the research approach. Babbie (2016) and Biggs et al. (2022) critique that a sample for a research study must be representative of the population or risk the generalisability capability of the study. Several sampling techniques are described below.

Convenience sampling

Babbie (2016) and Biggs et al. (2022) allude that convenience sampling resonates with the convenience aspect where the researcher may cross paths with someone and solicit their participation in the study.

Purposive sampling

Babbie (2016) and Biggs et al. (2022) comment that purposive sampling involves the researcher's determination as to who will participate in the study.

Snowball sampling

According to Babbie (2016) and Biggs et al. (2022), snowball sampling involves study participants being approached after their participation for a recommendation for new participants.

Quota sampling

Babbie (2016) describes quota sampling as a selection of participants meeting specific criteria for inclusion in the study to ensure an appropriate mix of participants.

Probability sampling

Babbie (2016) and Biggs et al. (2022) outline that probability sampling entails the selection of a sample that is representative of the population.

Randomisation

Babbie (2016:230) and Biggs et al. (2022) explain that randomisation pertains to experimental research where the participant may be randomly allotted to either the “experimental or control” group.

The researcher selected non-probability sampling, specifically convenience sampling. This sampling was used as the researcher could not foresee the compilation of the survey’s participants. The researcher intended using the survey data similar to interviews, where survey data would be used to generate the prevalent data privacy behaviour patterns. Potential participants were contacted via electronic mail, social media posts or direct social media messaging to solicit participation via an online survey platform. Kumar (2011) outlined heterogeneity and homogeneity in the sampling process, with the former necessitating a substantial number of respondents and the latter a low number of respondents, respectively, to deliver representative results.

The researcher aimed for either 150 participants or less than 100 participants and aimed to achieve data saturation. The ideal demographic for the study was comprised of close to an even split in gender, multiple South African mother-tongue speakers, diverse backgrounds and communities. However, the researcher did not have control over the representation of the sample.

3.6.3 Recruitment of study participants

Creswell and Creswell (2018) explain that the research participants must be strategically approached to participate.

The researcher will employ convenience sampling for the study. Marketing can be facilitated through electronic mail requests and direct social media messaging informing of the research study whilst conveying the value that a participant would provide through participation. Strategies to improve interest in completing the survey could involve the incentive of participants to increase their knowledge, illustrate the results, and promise to share the research findings.

Given the convenience sampling approach selected for the study, participants could be excluded from the study. The survey marketing will be facilitated using social media and electronic mail. This potentially would include persons without access to the internet. The survey is open to all device types that can be connected to the internet. This allows participants to complete the survey at their local library and various internet-enabled government centres. Additionally, a participant could access the free public wi-fi zones available in their respective South African cities.

In section 3.6.2, the researcher addresses the study's sampling decisions. Data collection will be outlined in the next section.

3.7 Data collection

3.7.1 Data collection instrument

Creswell and Creswell (2018) and Biggs et al. (2022) acknowledge that the data collection instruments for qualitative research are limited to “observation”, “interviews”, “documents”, and “audio visual and digital materials”. Moreover, surveys are identified as a quantitative research approach. Braun et al. (2021) argue that whilst underutilised, surveys are an apt data collection instrument for qualitative research. The authors contend that the survey can be utilised in the way that interviews request and generate the data. The design incorporates open-ended questions to solicit rich and complex responses (Braun et al., 2021).

The research methodology will entail a survey study. It must be noted that the researcher commenced with the data collection after a successful research proposal defence and ethics application approval. According to Blaxter et al. (2006), Creswell and Creswell (2018) and

Braun et al. (2021), the survey study is used to capture the natural perception, practices, experiences, behaviour, attitudes and general outlook of people. Thus, this methodology is well suited to the study of adult social media users' treatment or management of their data privacy. The study presents a level of complexity that the survey study can manage well and produce a source of data on which to base analysis.

In contrast, the analysis of data may prove difficult. The survey study provides a holistic and rich set of data that may hamper analysis since the researcher may grapple with knowing what data to keep and discard. The empirical study will utilise data observed directly from respondents via survey. The survey will be used to collect data relating to intangible aspects like feelings, thoughts and opinions (Braun et al., 2021).

3.7.2 Survey formulation

The researcher uses the research problem, aim, objectives, research questions and theoretical framework to inform the survey design. This must be formulated and proofread extensively to ensure a good quality product. Thereafter, approval must be sought from the researcher's supervisor to proceed with the captured survey.

The researcher considered the study's population and selected an adequate sample to ensure that the outcomes were representative, as outlined in sections 3.6.1 and 3.6.2. Creswell and Creswell (2018) and Biggs et al. (2022) are of the opinion that surveys aim to ease administration and negate the fieldwork requirement whilst allowing for the repeatability of results. The online productivity learnings from the coronavirus pandemic were excellent motivation for the researcher to conduct research via an online survey whilst realising the efficiency, timesaving, and cost-saving aspects of the study.

Babbie (2016), Creswell and Creswell (2018), and Biggs et al. (2022) propose the use of close-ended questions, open-ended questions and Likert scale questions to solicit feedback. The authors state that close-ended questions provide a list of fixed responses to the question where the participants must select at least one option. Additionally, open-ended questions provide a mechanism for the participants to provide candid and rich responses to the question. Lastly, the Likert scale provides a fixed list of options. For example, a participant is asked, "How do they perceive the traffic volume between 07:00 and 09:00 on a stretch of freeway". The fixed list of options could contain: 1. Light traffic, 2. Moderate traffic, and 3. Heavy traffic.

The researcher's survey design consists of three (3) sections, with Section One (1) providing an overview of the research, ethical details and benefits of the research, Section Two (2) consisting of demographic questions like gender, language, age and community, and Section Three (3) contains the questions to capture knowledge and behaviour of the respondent. These sections are discussed in more detail below, as well as Appendix A. Appendix A provides the approved survey design outline prior to uploading the survey questions to Google Forms.

Section 1 of the survey

Survey question 1 in Figure 4-5 requires the participant to select their age group. The age group selection is a determinant of whether the participant may proceed with the survey, as it is only open to adults. Participants under the age of 18 would be presented with the Google Forms survey exclusion page in Figure 4-6, which prevents them from participating. A participant equal to or over the age of 18 years old would be allowed to continue completing the survey.

Section 2 of the survey

In question 2 of the survey, the Individual Consent for Research Participation, Appendix A, is included to ensure that the participant provides consent to participate in the study. The selected age groups will be added to the demographic profile for participants. Moreover, survey questions 3 to 10 are used to capture the demography of the participants for the lens that will be used to interpret the raw data.

Section 3 of the survey

Survey questions 11 to 32 were linked to CPM and TPB aspects.

The study aims to determine the data privacy behaviour of adult users of social media through exploration of the user behaviours to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms. The survey questions touch on each aspect of the study's aim and the associated objectives.

3.7.3 Selection of appropriate data collection medium

Triga and Manavopoulos (2019) conclude that conventional manual surveys significantly increase the cost, time and effort to conduct the data collection exercise. The authors add that modern methods of survey using online tools allow the researcher to facilitate this remotely whilst limiting the necessary overheads. Moreover, modern methods foster richer responses, improved completion rates and enhanced response quality (Triga & Manavopoulos, 2019).

In lieu of the abovementioned outlook, Google Forms is selected as the online data collection medium for the survey. The questions are captured on the selected online survey platform. The researcher evaluated Microsoft Forms, Survey Monkey and Google Forms as potential online survey tools for the study. Microsoft Forms and Survey Monkey were eliminated as options due to the availability, cost, and privacy concerns posed by the researcher. Google Forms was selected due to the researcher's familiarity with the solution, its access, functionality, and ease of administration.

After uploading the questions, the researcher will conduct tests with several test participants to ensure that the questions are comprehensible to the test participants and that they perform as intended.

3.7.4 Process for data collection

Creswell and Creswell (2018) and Biggs et al. (2022) support the use of open-ended questions to draw the views of participants. The researcher must ensure compliance with the ethical prescripts of this study and will obtain consent before the online capturing of the surveys. The researcher must manage the data collected and ensure secure storage as a record of the data collection (Creswell & Creswell, 2018). Refer to section 1.5.4 on the storage of data for measures to restrict access and protect the data collected.

The researcher will initiate the survey data collection via Google Forms. Marketing of the survey will be facilitated via social media, where the researcher will post the survey participation request, description and link. Participants will be invited to partake in the study subject to their consent and meeting the minimum age requirement. The online survey will be provided a one (1) month period for participants to partake in the survey and will close thereafter. The data analysis section will be discussed hereunder.

3.8 Data analysis

3.8.1 Data preparation

The Google Forms data collection instrument manages the online submission of the surveys by participants. The exported Google Forms data will be imported into the ATLAS.ti software. ATLAS.ti uses an Extract, Transform and Load (ETL) logic. After the Google Forms' closure date, the researcher will extract the data in .csv file format and prepare the data for import by manipulating the headings. The researcher will extract the collected survey data from Google Forms and prepare it by manipulating the headings. An exclamation (!) must be added to the "Participant" column heading name and semi-colons (:) to the remaining headings. No additional work will be necessary for the transformation of the data.

3.8.2 Thematic Analysis

3.8.2.1 Description

The data analysis that will be employed in the study will consist of thematic analysis. The researcher will use the collected data to reveal any themes or patterns that can be interpreted. For example, the online survey platform will record the survey results and be displayed in a table format. The steps illustrated in Figure 3-3 were followed to analyse the data: (1) start preparations for data analysis, (2) consider all data, (3) codify all data, (4) create themes, and (5) devise a means to represent the themes.

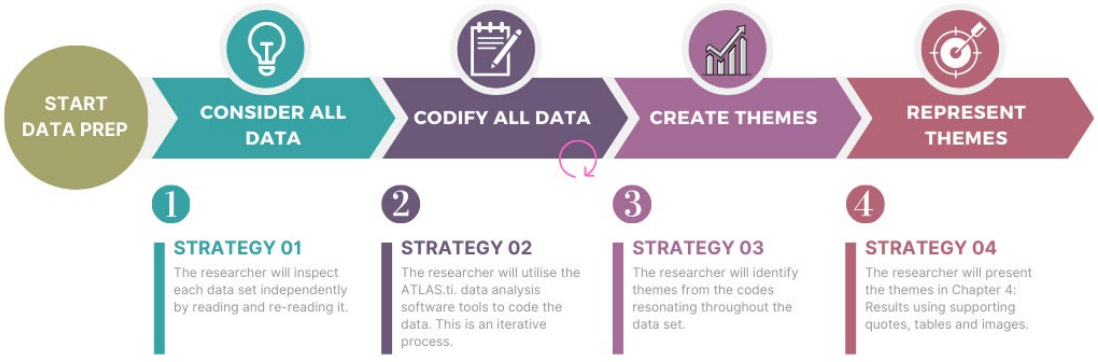


Figure 3-3: Thematic analysis process (Adapted from Saunders et al., 2023)

3.8.2.2 Purpose

Blaxter et al. (2006:206) and Biggs et al. (2022) propose that: “Analysis is about the search for explanation and understanding, in the course of which concepts and theories will likely be advanced, considered and developed.” This includes data analysis that perfectly relates to data collection in the research life cycle.

The researcher will attempt to differentiate this qualitative study from similar studies by considering influences like language, gender, age and community within the study’s context.

3.8.2.3 Process

The Google Forms data collection instrument manages the online submission of the surveys by participants. After the Google Forms’ closure date, the researcher will extract the data and consider options for data analysis. Analysis of the data can be processed through the manual table method or Computer-Assisted Qualitative Data Analysis (CAQDAS) tool.

Creswell and Creswell (2018) describe the table method as the manual process of arranging the data written on separate pieces of paper on a physical table and arranging the data to expose patterns. The pieces of data must be grouped and regrouped, moving the pieces of paper around on the table while attentively noting patterns to expose. Irrelevant data must be set aside (Creswell & Creswell, 2018).

According to Soratto et al. (2020) and Mastrobattista et al. (2024), CAQDAS tools like ATLAS.ti are invaluable tools, especially in the higher learning context. The authors describe ATLAS.ti as a qualitative CAQDAS tool that is available for ease of analysis. ATLAS.ti is lauded and regarded amongst the qualitative CAQDAS tools. The tool is attributed to allow the researcher to process large amounts of data to yield valuable analysis of the data (Mastrobattista et al., 2024). Although several CAQDAS tools are available, the researcher will utilise an ATLAS.ti license from the Cape Peninsula University of Technology (CPUT) to assist with the analysis. All the survey data will be thoroughly processed by the researcher to ensure that responses are aptly grouped and codified according to the emerging themes using the ATLAS.ti software. The researcher opted for the data analysis software tool to facilitate richer analysis than can be achieved through manual thematic analysis methods.

The exported Google Forms data will be imported into the ATLAS.ti software. No additional work will be necessary for the transformation of data. Each participant’s survey will be imported and receive a unique identifier to differentiate it. After the import of the data, the

researcher will orient himself on the layout of the data and commence reading it extensively. The overall steps illustrated in Figure 3-3 were followed to analyse the data: (1) start preparations for data analysis, (2) consider all data, (3) codify all data, (4) create themes, and (5) devise a means to represent the themes. It may be necessary for the researcher to closely inspect each data set by reading and re-reading it to identify codes that form from the content of the quotations. Code refinement may be necessary for subsequent re-reading passes where the researcher rationalises the codes for accuracy and efficiency. Mastrobattista et al. (2024) state that after the codes are identified, the researcher will identify categories and, ultimately, themes to be used in the analysis.

3.9 Validity and Reliability (or Trustworthiness)

Babbie (2016: 403) and Biggs et al. (2022) contend that evaluating the quality of qualitative studies is harder than quantitative studies. The author tenders “validity and reliability” as metrics to fulfil this evaluation. The metrics consider the trustworthiness, steadfastness and integrity of the data tendered in a qualitative study (Babbie, 2016). Babbie (2016) and Biggs et al. (2022) clarify that “validity” in a qualitative survey must be tested for comprehension to ensure that the reader of the survey interprets the survey questions as they were designed. Moreover, the ”reliability” of the qualitative survey tackles whether independent people interrogate the data and group it, that the groupings would be repeatable irrespective of who performed it.

The researcher will request their supervisor to peruse the survey for interpretability and quality. An additional round of testing will be conducted by a small pilot group to evaluate the validity. The researcher will facilitate reliability by researching widely and applying recommendations to mitigate it.

The researcher will use peer-debriefing to play back the process and outputs of their analysis. This will entail a session where the researcher will present their analysis, including theme formulation, for complete transparency. Their peers will be invited to provide honest criticism and constructive feedback. The critique and feedback will be used by the research team to refine, fix, and improve their analysis to ensure a good quality product.

Moreover, the researcher’s thesis will be intensively iteratively interrogated by their supervisor, and improvement will be facilitated using a feedback loop to further the goal of a good quality output.

Saunders et al. (2019:131) recommend that researchers take an opportunity to “hone the skill of reflexivity” to comprehend their philosophy. The authors contend that researchers must reflect and understand their worldview. Moreover, it is necessary to interrogate their thinking construct through introspection to determine what drives their thought and decision-making processes (Saunders et al., 2019:134). In lieu of the researcher’s entrenched axiological assumptions, the researcher will exercise deep introspection to account for their bias honestly and practically implement the bias mitigation strategies in the research.

Creswell and Creswell (2018) state that “member checking” can be used to verify the findings. The researcher can approach selected research participants to confirm that the findings are correctly reflected. This opportunity allows the researcher to validate the information at the source.

Biggs et al. (2022) contend that triangulation promotes validity and reliability in a study. It uses multiple views of information to cast an enhanced depiction of the results analytically. It mitigates the potential for bias that a single-method study is more predisposed to. Several semi-structured interviews can complement the surveys to support the findings. Data collected from multiple data collection methods can be overlaid to cast a more extensive view, thereby increasing opportunities for comprehension of the phenomenon and discovery of new meaning. The researcher can process each source of written information to validate the findings, thereby increasing the level of trust. The researcher will attempt to differentiate this qualitative study from similar studies by considering influences like language, gender and age within the study’s context.

Lastly, the researcher will present the information and findings exactly in an authentic state. Moreover, the researcher will not hide or manipulate the findings if they do not relay what they want presented.

3.10 Ethical considerations

Babbie (2016), Creswell and Creswell (2018), and Biggs et al. (2022) succinctly and powerfully state that researchers must protect the participants in their study. The section on ethical consideration explicitly states how the researcher will ensure that participants are safeguarded. Babbie (2016) and Biggs et al. (2022) state that provision must be made for the rights of the approached participants to refuse participation, allow for withdrawal and inform the participants of the details of the consent. Assurance must be provided that data is only

stored and retained in the location, on the medium and for the duration required for the research.

Creswell and Creswell (2018) and Biggs et al. (2022) stipulate that the data generated throughout the study must be protected. Access to the data will be strictly limited to the researcher and the Higher Degrees Committee (HDC) or University where required. The data will be protected by the researcher with either physical or electronic safeguards to prevent unauthorised access. The requirements of the Protection of Personal Information Act: Act 4 of 2013 will be applied, and the personal information in the research will be safeguarded.

The researcher must ensure that the University is protected. Furthermore, research conducted in an open-source environment remains the property of the University. The researcher must adhere to the University's licensing mechanism when intending to publish the research. All research from documents must be credited for their contribution by referencing the research in the body of the text and the reference or bibliography section.

Creswell and Creswell (2018) propose that there are various phases during the lifespan of the study that the researcher needs to consider ethics. These phases are discussed further below.

3.10.1 Phase 1: Ethics before the study

Biggs et al. (2022) discuss that the researcher must read the University's Plagiarism Policy, Ethics Policy and Code of Conduct, understand their ethical responsibilities and rigidly conform by applying it to their work. Moreover, the researcher must remain apprised of any amendments to these documents.

According to Creswell and Creswell (2018) and Biggs et al. (2022), the researcher must obtain ethics approval before commencing the data collection phase of the study. After the successful Research Proposal Defence and approval thereof, the researcher must apply for ethics approval using the prescribed application form. The researcher facilitates this process by comprehensively completing the form and discussing it with their supervisor. Upon agreement, the researcher's supervisor submits the form for review and consideration for approval. The researcher has received an ethics certificate to conduct the research. A copy is included in Appendix C.

Creswell and Creswell (2018) and Nind (2023) recommend the formulation of a consent form for the study's participants to complete. A survey form and consent form were designed by the

researcher in consultation with their supervisor. The purpose of the study is outlined therein. These documents are included in Appendixes A and B.

Creswell and Creswell (2018) and Biggs et al. (2022) are of the opinion that the requirements of the at-risk part of the population must be considered and safeguarded. The researcher intentionally designed the research to exclude children who were determined to be persons under the age of 18 years old. The researcher's motives for this are linked to the associated affordances necessary for including children to be included in a study and the associated complexity. As the researcher is a part-time student, the additional complexity deterred any ideas of inclusion.

3.10.2 Phase 2: Ethics at the outset of the study

Babbie (2016), Creswell and Creswell (2018) and Nind (2023) recommend the formulation of a consent form for the study's participants to complete. A consent form was designed by the researcher in consultation with their supervisor. The purpose of the study is outlined therein. This document is included as Appendix B. Each participant is required to consent to the research.

Biggs et al. (2022) recommend that the study should not collect harmful information. The researcher consulted extensively with their supervisor to ensure that no harmful information would be collected.

3.10.3 Phase 3: Ethics during the data gathering phase

Kumar (2011), Babbie (2016), Creswell and Creswell (2018), and Nind (2023) acknowledge the importance of obtaining informed consent before gathering data for research. The components of the data gathering must be explicitly stated to the potential participants so that they may decide whether to participate. The researcher will explain the purpose of the study and explicitly state that participants must provide written consent for the researcher to proceed. For example, the researcher must conduct this research in a responsible manner that will ensure that the participants are afforded anonymity and confidentiality.

3.10.4 Phase 4: Ethics during the analysis phase

Creswell and Creswell (2018) and Nind (2023) advise that the researcher must safeguard the information provided by the participants and must anonymise the participants when referencing them in the study. The researcher will code the participants to preserve anonymity.

Additionally, the researcher must severely limit access to the data through encryption and password control.

Creswell and Creswell (2018) and Nind (2023) are of the opinion that all results must be included in the analysis and that the researcher must not attempt to obfuscate the results or mislead the reader.

3.10.5 Phase 5: Ethics during the concluding phase

Creswell and Creswell (2018) caution the researcher about the obfuscation of results and plagiarism. The researcher is aware of the University's Plagiarism Policy, Ethics Policy and Code of Conduct. He has and continues to ensure that he does not contravene any of these prescripts.

Creswell and Creswell (2018) and Biggs et al. (2022) state that the researcher must ensure that participants are protected. The researcher will ensure that the participants are protected through anonymisation, protecting the data gathered and ensuring that results are accurately reported. The limitations and delimitations are discussed below.

3.11 Limitations and Delimitations

The study employs a qualitative study using surveys to examine the data privacy behaviour of adult social media users. Biggs et al. (2022) ascribes that quantitative research leans more toward a numerical disposition, whereas qualitative research delves into a description through words. Babbie (2016) and Braun et al. (2021) state that a qualitative study is best suited for the capturing of authentic perceptions, practices, experiences, behaviours, attitudes and general outlook. This qualitative study will allow the researcher to delve into the social construct of the study to acquire a comprehensive understanding of the adult social media user and insight into the social media users' experience in the natural setting.

Children are excluded from the study in lieu of the ethical affordances necessary for inclusion. Moreover, the study will be conducted within the confines of South Africa. The study is further delineated to the confines of South Africa as the researcher resides in the Western Cape in South Africa. This would be manageable due to the size, complexity, and time constraints of the study. The study's limitation to South Africa is to understand the influence of diverse cultures and communities on data privacy management.

In Appendix C, the researcher has been granted ethical clearance between 22 September 2022 – 30 June 2025. Therefore, the research must be concluded by 30 June 2025.

The study explores the data privacy management behaviour of social media users residing in South Africa. It is limited to the confines of South Africa. However, this study does not consider the technical data privacy aspects.

3.11.1.1 In-scope

The study is limited to the following parameters:

- Data privacy behaviour of adult social media users.
- The research population will be limited to adult social media users 18 years of age and older residing in South Africa.
- The study will be conducted within the confines of South Africa.
- Combined CPM and TPB theories will be employed.
- Influence of participants' age, language, education and community.

3.11.1.2 Out-of-scope

The study is limited to the parameters outlined in section 1.6.1. The study excludes the following:

- Social media users under 18 years of age.
- Legislation and policy instruments for managing data privacy.
- Information security.
- Cyber security.
- Encryption and decryption.
- Technical data privacy aspects.

3.12 Data Management

The researcher must ensure that he complies with the prescripts of the Cape University of Technology (CPUT) Data Management Plan (DMP). An outline of the responsibilities of the researcher and aspects of the DMP are provided below.

An Ethics Application was submitted to the CPUT to ensure that all ethical aspects are suitably addressed and prevent any harm to participants as described in section 3.10. No research will

be conducted prior to a positive ethics application outcome. The consent is included in the data collection instrument and must be consented to before being able to submit any data. Participants will be allowed to participate but similarly will be afforded the opportunity to withdraw at any moment. The participants' data will be safeguarded and not be accessible by any unauthorised persons. Their data will be limited to the intended purpose and will be destroyed responsibly when no longer needed. The purpose, process and outputs of the research will be explained to the research participants. Identities and personal information of the research participants will be safeguarded against unauthorised access and will be aggregated for the findings, thereby ensuring all participants remain anonymous.

Should a participant decide to withdraw from the study, the researcher will acknowledge receipt of the correspondence. The researcher will proceed to note the request or instruction to withdraw. All data entries relevant to the participant in question on all media will be deleted responsibly. Upon completion, the researcher will thank the participant for their time and notify the participant that all their data was deleted and will not be used in the study.

Any research participant will not be allowed to partake in the study unless their consent has been obtained. Participation will remain optional, and no person will be forced to participate. Limited personal information will be collected but will be safeguarded against unauthorised access. The supply of personal information will remain optional. The researcher will explain to participants how their personal information will be used and safeguarded. No participants under the age of 18 will be allowed to partake in the research.

The data collection will be limited to primary data collected using surveys. Participants will be recruited through social media platforms like LinkedIn or Facebook. Surveys will be distributed and administered using the Google Forms online platform. This platform will be used for convenience, efficiency, time management, and cost savings. Only the researcher and their supervisor will have access to the online data collection platform. The data will be downloaded to the researcher's personal computer, which is password-protected and encrypted. It will further be backed up to an encrypted external hard drive stored in a secured lockable cabinet. It will also be backed up to the researcher's encrypted and password-secure cloud storage. Access to the data will strictly be limited to the researcher and will not be shared with any unauthorised persons. The data will be preserved until the research has been approved/passed and the researcher has graduated. Some biographical and demographic data will be captured in the study. The primary and sole researcher will remain responsible for managing the data. The data will be extracted from this platform in Microsoft Excel and .pdf

formats. There is no existing data that can be re-used for the research, and therefore, collection is necessary. Upon conclusion of the research, the data will be saved in .csv and .pdf formats to extend the longevity of access to the data.

The potential for harm to participants or others is extremely low in this research. This research is limited to collecting the views, ideas, preferences and opinions of the research participants. The researcher will ensure that no copyright and Intellectual Property Rights (IPR) are infringed upon by eliminating the need to use them. Suppose there is a need to use the copyrighting and Intellectual Property Rights (IPR) information. In that case, it will only be done with the permission of the owner and with the appropriate citation acknowledgement.

The researcher will need some funding to conduct the research and will personally be funded. Additionally, the researcher will need time and his own equipment to conduct the research. The ATLAS.ti will be used under the CPUT's license to analyse the data.

The researcher aims to reveal deeper meaning using the theoretical lens for the Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB) theories. The researcher will further attempt to differentiate this qualitative study from similar studies by considering influences like culture, language, gender and age within the context of the research study. Therefore, the data mentioned earlier is necessary to analyse this. Whilst some of the data may be sensitive, the researcher will employ methods to anonymise the data through the use of groupings when the participants provide their submissions.

3.13 Conclusion

3.13.1 Research objectives

The study aims to determine the data privacy behaviour of adult social media users residing in South Africa. The objectives of the research are: 1. To explore the privacy management methods and techniques employed by adult social media users; 2. To determine the data privacy threat perception of adult social media users, and 3. To identify behavioural barriers to data privacy management implementation of adult social media users. The researcher intends to explore the reasons for the observed behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

3.13.2 Theoretical framework

Al-Rabeeah and Saeed (2017) assert that privacy can be affected when a person experiences a data privacy breach and requires intervention. The researcher employed the Al-Rabeeah and Saeed (2017) combined theory model illustrated in Figure 3-1 as the theoretical lens for the study to reveal a deeper meaning. The researcher used this combined theory to explore the reasons for the observed social media user behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms. The researcher differentiated this qualitative study from similar studies by considering the under-mentioned components within the study's context.

3.13.3 Research approach

The study is a mono-qualitative interpretivist study. Creswell and Creswell (2018) and Biggs et al. (2022) outline the research approach as consisting of qualitative, quantitative or mixed-method research. The authors distinguish between qualitative and quantitative research, which deals with intangible actions through words and qualitative evaluations(Creswell & Creswell, 2018).

The researcher has carefully considered the study. It has been shaped by the aim, objectives and research questions described in section 3.13.1. The study will consist of a mono-qualitative interpretivist study that explores the phenomenon of data privacy management behaviour of adult social media users in South Africa.

3.13.4 Research method, design and data collection

The aim of the study is to determine the data privacy behaviour of adult social media users residing in South Africa. The aim, objectives and research questions outlined in section 3.2 are directly linked to the research method, research approach and research design.

The research methodology will entail a survey study. This methodology is well suited to the study of adult social media users' management of their data privacy as it can capture people's natural perceptions, practices, experiences, behaviours, attitudes, and general outlooks. The study presents a level of complexity that the survey study can manage well and produce a source of data on which to base the analysis. Survey study provides a holistic and rich set of

data that is beneficial to the researcher. The empirical study will utilise data observed directly from respondents via the survey.

Kemp (2024) estimates the South African social media user population, to be around twenty-six (26) million users as of January 2024. The researcher has selected non-probability sampling, specifically convenience sampling. This sampling was selected because the researcher could not foresee the compilation of the survey's participants. The researcher intends to use the survey data in a manner similar to interviews, where the survey data will be used to qualitatively generate the prevalent data privacy behaviour patterns. Potential participants will be invited via social media to participate in the study. The researcher aims to reach around 100 participants and achieve data saturation. The ideal demographic for the study is comprised of a close to even split in gender, multiple South African mother-tongue speakers, diverse spread backgrounds and well-represented communities.

Creswell and Creswell (2018) acknowledge that the data collection instruments for qualitative research design are limited to "observation", "interviews", "documents", and "audio-visual and digital materials". The authors explain that surveys are best suited for a quantitative research approach. Braun et al. (2021) argue that whilst underutilised, surveys are appropriate data collection instruments for qualitative research.

A survey will be used to collect data relating to intangible aspects like feelings, thoughts and opinions. The researcher's survey design consists of three (3) sections, with Section One (1) providing an overview of the research, ethical details and benefits of the research, Section Two (2) consisting of demographic questions like gender, language, age and community, and Section Three (3) contains the questions to capture knowledge and behaviour of the respondent. These sections are discussed in more detail below, as well as Appendix A. Appendix A provides the approved survey design outline before uploading the survey questions to an online data collection platform.

Google Forms is selected as the online data collection medium for the survey. The researcher evaluated Microsoft Forms, Survey Monkey and Google Forms as potential online survey tools for the study. Google Forms was selected due to the researcher's familiarity with the solution, its access, functionality, and ease of administration. Prior to the official release of the survey, a pilot of the Google Forms survey will be conducted to ensure that the questions are understandable to the test participants and that they perform as intended.

The researcher must ensure compliance with the ethical prescripts of this study and will obtain consent before the online capturing of the surveys. The researcher must manage the data collected and ensure secure storage as a record of the data collection.

3.13.5 Data analysis

The Google Forms data collection instrument manages the online submission of the surveys by participants. After the Google Forms' closure date, the researcher will extract the data in .csv file format and import it into the ATLAS.ti software.

Thematic analysis will be utilised to reveal any trends or patterns that can be interpreted. The steps illustrated in Figure 3-3 were followed to analyse the data: (1) start preparations for data analysis, (2) consider all data, (3) codify all data, (4) create themes, and (5) devise a means to represent the themes. The researcher will attempt to differentiate this qualitative study from similar studies by considering influences like language, gender, age and community within the study's context.

Numerous CAQDAS tools like ATLAS.ti and NVIVO are available to facilitate richer analysis than can be achieved through manual methods. The researcher will utilise an ATLAS.ti license from the CPUT to support the analysis. All the survey data will be thoroughly processed by the researcher to ensure adequate coding of the quotations. Additional reading and re-reading will be required to identify codes that form from the content of the quotations for enhanced accuracy and efficiency. After the codes are identified, the researcher will identify categories and, ultimately, themes to be used in the analysis.

3.13.6 Validity and reliability

It is essential to ensure the trustworthiness, steadfastness and integrity of the data tendered in a qualitative study. The survey must be tested for rigour to ensure that it delivers reproducible results. The researcher will also request their supervisor to peruse the survey for interpretability and quality. An additional round of testing will be conducted by a small pilot group to evaluate the validity.

3.13.7 Ethical considerations

The researcher must ensure that the study receives the necessary attention in respect of ethics. An ethics application must be processed and approved before commencing data collection, analysis and interpretation of the study. Above all else, the researcher must ensure

that participants are afforded sufficient protection. Moreover, there are ethics requirements in Phase 1: Ethics before the study, Phase 2: Ethics at the outset of the study, Phase 3: Ethics during the data gathering phase, Phase 4: Ethics during the analysis phase and Phase 5: Ethics during the concluding phase.

The results of the study are presented in Chapter 4.

CHAPTER 4: RESULTS

4.1 Introduction

The chapter is organised into eight (8) sections. Section One (1) provides the introduction, where the researcher outlines the results of the analysis. The next section, Section Two (2), casts the background to the study and the data analysis process applied. Sections Three (3) and Four (4) provide a synopsis of the research objectives and the data collection process, respectively. Section Five (5) explains the application of the selected theories, and Section Six (6) spans the description of the analysis. The findings are presented in Section Seven (7), and Section Eight (8) delivers the conclusion for this chapter.

The study's title, aim, objectives, research question and sub-research questions are illustrated in Figure 4-1 below for easy reference.

Figure 4-1: Problem statement (Adapted from research proposal, 2022)

The analysis utilises thematic analysis, and several themes are revealed from the associated codes. Table 4-1 provides an alternate view of the Aim, Research Question, Sub-Research Question and the linked themes presented in the analysis. Three (3) themes are observed, namely: Theme 1: Data privacy management, Theme 2: Social media utilisation and threat perception and Theme 3: Behaviour.

Table 4-1: Research questions and theme linkages

Nature	Research Questions	Research Objectives	Theme
Aim	The aim of the study is to determine the **data privacy behaviour** of adult **users of social media** residing in South Africa whilst interacting on the social media platforms.		
Main **RQ**	What is the **data privacy** management **behaviour** of adult **social media users**?		
Sub RQ1	How do adult **social media users** manage their **privacy** when interacting on a **social media** platform?	To explore the **privacy** management methods and techniques employed by adult **users of social media** residing in South Africa to manage their privacy when interacting on a **social media** platform.	**Theme 1:** Data privacy management
Sub RQ2	What is the perceived **privacy** threat awareness level of adult **social media users**?	To determine the data **privacy** threat perception of adult **social media users** residing in South Africa.	**Theme 2:** Social media utilisation and threat perception
Sub RQ3	What are the **behavioural barriers** to **privacy** management implementation for adult **social media users**?	To identify **behavioural barriers** to data **privacy** management implementation of adult **social media users** residing in South Africa.	**Theme 3:** Behaviour

The mono-qualitative study utilises surveys administered electronically via Google Forms to collect the raw data and garnered a total of 95 responses. This is broken into two collection phases of 73 respondents and 22 respondents, respectively.

Theme 1: Data privacy management

Theme 1 involves the data privacy management of social media users when interacting on the respective social media platforms. In the numerous categories in the list below, identify the raw data that leads to the formulation of the theme, as mentioned earlier. The theme attempts to determine the data privacy management approach and outlook of the users through data

sharing, as well as the perceived importance of privacy, trust, risk, and data protection. This section provides an overview of theme 1 and will be discussed further in section 4.6.4.4.

Categories

- Can it be used by others
- Permission to use data for incentive
- Privacy importance
- Trust
- Risk
- Data protection
- Upload

Theme 2: Social media utilisation and threat perception

Theme 2 involves the social media utilisation and threat perception of users when interacting on the respective social media platforms. Numerous categories in the list below are identified in the raw data that lead to the formulation of the theme, as mentioned earlier. The theme attempts to determine how users use and perceive ownership of content, pre- and post-registration reasons and whether users understand the Terms of Service of the respective social media platforms. This section provides an overview of theme 2, which will be discussed further in section 4.6.4.4.

Categories

- Ownership
- Registration reason
- Usage purpose
- Terms of service
- Usage

Theme 3: Behaviour

Theme 3 relates to the behaviour of users when interacting on the respective social media platforms. Numerous categories in the list below, identified in the raw data, lead to the formulation of the theme, as mentioned earlier. The theme attempts to determine users'

attitudes and behaviour to the respective social media platforms. This section provides an overview of theme 3, which will be discussed further in section 4.6.4.4.

Categories

- Breach awareness
- Breach attitude
- Breach behaviour
- Personal experience

The user demography is also presented to demonstrate what is included in the raw data. The components of the user demography, namely Age group, Gender, Language, Community and Education, will be used as the lens through which to view the data. These components form part of the CPM and TPB theories selected by the researcher.

Results are reflective of the subjective opinions of the participants. Furthermore, as the survey spans 32 questions, it is not feasible for the researcher to present findings for all the survey questions in the analysis section. Survey questions consist of numerous demographic questions, five (5) multi-select list questions, fourteen (14) Likert scale questions and three (3) open-ended questions. Hence, the most notable and interesting questions will be presented in the analysis, and the remaining results will be provided in the appendix.

The selection of the survey questions was based on the assessment against the researcher's prioritisation criteria. This entailed: 1. Question type and 2. Usefulness in answering the research question. The researcher favoured the open-ended questions for criterion 1 as they are rich and multi-dimensional responses capable of revealing more than one (1) result. Criterion 2 was used for the remaining questions as the researcher selected questions that were most useful in answering the research questions. The applicability of the survey question was assessed against the research questions and research objectives.

The findings of the study will be presented in this chapter, which is devoid of interpretation. The interpretation will follow in Chapter Five: Discussion. There will be a focus on the raw data and the themes emanating from the data analysis coupled with the research objectives.

4.2 Background of study

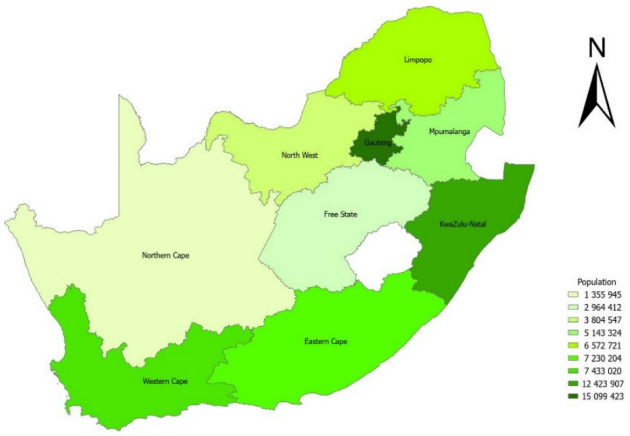


Figure 4-2: South African population proportions per province (South Africa, 2022)

The study attempts to determine the data privacy management behaviour of social media users residing in South Africa. According to Statistics South Africa (2024), as of Census 2022, the country has a population of 62,027,503 people. The proportions of the South African population are shown in Figure 4-2 above (Statistics South Africa, 2024)(Statistics South Africa, 2024).

Statistics South Africa (2024) acknowledges that the South African population is comprised of numerous racial groups. Moreover, the languages used are diverse, as illustrated in Figure 4-3 (Statistics South Africa, 2024).

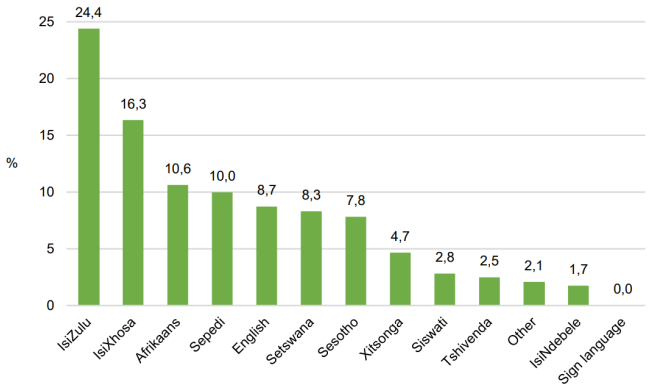


Figure 4-3: Proportions of languages (South Africa, 2022)

Kemp (2021); Kemp (2024) estimates the South African social media user population at around twenty-five (25) million users and twenty-six (26) million users as of January 2021 and January 2024, respectively. Significant growth in the South African social media user base has transpired, equating to an increase of one (1) million users. The January 2021 and January 2024 proportion of social media users account for 41,9% of the total population in the country for both reference years. This fact infers that the social media user base in South Africa has experienced growth commensurate with population growth (Kemp, 2021; Kemp, 2024). Statista (2021) reports that there has been widespread uptake of social media by the South African population. The various age groups and genders of South African social media users are depicted in Figure 4-4 (Statista, 2021). Figure 4-4 demonstrates that the 18 – 24 and 25 – 34-year-old age groups account for the largest proportion of the South African social media population.

Beigi and Liu (2020) are of the opinion that the abundance and scale of private data available on social media primes the platforms for exploitation by bad actors. This sets the stage for opportunities for identity fraud, hacking to use or sell personal information and cyberbullying Beigi & Liu, 2020).

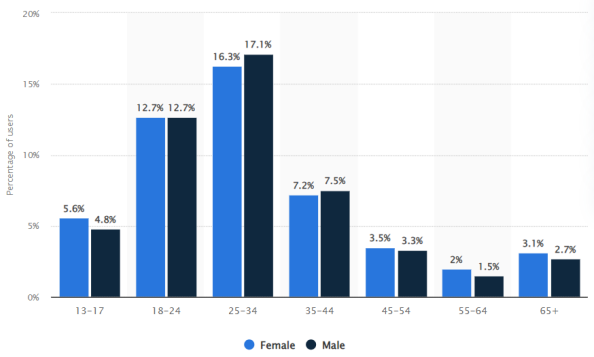


Figure 4-4: South African social media user age and gender distribution
(Adapted from www.statista.com, 2021)

4.3 Research objectives

The study is exploratory in nature, where the researcher explores through survey questionnaires how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy.

The research aim and objectives are provided as a reminder and to orientate the analysis of the study. It is crucial to focus on the analysis to ensure that the findings are revealed to further the understanding of the research problem.

In this chapter, the researcher intends to use the findings to reveal any themes or patterns that could be interpreted.

4.3.1 Aim

The study aims to determine the data privacy behaviour of adult users of social media residing in South Africa whilst interacting on social media platforms. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

4.3.2 Objectives

1. To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.
2. To determine the data privacy threat perception of adult social media users residing in South Africa.
3. To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

4.4 Data collection

4.4.1 Surveys for data collection

The researcher selected a mono-qualitative study to determine the data privacy management behaviour of adult social media users in South Africa. The researcher utilised Google Forms to administer the survey and garner responses that would answer the following research

questions. Appendix A provides a view of the survey design, and Figure 4-5 depicts the Google Forms opening page.

RQ: What is the data privacy management behaviour of adult social media users?

> **SRQ1:** How do adult social media users manage their privacy when interacting on a social media platform?
>
> **SRQ2:** What is the perceived privacy threat awareness level of adult social media users?
>
> **SRQ3:** What are the behavioural barriers to privacy management implementation for adult social media users?

The researcher has done everything in his power to protect the confidentiality of the data collected and uphold the ethical requirements' prescripts of the Cape Peninsula University of Technology (CPUT).

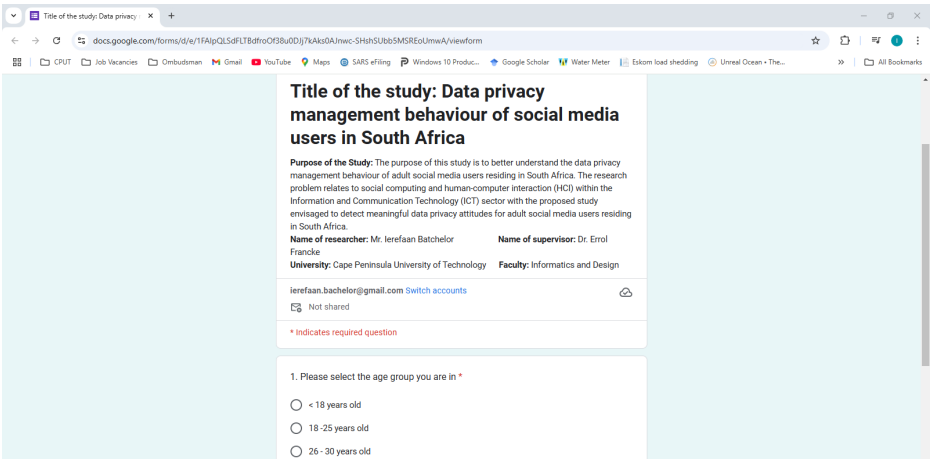


Figure 4-5: Google Forms survey (Google Forms, 2024)

Survey question 1 in Figure 4-5 requires the participant to select their age group. The age group selection is a determinant of whether the participant may proceed with the survey, as it is only open to adults. Participants under the age of 18 would be presented with the Google Forms survey exclusion page in Figure 4-6, which prevents them from participating.

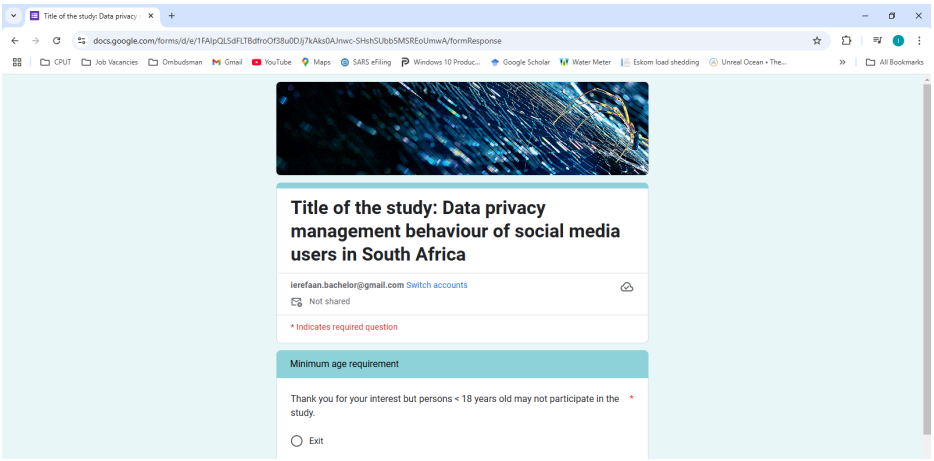


Figure 4-6: Google Forms survey minimum age exclusion handler (Google Forms, 2024)

In question 2 of the survey, the Individual Consent for Research Participation, Appendix B, is included to ensure that the participant provides consent to participate in the study. The selected age groups will be added to the demographic profile for participants. Moreover, survey questions 3 to 10 are used to capture the demography of the participants for the lens that will be used to interpret the raw data.

Survey questions 11 to 17 focus on answering Sub-research Question 1, whereas survey questions 18 to 28 seek to address Sub-research Question 2. The final survey questions 29 to 32 delve into Sub-research Question 3.

4.4.2 Composition of survey participants

The under-mentioned figures and Table 4-2 provide the various aspects of demography like Age Group, Gender, Education, Language, Employment and Community. The demographic data was collected to shape the lens through which the data privacy management behaviour is viewed. Additionally, the Participant Code is provided in Table 4-2 below for application in section 4.7 to link the quotations that are inserted.

Survey Question 1: Please select the age group you are in

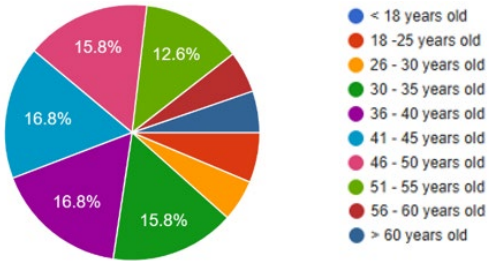


Figure 4-7: Age groups of participants (Google Forms, 2024)

Despite a small number of study participants, all age groups are represented in Figure 4-7. The age groups 31-35, 36-40, 41-45, 46-50 and 51-55 are the highest counts of participants at 15, 16, 16, 15 and 12, respectively. The minimum age for participation was 18 years of age. No participants under the age of 18 participated in the study.

Survey Question 3: Select your gender

The gender count shown in Figure 4-8 is very evenly split at 46 females versus 48 males. Participants were allowed to opt out by selecting the “Prefer not to say” option. One participant made a selection.

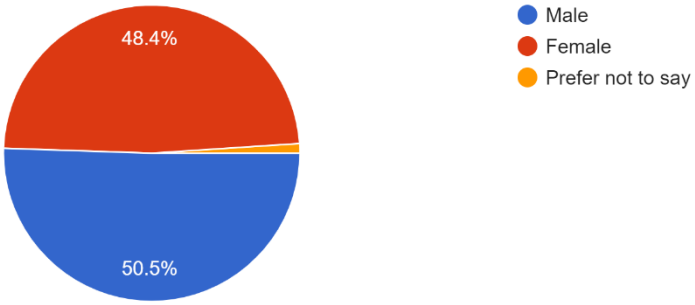


Figure 4-8: Gender of participants (Google Forms, 2024)

Survey Question 4: Select your highest level of education

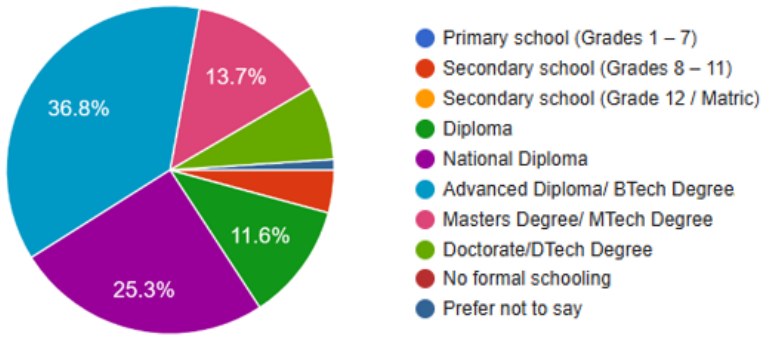


Figure 4-9: Highest level of education of participants (Google Forms, 2024)

Most participants selected the National Diploma, Advanced Diploma/BTech Degree and Master's Degree at 24, 35 and 13, respectively, in Figure 4-9. Four out of the 95 participants are not employed or full-time students. Notably, seven participants with Doctorate/DTech Degrees are included. Participants were allowed to opt out by selecting the "Prefer not to say" option, and one participant made a selection.

Survey Question 5: Which of the following best describes your current employment status?

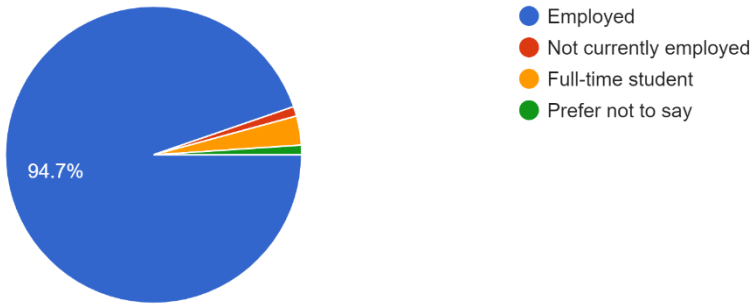


Figure 4-10: Employment status of participants (Google Forms, 2024)

The majority of the participants selected the employed as depicted in Figure 4-10. Four out of the 95 participants are either not employed or full-time students. Participants were allowed to opt out by selecting the "Prefer not to say" option.

Survey Question 6: Which city do you live in?

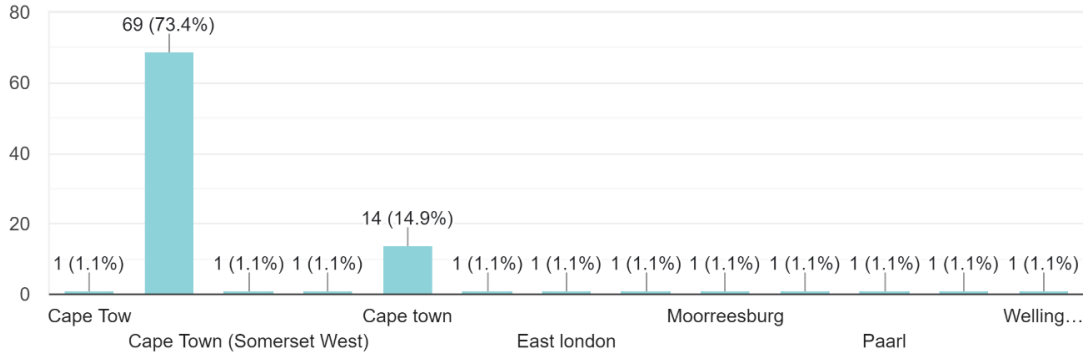


Figure 4-11: Residence city of participants (Google Forms, 2024)

Figure 4-11 demonstrates that most of the participants reside in Cape Town. This manifests in various typographical variants of Cape Town. Additionally, a few participants captured suburbs like Paarl and Wellington. These suburbs are located in Cape Town and are bundled into the Cape Town count. Two participants are from East London, one from Moorreesburg and one from Sasolburg. The survey results include one international participant who captured Nizwa, Oman, as their city of residence. Lastly, one participant elected to not submit a response.

Survey Question 7: What languages do you read and speak? Select all that apply.

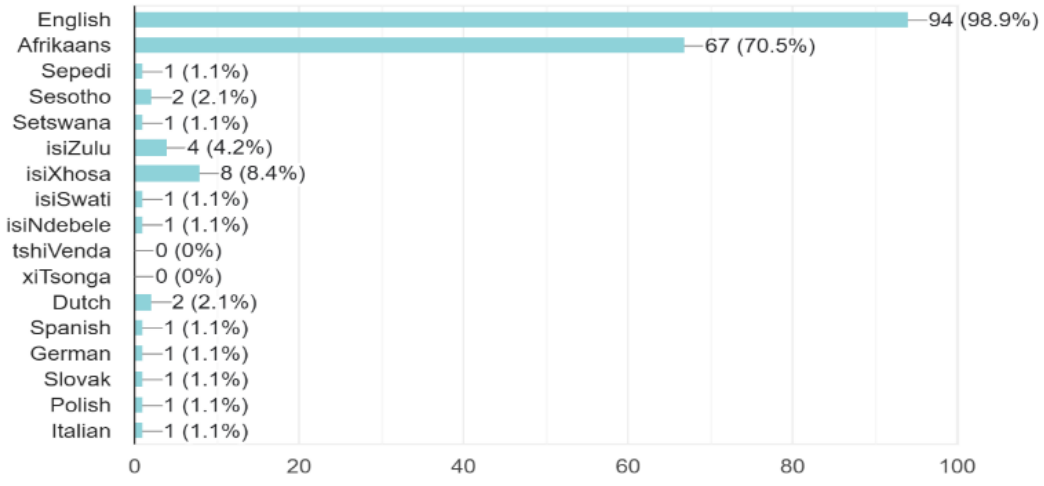


Figure 4-12: Languages spoken and read by participants (Google Forms, 2024)

English and Afrikaans are mostly spoken in the study sample at 94 and 67, respectively, in Figure 4-12. The third most spoken language is isiXhosa. Non-South African languages that the participants speak include Dutch, Spanish, German, Slovak, Polish and Italian, albeit with one participant each.

Survey Question 8: What is your mother-tongue/first language?

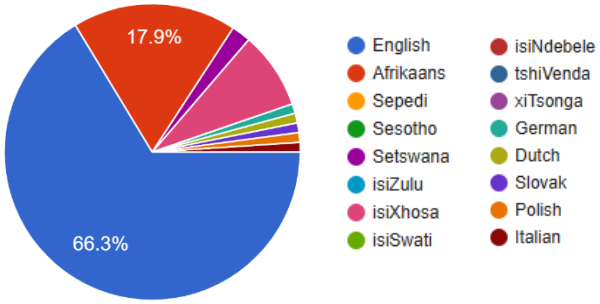


Figure 4-13: Mother-tongue of participants (Google Forms, 2024)

Figure 4-13 depicts that English mother-tongue speakers constitute the majority of the participants at 63. Afrikaans and isiXhosa place second and third, respectively. The remaining mother-tongue languages are spoken in low volumes.

Survey Question 9: Which Province did you spend most of your childhood in?

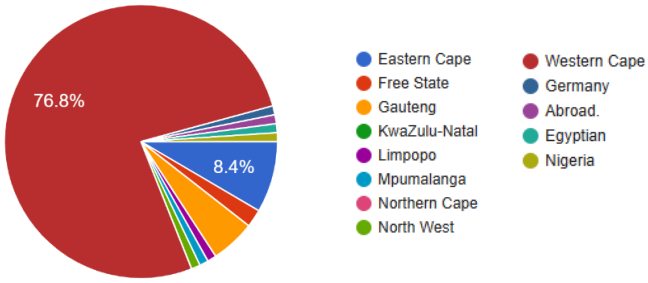


Figure 4-14: Province where participants spent most of their childhood (Google Forms, 2024)

Most participants spent most of their childhood in the Western Cape, as illustrated in Figure 4-14. The second and third largest groups harked from the Eastern Cape and Gauteng. The remaining participants spent most of their childhood in the Free State, KwaZulu Natal, Limpopo, Mpumalanga, Northern Cape, North West, Germany, Egypt and Nigeria. One participant only captured “abroad” in their response.

Survey Question 10: Which town or city did you spend most of your childhood?

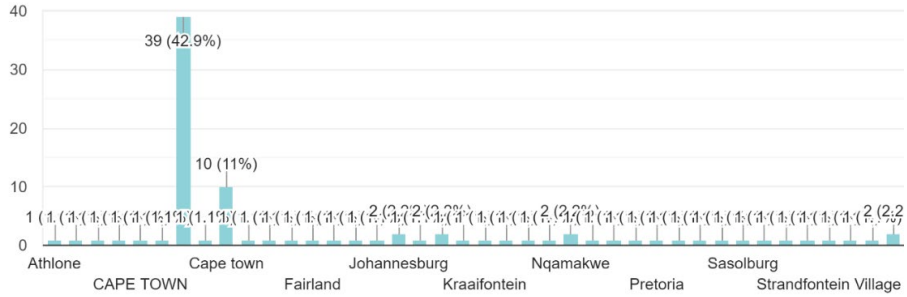


Figure 4-15: City where participants spent most of their childhood (Google Forms, 2024)

The majority of the participants spent most of their childhood in Cape Town. These participants captured Cape Town in numerous forms, as is evident in Figure 4-15. Additionally, several participants captured suburbs instead of the city. These are corrected to Cape Town. Lastly, four participants elected to not submit a response.

In summary, the sample in this study is representative of the population’s demographics. However, the sample is so small that no generalisations will be made in the findings. The findings will merely reveal the themes that the study sample resonates with.

Table 4-2: Composition of the study participants (Adapted from Google Forms, 2024)

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P1	Participant 1	18 -25	Female	Secondary school (Grades 8 – 11)	Employed	Cape Town
P2	Participant 2	30 - 35	Male	Master's Degree/ MTech Degree	Employed	Cape Town
P3	Participant 3	26 - 30	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P4	Participant 4	51 - 55	Female	National Diploma	Employed	Cape Town
P5	Participant 5	26 - 30	Male	Secondary school (Grades 8 – 11)	Employed	Paarl
P6	Participant 6	36 - 40	Female	National Diploma	Employed	Cape Town
P7	Participant 7	51 - 55	Male	Secondary school (Grades 8 – 11)	Employed	Cape Town
P8	Participant 8	26 - 30	Male	Diploma	Employed	Cape Town
P9	Participant 9	46 - 50	Female	National Diploma	Employed	Cape Town
P10	Participant 10	51 - 55	Female	National Diploma	Employed	Cape Town
P11	Participant 11	46 - 50	Male	National Diploma	Employed	Cape Town
P12	Participant 12	41 - 45	Female	National Diploma	Employed	Cape Town
P13	Participant 13	46 - 50	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P14	Participant 14	> 60	Female	National Diploma	Prefer not to say	Cape Town

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P15	Participant 15	> 60	Male	National Diploma	Employed	Cape Town
P16	Participant 16	30 - 35	Male	National Diploma	Employed	Cape Town
P17	Participant 17	51 - 55	Male	National Diploma	Employed	Cape Town
P18	Participant 18	26 - 30	Male	National Diploma	Employed	Cape Town
P19	Participant 19	41 - 45	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P20	Participant 20	41 - 45	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P21	Participant 21	51 - 55	Female	Diploma	Employed	Cape Town
P22	Participant 22	30 - 35	Female	National Diploma	Employed	Cape Town
P23	Participant 23	46 - 50	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Full-time student	Cape Town
P24	Participant 24	30 - 35	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P25	Participant 25	30 - 35	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P26	Participant 26	41 - 45	Male	Secondary school (Grades 8 – 11)	Employed	Cape Town
P27	Participant 27	41 - 45	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P28	Participant 28	30 - 35	Female	National Diploma	Employed	Cape Town
P29	Participant 29	30 - 35	Male	Diploma	Employed	Cape Town

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P30	Participant 30	36 - 40	Male	Prefer not to say	Employed	Cape Town
P31	Participant 31	46 - 50	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P32	Participant 32	36 - 40	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P33	Participant 33	56 - 60	Male	National Diploma	Employed	Cape town
P34	Participant 34	46 - 50	Male	Master's Degree/ MTech Degree	Employed	Cape Town
P35	Participant 35	56 - 60	Male	National Diploma	Employed	Cape Town
P36	Participant 36	41 - 45	Male	National Diploma	Employed	Moorreesburg
P37	Participant 37	41 - 45	Male	Diploma	Employed	Cape Town
P38	Participant 38	46 - 50	Male	Diploma	Employed	Cape Town
P39	Participant 39	41 - 45	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P40	Participant 40	51 - 55	Male	National Diploma	Employed	Cape Town
P41	Participant 41	36 - 40	Male	National Diploma	Employed	Cape Town
P42	Participant 42	51 - 55	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Edgemead
P43	Participant 43	46 - 50	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P44	Participant 44	30 - 35	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P45	Participant 45	> 60	Male	Doctorate/DTech Degree	Not currently employed	Cape Town
P46	Participant 46	51 - 55	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P47	Participant 47	46 - 50	Male	Diploma	Employed	Cape Town
P48	Participant 48	46 - 50	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P49	Participant 49	36 - 40	Female	Diploma	Employed	Cape Town
P50	Participant 50	36 - 40	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P51	Participant 51	46 - 50	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape town
P52	Participant 52	41 - 45	Female	Master’s Degree/ MTech Degree	Employed	Cape Town
P53	Participant 53	41 - 45	Male	National Diploma	Employed	Cape Town
P54	Participant 54	41 - 45	Female	National Diploma	Employed	Cape Town
P55	Participant 55	51 - 55	Male	Doctorate/DTech Degree	Employed	Cape Town
P56	Participant 56	36 - 40	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P57	Participant 57	46 - 50	Female	National Diploma	Employed	Cape Town
P58	Participant 58	41 - 45	Female	Diploma	Employed	Cape Town

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P59	Participant 59	18 -25	Female	National Diploma	Employed	Cape Town
P60	Participant 60	18 -25	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P61	Participant 61	46 - 50	Male	Doctorate/DTech Degree	Employed	Cape Town
P62	Participant 62	18 -25	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P63	Participant 63	46 - 50	Male	National Diploma	Employed	Cape Town
P64	Participant 64	51 - 55	Female	Diploma	Employed	Cape Town
P65	Participant 65	30 - 35	Female	Master’s Degree/ MTech Degree	Employed	Cape Town
P66	Participant 66	36 - 40	Female	National Diploma	Employed	Cape Town
P67	Participant 67	56 - 60	Male	Master’s Degree/ MTech Degree	Employed	Nizwa, Oman
P68	Participant 68	36 - 40	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P69	Participant 69	36 - 40	Female	Diploma	Employed	Cape Town
P70	Participant 70	18 -25	Female	Diploma	Full-time student	Cape town
P71	Participant 71	18 -25	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P72	Participant 72	30 - 35	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P73	Participant 73	30 - 35	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P74	Participant 74	56 - 60	Male	Masters Degree/ MTech Degree	Employed	Cape Town
P75	Participant 75	36 - 40	Female	Doctorate/DTech Degree	Employed	Cape Town
P76	Participant 76	> 60	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P77	Participant 77	41 - 45	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P78	Participant 78	36 - 40	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P79	Participant 79	41 - 45	Prefer not to say	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P80	Participant 80	36 - 40	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P81	Participant 81	30 - 35	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P82	Participant 82	26 - 30	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P83	Participant 83	30 - 35	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P84	Participant 84	30 - 35	Male	Master’s Degree/ MTech Degree	Employed	East London
P85	Participant 85	41 - 45	Female	Master’s Degree/ MTech Degree	Employed	East London
P86	Participant 86	36 - 40	Male	Master’s Degree/ MTech Degree	Employed	Cape Town
P87	Participant 87	36 - 40	Female	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town

CODE	PARTICIPANT NUMBER	AGE GROUP	GENDER	EDUCATION LEVEL	EMPLOYMENT STATUS	RESIDENCE CITY
P88	Participant 88	36 - 40	Male	Advanced Diploma/ BTech Degree/ Honours Degree	Employed	Cape Town
P89	Participant 89	46 - 50	Female	Doctorate/DTech Degree	Employed	Sasolburg
P90	Participant 90	56 - 60	Female	Doctorate/DTech Degree	Employed	Cape Town
P91	Participant 91	41 - 45	Female	Master's Degree/ MTech Degree	Employed	Cape Town
P92	Participant 92	> 60	Female	Doctorate/DTech Degree	Employed	Wellington
P93	Participant 93	30 - 35	Female	Master's Degree/ MTech Degree	Employed	Cape Town
P94	Participant 94	51 - 55	Male	Master's Degree/ MTech Degree	Full-time student	Cape Town
P95	Participant 95	51 - 55	Male	Master's Degree/ MTech Degree	Employed	Cape Town

4.5 Theory

Petronio and Child (2020) are of the opinion that the Communication Privacy Management (CPM) theory hinges on the entrenched tenets of users' social and cultural influences. The authors contend that the values mentioned earlier drive the approach that users apply to their privacy management (Petronio & Child, 2020). Al-Rabeeah and Saeed (2017) and Kasim et al. (2021) assert that the privacy management behaviour of users can be pre-empted by applying the Theory of Planned Behaviour (TPB). Al-Rabeeah and Saeed (2017) propose a data privacy model consisting of an amalgam of CPM and TPB, illustrated in Figure 4-16, to rigorously scrutinise data privacy management behaviour.

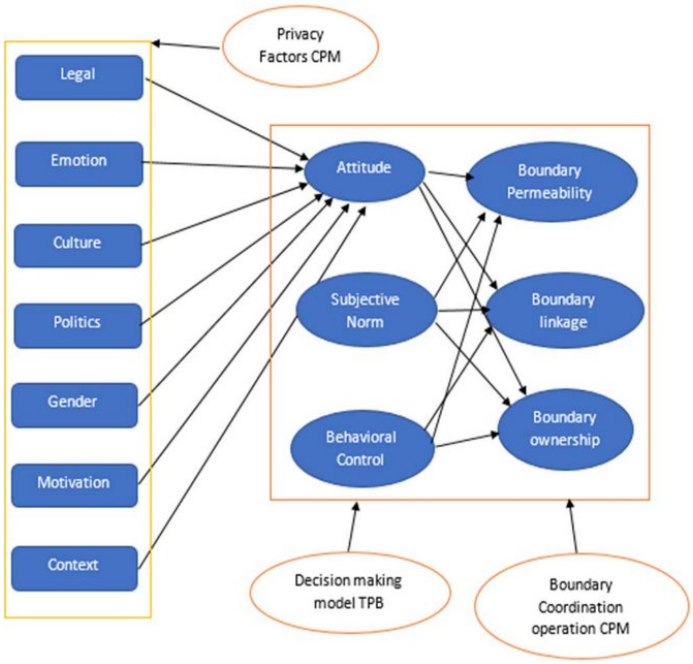


Figure 4-16: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017)

CPM and TPB have previously been used independently in ICT studies, notably in the IEEE Explore and the International Journal of Advanced Computer Science and Applications. In lieu of the Al-Rabeeah and Saeed (2017) combined model recommendation, the researcher employs the combined CPM and TPB theory model as the theoretical lens for the study to reveal deeper meaning. The researcher will attempt to differentiate this qualitative study from similar studies by considering the components indicated earlier in the study as Table 3-2 and Figure 3-1, within the context of the research study.

4.6 Analysis

4.6.1 Getting started

The researcher selected thematic analysis for the data analysis. Saunders et al. (2023) describe their practical steps employed for thematic analysis broadly consisting of “Step 1: Reading”, “Step 2: Coding”, and “Step 3: Theming”. The authors share a rather complex model for the practical thematic analysis to reveal any themes or patterns that could be interpreted (Saunders et al., 2023).

The researcher opted for a simplified version of the model, as mentioned earlier, whilst ensuring conformance with the broad steps and principles. It includes the following steps to analyse the data: 1. Start preparations for data analysis, 2. Consider all data, 3. Codify all data, 4. Create themes, and 5. Devise a means to represent the themes. These steps are illustrated in Figure 4-17 and are further explained hereunder.

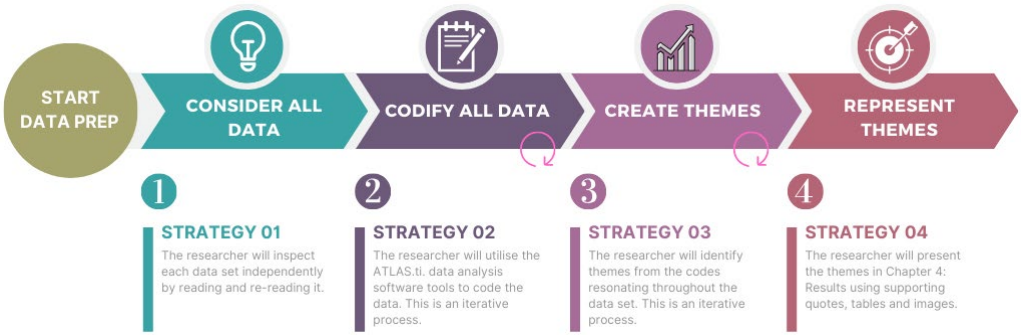


Figure 4-17: Thematic analysis approach
(Adapted from Saunders et al., 2023)

Blaxter *et al.* (2006:206) propose that: “Analysis is about the search for explanation and understanding, in the course of which concepts and theories will likely be advanced, considered and developed.” This includes data analysis that perfectly relates to data collection in the research life cycle. The researcher will attempt to differentiate this mono-qualitative study from similar studies by considering influences like language, gender, age and community within the study’s context.

4.6.2 Data analysis software tools

The researcher opted for a data analysis software tool to facilitate richer analysis than can be achieved through manual thematic analysis methods. Since the researcher has limited means at their disposal, the researcher approached the Cape Peninsula University of Technology (CPUT) for an ATLAS.ti license via the appropriate university channels. The ATLAS.ti data analysis software is well-regarded and easy to use.

Whilst the natural inclination may be to install the software and immediately commence using it, the researcher elected a conservative approach. He read various ATLAS.ti documents attended CPUT ATLAS.ti training sessions and viewed several related YouTube videos to structure his approach to analysis.

The researcher used ATLAS.ti version 24.2.1.32227 for their analysis.

4.6.3 Start data prep

ATLAS.ti essentially uses an Extract, Transform and Load (ETL) logic. The researcher extracted the collected survey data from Google Forms and prepared it by manipulating the headings. An exclamation (!) was added to “Participant” and semi-colons (:) to the remaining headings, as shown below in Figure 4-18. The manipulation of the headings was necessary to import it into ATLAS.ti as a survey source.

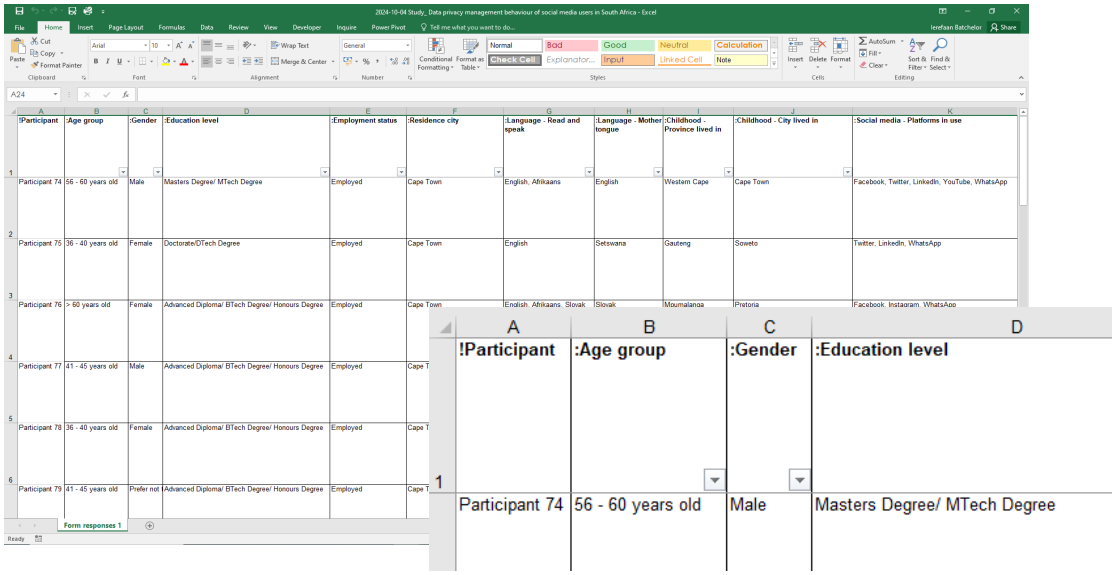


Figure 4-18: Data heading manipulation for import into ATLAS.ti

The researcher navigated to the “Import & Export” tab within ATLAS.ti and commenced the import by selecting the “Survey” button in Figure 4-19, navigating to the .csv Google Form survey extract and clicking the “Open” button.

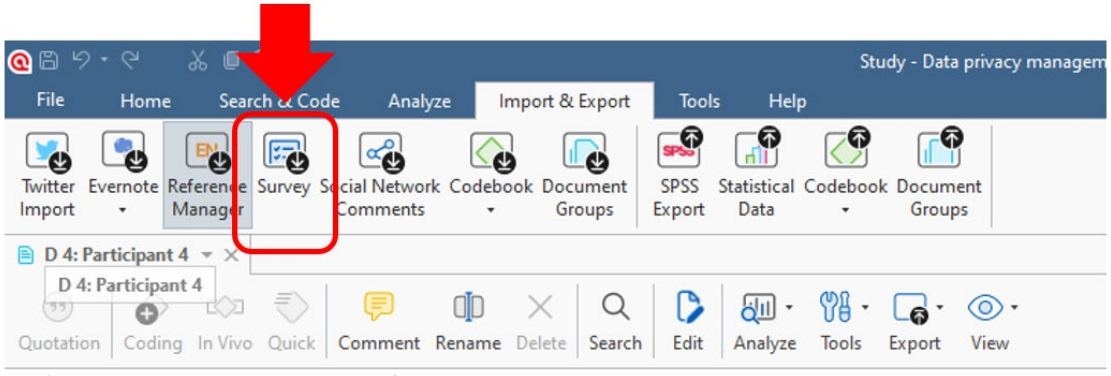


Figure 4-19: Importing .csv format survey into ATLAS.ti

The survey data questions were queued for loading in the dialogue and necessitated the researcher to make selections, as depicted in Figure 4-20, for each survey question to be transformed correctly. Subsequently, the data was successfully loaded into ATLAS.ti.

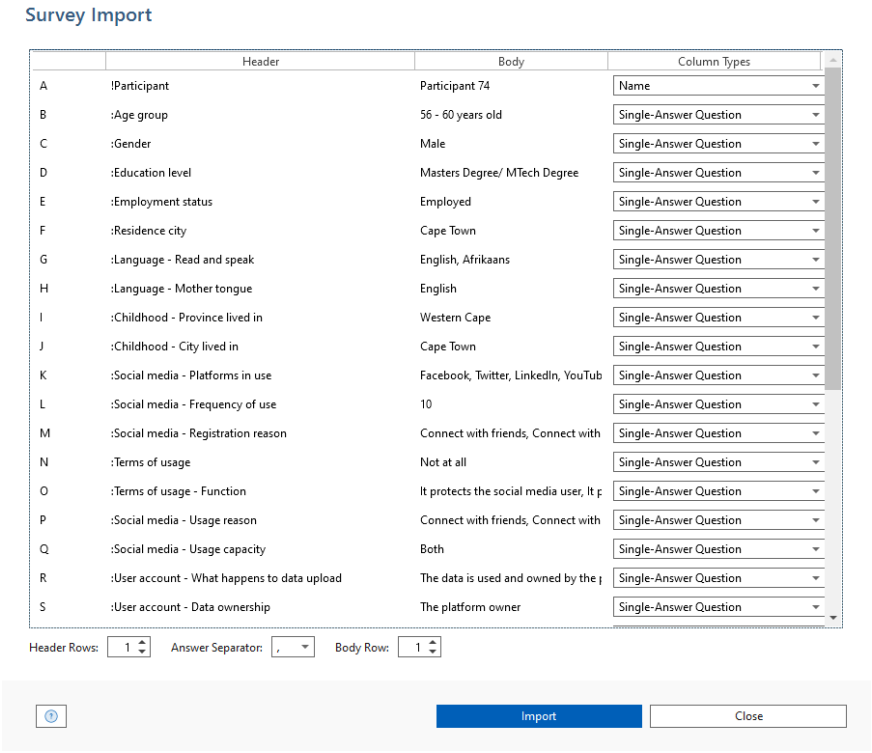


Figure 4-20: Survey import question selections in ATLAS.ti

The next step was for the researcher to inspect each data set independently by reading and re-reading it.

4.6.4 Thematic analysis

4.6.4.1 Step 1: Consider all data

The researcher reminded himself of the research problem statement, research question and objectives in Figure 4-1 and

~~.~~Additionally, the researcher had to orient himself as ATLAS.ti locates the open-ended survey questions under the “Documents” shown in Figure 4-21, and the multiple choice survey questions are found under the “Document Groups” depicted in Figure 4-22 and Table 4-1 above.

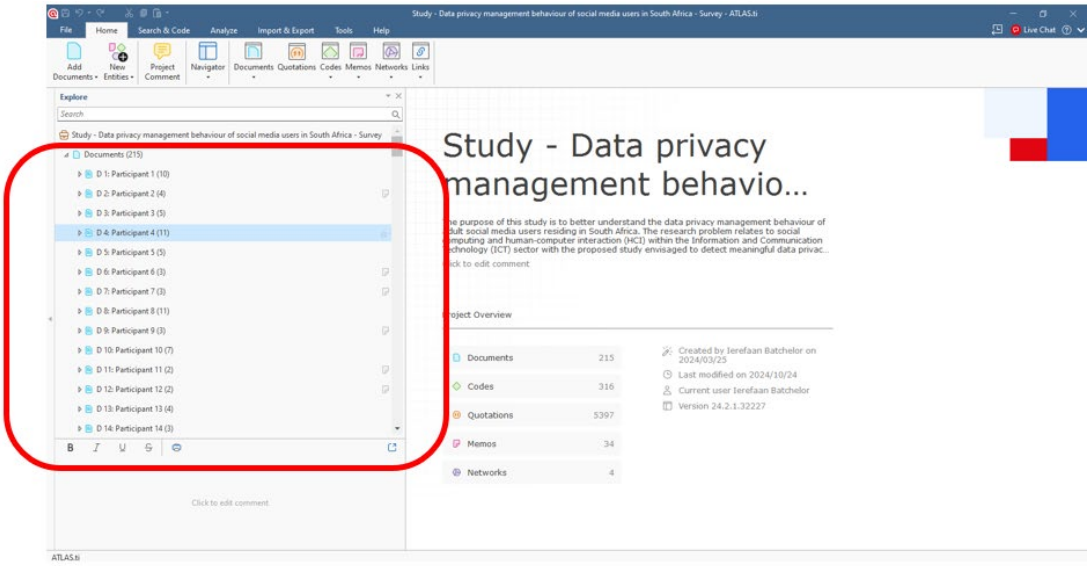


Figure 4-21: Documents in ATLAS.ti

Each participant's response is listed under these respective sections. The individual participant responses are named "Participant" and paired with their relevant sequential number, illustrated in Table 4-2, for clear identification. After understanding where the relevant data was located in ATLAS.ti, the researcher proceeded to comprehensively read and re-read the individual survey responses. It is necessary to fully grasp the response to ensure that it is appropriately codified.

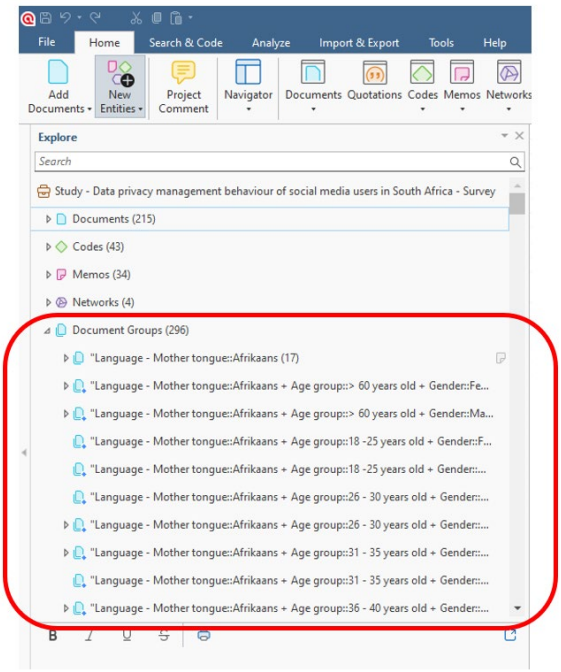


Figure 4-22: Document groups in ATLAS.ti

Iteration is key. It may prove necessary to re-read sections that were previously considered complete. The researcher followed this approach to ensure that the content was accurately reflected and nothing was missed. For example, the researcher read and re-read a passage of text to fully understand it prior to initiating the coding process. As stated above, it is sometimes necessary to revisit previously read and codified passages of text to ensure that they were coded correctly and that no valuable pieces of raw data are overlooked in the analysis. The first pass of the under-mentioned passage of text revealed a code-named “User account – What happens to data upload”. Initially, codes for “Upload – Marketing: Understand client better” and “Upload: Benefit: Benefit to service provider” were missing. Additionally, variants of the code “User account – What happens to data upload” were initially captured by the researcher. These issues were remediated through the iterative approach applied.

Sample quotation

P1 states “It is used to interpret what consumers do, what their interests are, their beliefs. They use the data they choose, the useful data, to benefit their business and their future. Personalised advertising. They would get paid to advertise. Essentially, using the data to personalise ads would result in more sales. And getting paid more to keep advertising.”

4.6.4.2 Step 2: Codify all data

After thoroughly reading the responses, the researcher codified the data by highlighting the text in ATLAS.ti and selecting the “Coding” button. The researcher either had to capture a new code or use an existing code to code the highlighted text. The selection of the code depends on the content and what the researcher finds most appropriately represents the selected text. Therefore, the decision to name the code is directly linked to the main idea that is raised in the quotation. This can be observed in Figure 4-23, where the participant’s response is located on the left-hand side of the image. As the researcher codes the text, the code and quotation will appear on the right-hand side of Figure 4-23.

The coding step could be iteratively refined. In this analysis, after the initial coding, the researcher revisited the coding by either leaving it as originally coded, editing the name of a code, splitting a code or merging multiple similar codes into one code informed by the patterns that form. For example, the researcher revisited the under-mentioned passage of text to ensure that it was coded correctly. In the initial coding pass, the researcher created several codes, including “Breach outlook” and “Breach attitude”. He revisited the passage of text and noticed the similarities in the codes. He rationalised the separate quotes into a single code-named “Breach attitude” to ensure coding efficiency and effectiveness of analysis. Subsequent passes of the text led to an enhanced understanding of the text and improved accuracy in coding.

Sample quotation

“I have been on high alert regarding my privacy since my account was hacked. Taking extreme caution to protect my account.”

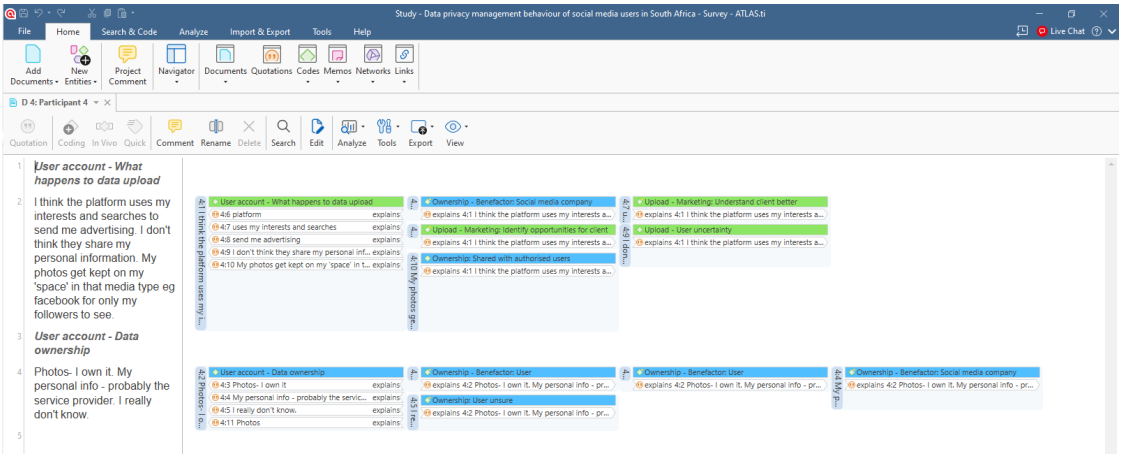


Figure 4-23: Codification of the raw data in ATLAS.ti

The researcher continued to code the various pieces of text and noticed numerous codes that appeared related. He opted to create “Categories” and associated these related codes under the “Categories”. “Data - Risk” is an example of a “Category” with the codes “Low”, “Medium”, and “High” nested underneath it in Figure 4-24. The Codes were initially independently coded with long, complex names. The coding iteration for the example, as mentioned earlier, allows for improved grouping under a Category and improved coding names to allow for analysis improvements.

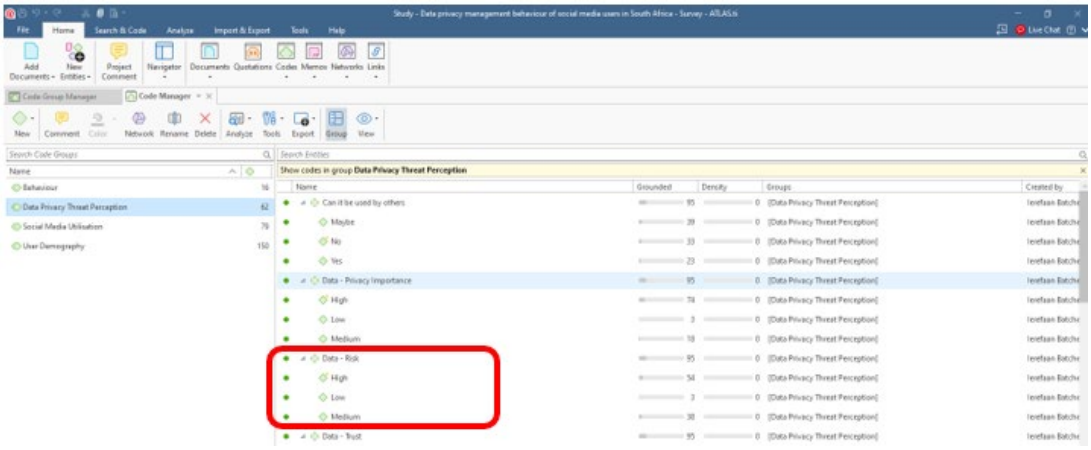


Figure 4-24: Codes and categories in ATLAS.ti

Additionally, some of the original Likert scale responses were onerous, with some options very closely resembling other options. The researcher addressed this by collapsing some of the

separately coded responses. For example, survey question 14 presents the options “Not at all”, “Does not matter, it is all the same”, “Skimmed over it”, “Partly read it”, and “Read in full”. After revisiting the initial codes, the researcher realised that “Not at all” and “Does not matter, it is all the same” were very similar and decided to collapse this into the code “Not read at all”. The coding iteration for the example, as mentioned earlier, allows for coding refinement and improved coding names to allow for analysis improvements.

Furthermore, the researcher formed compound codes referred to as “Smart Codes” for deeper analysis and insights. These “Smart Codes” are formed by selecting two or more codes, right-clicking and selecting “Create Smart Code” from the menu shown in Figure 4-25. The “Smart Code”, by default, assumes the name concatenated from the independent codes selected. After the “Smart Code” is created, it can be used in the analysis of the raw data. It is important to note that the “Smart Codes” can only be identified and created after the initial coding passes.

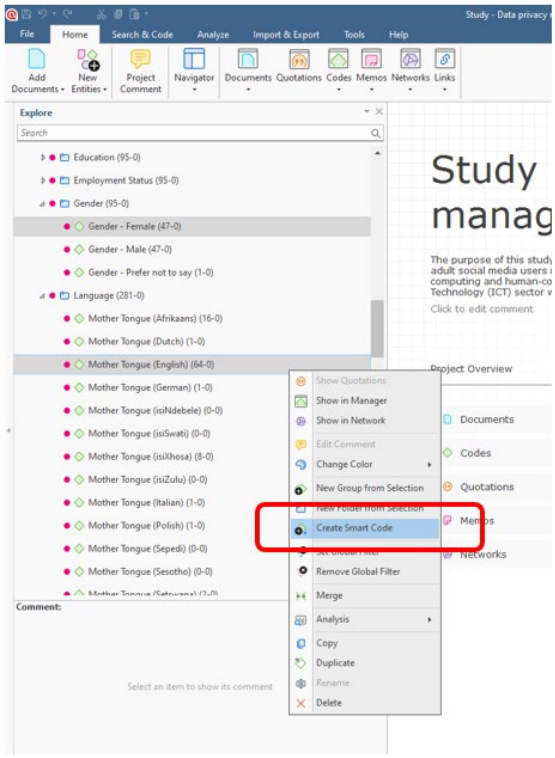


Figure 4-25: Smart codes in ATLAS.ti

4.6.4.3 Step 3: Create themes

The researcher concluded the coding function and identified themes in ATLAS.ti. This was achieved in ATLAS.ti by selecting one or more codes and moving them under the appropriate Code Groups, as shown in Figure 4-26. Similarly, codes can be removed from themes.

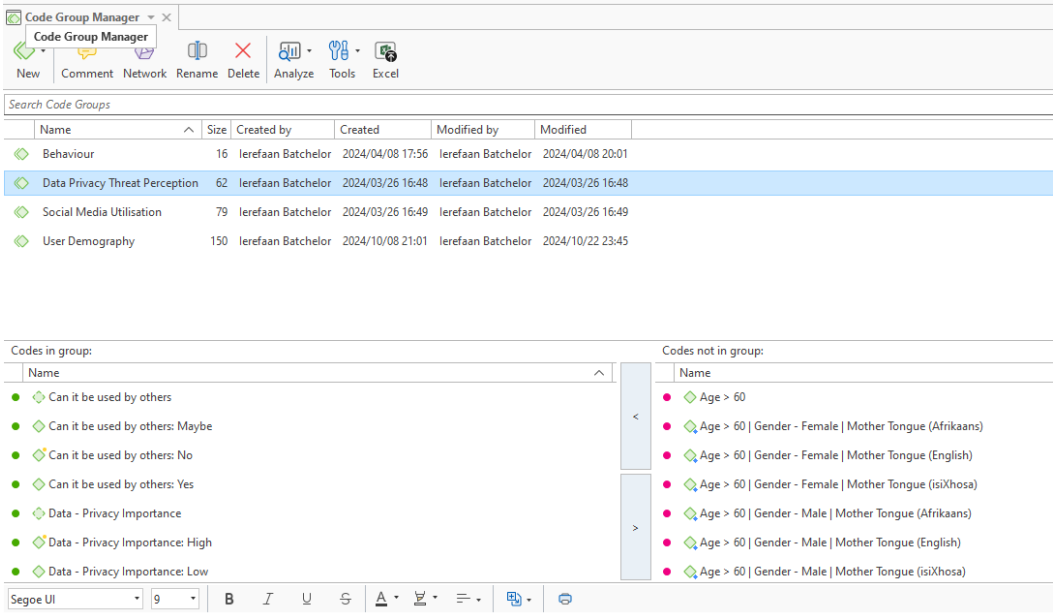


Figure 4-26: Adding codes to code groups in ATLAS.ti

This step could be iteratively refined. In this analysis, after the initial grouping, the researcher revisited the grouping, leaving it either unaltered or shifting it to the appropriate Code Group. These amendments are informed by patterns that form in the text. For example, the first pass of theme formation led to the researcher identifying two (2) themes, namely: “Social media utilisation” and “Social media beneficiary”. This was due to the codes relating to ownership where the beneficiary was either the social media user or the social media platform. After a few passes of the thematic analysis, the researcher realised that it was more appropriate for the “Social media beneficiary” theme to be collapsed under the “Social media utilisation” theme.

4.6.4.4 Step 4: Represent themes

The prevailing themes from the data analysis are outlined to answer the main research question. The three (3) themes are summarised in the tables below and will be discussed in

more detail in the next sections. The under-mentioned themes started the initial theme formulation journey as seven (7) themes and were iteratively refined into the three (3) listed below in Table 4-3, Table 4-4 and Table 4-5. The transition from seven (7) to three (3) themes is due to the code, category and theme refinement resulting from iteration.

RQ: What is the data privacy management behaviour of adult social media users?

Table 4-3: Theme 1 - Data privacy management (Adapted from ATLAS.ti, 2024)

COMPONENTS OF THEME 1	OBJECTIVE 1
Can it be used by others?	Objective: To explore the privacy management methods and techniques employed
Permission to use data for incentive	
Privacy importance	
Trust	
Risk	
Data protection	
Upload	

Theme 1, identified as “Data privacy management”, is formulated for the components represented in Table 4-3 and links to the objective “To explore the privacy management methods and techniques employed”. Theme 1 attempts to answer the Sub-research Question 1, “How do adult social media users manage their privacy when interacting on a social media platform?” The components are essentially each a “Category” formed from the independent “Code”. Section 4.6.4.2 explains the process applied for iteration and coding refinement in detail. Each component of the theme or “Category” is made up of a “Code”, and each “Code” is discovered from the researcher’s evaluation of the passages of text.

The respective “Theme”, “Category”, and “Code” are outlined below. The researcher started by selecting the text and codifying it. Thereafter, he rationalised and refined the codes with subsequent codification passes. Lastly, the researcher formed categories from the linked codes that ultimately led to the development of themes.

- **Theme:** Data privacy management
    - **Category:** Can it be used by others
        - **Code:** No
        - **Code:** Maybe
        - **Code:** Yes
- **Theme:** Data privacy management
    - **Category:** Permission to use data for incentive
        - **Code:** No
        - **Code:** Maybe
        - **Code:** Yes
- **Theme:** Data privacy management
    - **Category:** Privacy importance
        - **Code:** Low
        - **Code:** Medium
        - **Code:** High
- **Theme:** Data privacy management
    - **Category:** Trust
        - **Code:** Low
        - **Code:** Medium
        - **Code:** High

- **Theme:** Data privacy management
    - **Category:** Risk
        - **Code:** Low
        - **Code:** Medium
        - **Code:** High
- **Theme:** Data privacy management
    - **Category:** Data protection
        - **Code:** Not at all
        - **Code:** Take basic precaution
        - **Code:** Take every precaution
- **Theme:** Data privacy management
    - **Category:** Upload benefit
        - **Code:** Benefit for social media users
        - **Code:** Benefit for government
        - **Code:** Benefit to service provider

The section, as mentioned earlier, describes the representation of Theme 1. It lists the codes formed from the passages of text or quotation that the researcher evaluated. The codes are rationalised and improved for efficiency, leading to categories. After the coding and categorisation, the researcher reviewed the data and noted a theme forming that related to “data privacy”, “threats”, and user “perception”. Theme 2 on “Social media utilisation” will be discussed hereunder.

Table 4-4: Theme 2 - Social media utilisation and threat perception
(Adapted from ATLAS.ti, 2024)

COMPONENTS OF THEME 2	OBJECTIVE 2
Ownership	Objective: To determine the data privacy threat perception
Registration reason	
Usage purpose	
Terms of service	

Theme 2, identified as “Social media utilisation”, is formulated for the components represented in Table 4-4 and links to the objective “To determine the data privacy threat perception”. Theme 2 attempts to answer the Sub-research Question 2, “What is the perceived privacy threat awareness level of adult social media users?” The components are essentially each a “Category” formed from the independent “Code”. Section 4.6.4.2 explains the process applied for iteration and coding refinement in detail. Each component of the theme or “Category” is made up of a “Code”, and each “Code” is discovered from the researcher’s evaluation of the passages of text.

The respective “Theme”, “Category”, and “Code” are outlined below. The researcher started by selecting the text and codifying it. Thereafter, he rationalised and refined the codes with subsequent codification passes. Lastly, the researcher formed categories from the linked codes that ultimately led to the development of themes.

- ***Theme: Social media utilisation***
    - **Category: Ownership**
        - **Code:** User
        - **Code:** Social media company
        - **Code:** Other company
        - **Code:** Government entity

- ***Theme: Social media utilisation***
    - **Category:** Registration reason
        - **Code:** Friends
        - **Code:** Family
        - **Code:** Communities
        - **Code:** Follow trends
        - **Code:** Interests
        - **Code:** Market business
        - **Code:** Other (Entertainment)
        - **Code:** Participate in online discussions
        - **Code:** Post media
        - **Code:** Share information
        - **Code:** Spare time
        - **Code:** Classifieds (Buying)
        - **Code:** Classifieds (Selling)
- ***Theme: Social media utilisation***
    - **Category:** Usage purpose
        - **Code:** Friends
        - **Code:** Family
        - **Code:** Communities
        - **Code:** Follow trends
        - **Code:** Interests

        - **Code:** Market business
        - **Code:** Other (Entertainment)
        - **Code:** Participate in online discussions
        - **Code:** Post media
        - **Code:** Share information
        - **Code:** Spare time
        - **Code:** Classifieds (Buying)
        - **Code:** Classifieds (Selling)

- ***Theme: Social media utilisation***
    - **Category:** Terms of service
        - **Code:** Not read at all
        - **Code:** Partly read
        - **Code:** Read in full

The section, as mentioned earlier, describes the representation of Theme 2. It lists the codes formed from the passages of text or quotation that the researcher evaluated. The codes are rationalised and improved for efficiency, leading to categories. After the coding and categorisation, the researcher reviewed the data and noted a theme forming that related to “social media” platforms and “usage” thereof. Theme 3 on “Behaviour” will be discussed hereunder.

Table 4-5: Theme 3 – Behaviour (Adapted from ATLAS.ti, 2024)

COMPONENTS OF THEME 3	OBJECTIVE 3
Breach awareness	Objective: To identify behavioural barriers to data privacy management implementation
Breach attitude	
Breach behaviour	
Personal experience	

Theme 3, identified as “Behaviour”, is formulated for the components represented in Table 4-5 and links to the objective “To identify behavioural barriers to data privacy management implementation”. Theme 3 attempts to answer the Sub-research Question 3, “What are the behavioural barriers to privacy management implementation for adult social media users?” The components are essentially each a “Category” formed from the independent “Code”. Section 4.6.4.2 explains the process applied for iteration and coding refinement in detail. Each component of the theme or “Category” is made up of a “Code”, and each “Code” is discovered from the researcher’s evaluation of the passages of text.

The respective “Theme”, “Category”, and “Code” are outlined below. The researcher started by selecting the text and codifying it. Thereafter, he rationalised and refined the codes with subsequent codification passes. Lastly, the researcher formed categories from the linked codes that ultimately led to the development of themes.

- ***Theme:*** *Behaviour*
    - **Category:** Breach awareness
        - **Code:** No
        - **Code:** Not sure
        - **Code:** Yes

- ***Theme:*** *Behaviour*
    - **Category:** Breach attitude
        - **Code:** Minimal protection approach
        - **Code:** Maximum protection approach
- ***Theme:*** *Behaviour*
    - **Category:** Breach behaviour
        - **Code:** No - change observed
        - **Code:** Yes – change observed
- ***Theme:*** *Behaviour*
    - **Category:** Personal experience
        - **Code:** No
        - **Code:** Not sure
        - **Code:** Yes

Kemp (2024) asserts that the adult social media user population in South Africa amounts to approximately twenty-six (26) million users. It is important to note that the study sample is comprised of 95 participants and can, therefore, not be generalised. However, the findings observed will resonate within the study sample.

4.7 Data presentation of findings

The findings are presented using the prevailing themes and codes from the data analysis to answer the main research question.

RQ: What is the data privacy management behaviour of adult social media users?

Figure 4-27 hereunder provides a holistic view of the researcher's approach to the data analysis. The purpose of the analysis is to answer the research question and sub-research questions. The researcher will use the under-mentioned approach to determine the data

privacy management behaviour of adult social media users in South Africa. The demographic data shapes the lens through which the analysis will be filtered, looking at the respective themes and components thereof. The items mentioned earlier are presented independently and will be discussed in more detail in the next sections.

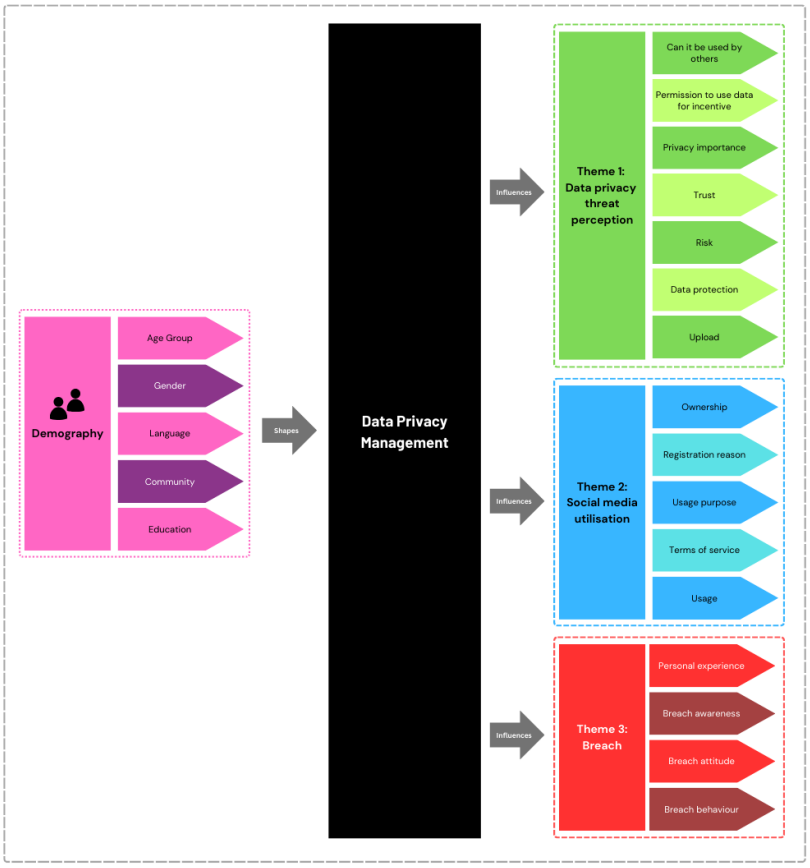


Figure 4-27: Conceptual framework – combined CPM & TPB theory model (Adapted from Al-Rabeeah and Saeed, 2017)

4.7.1 Research objective 1

Research Objective 1: To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.

SRQ1: How do adult social media users manage their privacy when interacting on a social media platform?

Survey Question 14: When you registered with a social media platform, did you read the “Terms of Usage” for the social media platform?

Selection criterion:

Survey question 14 is selected to determine the privacy techniques and outlook of adult social media users when interacting on a social media platform. The question uses a Likert scale to capture the authentic responses of the participants.

The Sankey diagram in Figure 4-28 is generated using Atlas.ti. Figure 4-28 represents the study participants' responses to survey question 14. The question provided five (5) response options, including “Not at all”, “Does not matter, it is all the same”, “Skimmed over it”, “Partly read it”, and “Read in full”. As described in section 4.6.4.2, the researcher rationalised the codes in lieu of their similarities into three (3) codes, namely: “Terms of service: Read in full”, “Terms of service: Partly read” and “Terms of service: Not read at all”. “Not at all” and “Does not matter, it is all the same” are coded as “Terms of service: Not read at all”, and “Skimmed over it” and “Partly read it” are coded as “Terms of service: Partly read”. Simplification of the codes from five (5) to three (3) allows for more efficient representation. The participants’ responses to survey questions are illustrated in Figure 4-28 and described in detail below.

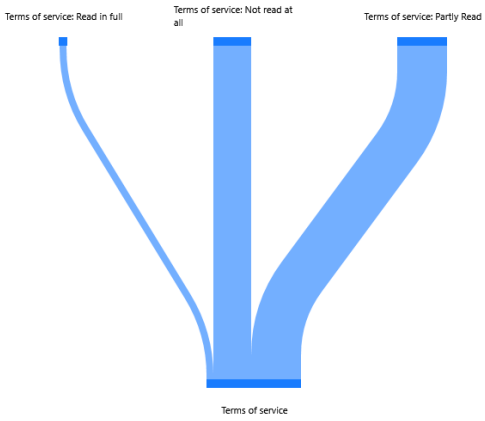


Figure 4-28: Code - Terms of Service
(ATLAS.ti, 2024)

P2, P3, P4, P13, P18, P23, P25, P27, P30, P31, P32, P33, P36, P37, P43, P45, P47, P49, P52, P55, P56, P57, P59, P60, P61, P62, P66, P68, P71, P72, P74, P81, P82, P83, P84, P88, P89 and **P95** amounting to 38 participants acknowledged that they did not read the Terms of Service of their subscribed social media platforms. The thickness and weighting of the line in Figure 4-28 mean that this is the second-highest count of participant responses for this survey question. The fact that this group of participants affirmed that they did not read the Terms of Service is remarkable.

P1, P5, P6, P10, P11, P12, P14, P15, P16, P17, P19, P20, P22, P24, P26, P28, P29, P34, P35, P38, P39, P40, P41, P42, P46, P48, P50, P51, P54, P58, P63, P65, P67, P69, P70, P73, P75, P76, P77, P78, P79, P80, P85, P86, P87, P90, P91, P92, P93 and **P94** representing 50 participants partly read the Terms of Service of their subscribed social media platforms. The thickness and weighting of the line for participants' responses that they partly read the Terms of Service is the most prominent in the Sankey diagram in Figure 4-28. This serves as a visual affirmation of the highest count.

Lastly, **P7, P8, P9, P21, P44, P53** and **P64** constituted seven (7) participants who responded that they read the Terms of Service in full for their subscribed social media platforms. The thickness and weighting of the line in Figure 4-28 denote that this is the lowest count of participant responses for this survey question.

Survey question 14 is explored further in Table 4-6, Table 4-7 and Table 4 8.

A total of six (6) participants do not have post-senior secondary education and constitute a minute portion of the sample. Additionally, 68 of the participants spent their childhood years

in Cape Town, and the data does not demonstrate any clear patterns. Therefore, the education levels and childhood data have been excluded from the representation.

Table 4-6: Terms of Service vs Language

Terms of Service	Language - Mother tongue	Count
Not read at all	Afrikaans	6
	Dutch	1
	English	26
	isiXhosa	3
	Polish	1
	Setswana	1
Partly read	Afrikaans	8
	English	33
	German	1
	isiXhosa	5
	Italian	1
	Setswana	1
	Slovak	1
Read in full	Afrikaans	3
	English	4
Grand Total		**95**

Table 4-6 presents a breakdown of the mother-tongue speakers and their approach adopted for the Terms of Service for the social media platforms. A small contingent of seven (7) participants read the Terms of Service in full. This small group of participants are limited to three (3) Afrikaans and four (4) English mother-tongue speakers. The remaining participants either partly read or did not read it at all. No further observations are recorded.

Table 4-7: Terms of Service vs Age Group

Terms of Service	Age group	Count
Not read at all	18 - 25	4
	26 - 30	3
	31 - 35	6
	36 - 40	7
	41 - 45	4
	46 - 50	8
	51 - 55	3
	56 - 60	2
	61 and above	1
Partly read	18 - 25	2
	26 - 30	1
	31 - 35	8
	36 - 40	9
	41 - 45	11
	46 - 50	6
	51 - 55	6
	56 - 60	3
	61 and above	4
Read in full	26 - 30	1
	31 - 35	1
	41 - 45	1
	46 - 50	1
	51 - 55	3
Grand Total		**95**

Terms of Service versus Age group are represented in Table 4-7. All age groups are represented in the “Not read at all” and “Partly read” groups. A small contingent of seven (7) participants read the Terms of Service in full. This small group of participants are limited to the 26-30, 31-35, 41-45, 46-50 and 51-55 age groups. Moreover, the 18-25, 36-40, 56-60 and 61 and above age groups are not represented in the “Read in full” group. No further observations are recorded. Terms of Service versus Gender and Age group are represented in Table 4-8.

Most genders and age groups are represented in the “Not read at all” and “Partly read” groups. The small contingent of seven (7) participants that read the Terms of Service in full is made up of females in the 46-50 and 51-55 age groups and males in the 26-30, 31-35, 41-45 and

51-55 age groups. The gender and age group cohorts lack representation for most age groups, both male and female. No further observations are recorded.

Table 4-8: Terms of Service vs Gender and Age Group

Terms of Service	Gender	Age group	Count
Not read at all	Female	18 - 25	4
		26 - 30	1
		31 - 35	4
		36 - 40	4
		41 - 45	1
		46 - 50	3
		51 - 55	1
	Male	26 - 30	2
		31 - 35	2
		36 - 40	3
		41 - 45	3
		46 - 50	5
		51 - 55	2
		56 - 60	2
		61 and above	1
Partly read	Female	18 - 25	2
		31 - 35	5
		36 - 40	6
		41 - 45	5
		46 - 50	1
		51 - 55	2
		56 - 60	1
		61 and above	3
	Male	26 - 30	1
		31 - 35	3
		36 - 40	3
		41 - 45	5
		46 - 50	5
		51 - 55	4
		56 - 60	2
		61 and above	1
	Prefer not to say	41 - 45	1
Read in full	Female	46 - 50	1
		51 - 55	2
	Male	26 - 30	1
		31 - 35	1
		41 - 45	1
		51 - 55	1
Grand Total			**95**

The next survey questions delve into the evolution of social media users' usage over time.

Survey Question 13: Why did you register for a social media platform?

and

Survey Question 16: How do you use social media? Select all that apply.

Selection criterion:

Survey questions 13 and 16 are selected to determine the use case shift over time of adult social media users when interacting on a social media platform. Whilst the focus of this question is on how users interact on the social media platform, it also speaks to their privacy techniques and outlook. The question uses a multi-select list to capture the authentic responses of the participants.

The participants' responses to survey questions 13 and 16 are represented in Figure 4-29 as "Registration reason" and "Usage reason", respectively. The results are discussed in detail hereunder.

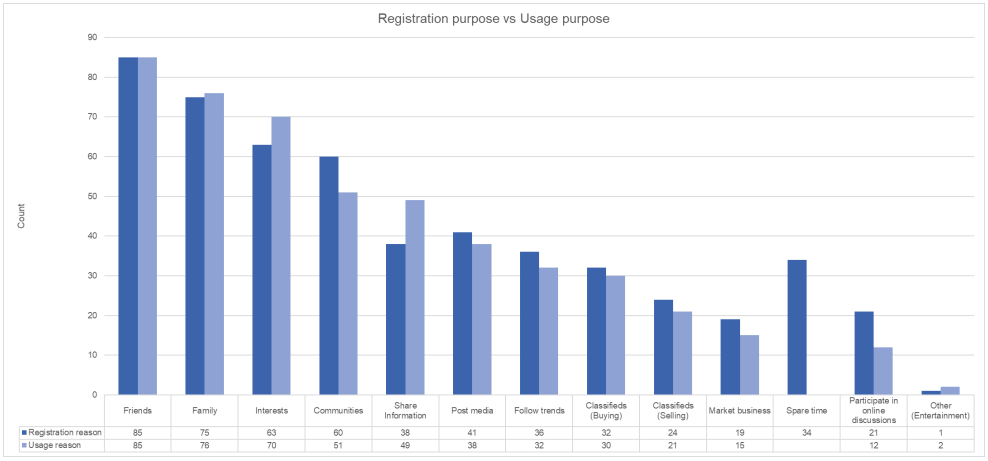


Figure 4-29: Code - Registration vs Usage Purpose
(Adapted from ATLAS.ti, 2024)

The researcher extracted the raw data for survey questions 13 and 16 and loaded it into Microsoft Excel. The bar chart in Figure 4-29, compiled using the Microsoft Excel Pivot Chart functionality, illustrates the data collected for survey questions 13 and 16. Several shifts between the initial registration reason and the current usage reason are noted.

The social media cases for the Family, Interests, Share Information and Other (Entertainment) groupings all demonstrate increases. The most notable increases are for the Interests and Share Information groupings at increases of seven (7) and eleven (11), respectively. Whilst the increased numbers are relatively small, it must be noted that the number of participants is also small, at a total of 95 participants. The increase, as mentioned earlier, constitutes improvements of 11% and 29%, respectively.

Additionally, it can be seen that the registration reasons for groupings like Communities, Post media, Follow trends, Classifieds (Buying), Classifieds (Selling), Market business, Spare time and Participate in online discussions have decreased. The most notable decreases are for Spare time Participate in online discussions and Communities. The dramatic shift observed for Spare time usage dropped from 34 participants to zero. The spare time shift represents a 100% decrease in usage behaviour.

The next survey question attempts to understand content ownership from the perspective of social media users to answer the privacy techniques and outlook of participants. It is important to note that this question has been used to answer both SRQ1 and SRQ2. This is possible given the richness of the response and the identified codes linked to SRQ1 and SRQ2.

Survey Question 19: Who do you think owns the data that you upload?

Selection criterion:

Survey question 19 is selected to determine the privacy techniques and outlook of adult social media users when interacting on a social media platform. An open-ended question is posed to capture the rich, authentic responses of the participants to determine who they perceive as the owners of the uploaded data.

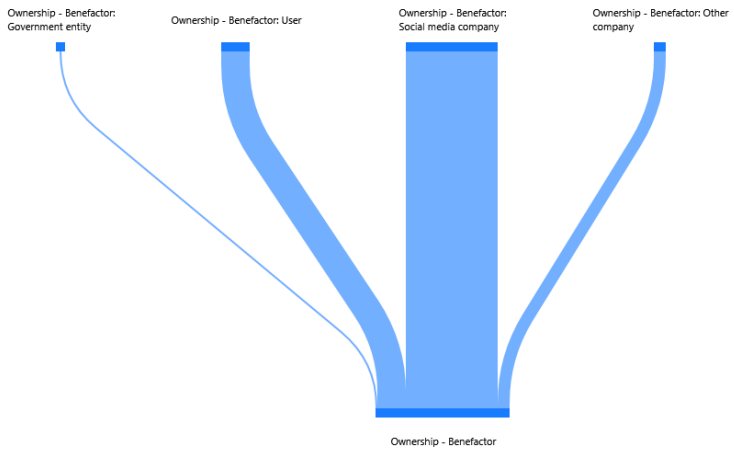


Figure 4-30: Code - Data ownership (ATLAS.ti, 2024)

Figure 4-30 depicts the study participants' responses to survey question 19 in a Sankey diagram generated by Atlas.ti. Participants were asked an open-ended question as to who they believed owned the data uploaded to social media platforms. The participants' responses were codified in ATLAS.ti as "Ownership – Benefactor: User", "Ownership – Benefactor: Social media company", "Ownership – Benefactor: Other company", and "Ownership – Benefactor: Government entity". The overwhelming response is depicted in the Sankey diagram in Figure 4-30, with most participants stating that the social media company is the owner and beneficiary of the uploaded data.

P1, P4, P5, P6, P8, P10, P12, P14, P15, P16, P18, P19, P21, P22, P23, P24, P235, P26, P27, P28, P29, P30, P31, P 33, P34, P35, P36, P37, P38, P40, P41, P42, P43, P44, P45, P46, P47, P48, P50, P51, 55, P56, P58, P59, P61, P62, P64, P66, P67, P69, P70, P71, P73, P74, P76, P77, P78, P79, P80, P81, P82, P84, P86, P87, P88, P90, P91, P93, P94 and **P95** amounting to a unanimous count of 70 out of 86 participants responded that they believed that the social media company or platform owned the uploaded content. This fact is confirmed by the broad line denoting "Ownership – Benefactor: Social media company" in the Sankey diagram in Figure 4-30. The result is remarkably interesting when viewed against section 2.6.

P7, P9, P13, P17, and **P60,** accounting for five (5) participants, alluded to other companies or service providers owning the data uploads provided by social media users. Similarly, one (1) participant, **P63,** stated that the uploaded data was wholly owned by government entities. The Sankey diagram in Figure 4-30 provides two (2) separate and slender lines to represent the

“Ownership – Benefactor: Other company” and “Ownership – Benefactor: Government entity”. Both lines are in sharp contrast to the “Ownership – Benefactor: Social media company” line.

Nine (9) participants elected to not submit a response and have been excluded from the analysis of this survey question.

Lastly, **P2, P3, P10, P20, P39, P52, P54, P68, P75** and **P83** constituted ten (10) participants who responded that the social media users owned the uploaded content. The Sankey diagram depicts the moderately sized “Ownership – Benefactor: User” line. It has a fair representation but cannot come close to the “Ownership – Benefactor: Social media company” line.

The under-mentioned word cloud provides a holistic view of the participants’ data privacy concerns when interacting on social media platforms.

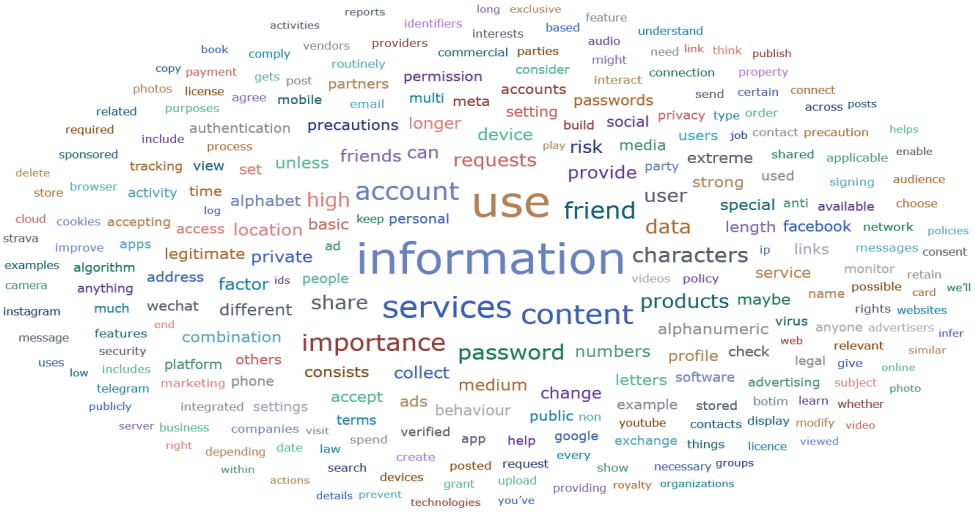


Figure 4-31: Theme 1: Data privacy threat perception word cloud (ATLAS.ti, 2024)

The size and prominence of the word are linked to the frequency that participants have expressed in their responses to select survey questions aimed at answering data privacy management. It confirms that the participants consider “information” their primary concern for data privacy management. Furthermore, the words “use”, “services”, “content”, “account”, “high”, “importance”, “friend”, “data”, and “password” form the next two (2) levels of concern as they are the next largest and prominent words in the word cloud. These words relay the

participants' next most pressing concerns when they manage their privacy whilst interacting on a social media platform.

The above-mentioned survey questions were selected to determine the privacy techniques and outlook of adult social media users when interacting on a social media platform. The findings are formulated using the results from the very same privacy techniques and outlook of adult social media users when interacting on a social media platform. The findings are presented hereunder.

Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.6. of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.

Finding 2: Most of the participants express heightened concern over their information, content and data on social media platforms.

Finding 3: Social media platform use cases evolving demonstrate usefulness either not available or not as well implemented as at the time of registration. The groupings for Interests and Share information have proven most useful.

Finding 4: There is a reduction in the use of groupings for Spare time, Participate in online discussions and Communities.

In summary, most of the participants did not read or did not understand the Terms of Service. The aforementioned data privacy management behaviour exhibited is contrary to the concerns flagged by the participants in subsequent survey questions. Moreover, there have been shifts in social media usage patterns over time, which illustrate that the usage requirements of participants have changed. The findings reveal gaps and issues that pervade most adult social media users, thereby impacting their data privacy practices.

4.7.2 Research objective 2

Research Objective 2: To determine the data privacy threat perception of adult social media users residing in South Africa.

SRQ2: What is the perceived privacy threat awareness level of adult social media users?

Survey Question 18: Please explain in your own words what you think happens with the data/information you upload to a social media platform?

Selection criterion:

Survey question 18 is selected to reveal the privacy threat awareness level of adult social media users when interacting on a social media platform. An open-ended question is posed to capture the rich, authentic responses of the participants to unearth their awareness level of privacy threats.

The participant's responses to the open-ended Survey Question 18 are onerous. Moreover, the core of some participant's responses is similar. Therefore, the quotations below will be limited to the most notable examples that are representative of the grouped responses.

P1 states that "It is used to interpret what consumers do, what their interests are, their beliefs. They use the data they choose, the useful data, to benefit their business and their future. Personalised advertising. They would get paid to advertise. Then using the data to personalise ads would result in more sales essentially. And getting paid more to keep advertising". According to **P4**, "I think the platform uses my interests and searches to send me advertising. I don't think they share my personal information. My photos get kept on my 'space' in that media type, e.g. Facebook, for only my followers to see". **P8** concludes that **"**Social platforms sell your data and information to different collection companies". **P14** proposes that "Its being used by companies to see what interests you." **P18** critiques that "The service provider uses the data/information in order track your activity. They then analyse the data in order to present things to keep the user using the platform based on your activity. I assume they also use the data to improve the platform."

P1, P4, P8, P14 and **P18** outline that the social media companies mine the uploaded data and users' interactions on the platforms for financial gain through targeted marketing and content recommendations. **P8** adds that the data is sold to third parties for marketing and research purposes. **P18** argues that social media platforms further track utilisation to drive improvement in their offering. The participants relayed their thoughts on the data they uploaded to social media platforms and expressed legitimate sentiments.

P10 stated that, "It is available for all to see, at any given time. Anything uploaded to social media will always be in the backend. Can be found/traced for years to come." **P58** reports that

“Others will be able to view and share the information.” **P67** is of the opinion that “Anyone who can see the information can download and use it”.

P10, P58 and **P67** propose that the uploaded data is visible and can be downloaded by all social media users. The participants believe that the uploaded data is devoid of any safeguards. The participants’ sentiments conveyed are not entirely accurate. However, the participants do express some concerns that need clarification.

P52 claims that “It is stored online according to my specifications on the platform (ito privacy)”. **P83** argues that "I think it depends on whether or not you have made your account private or public. I should think that when your account is set to private, only people who you have as friends or contacts can view your info. But now that I’m typing in wondering how topics or products I’ve spoken about in conversation end up being advertised to me on Instagram…perhaps it is not as private as I thought".

P52 and **P83** are of the opinion that the uploaded data is stored as they have prescribed with the necessary public and private facing permissions. These participants have a good understanding of the basic privacy settings to manage who can see and access your uploaded content. However, **P83** concludes that they are equally uncertain that their data is safe and treated as per their prescripts. The uncertainty of the P83 is concerning.

P57 claims that “My information is used for heaven only knows. Honestly I don't know.”

P57 acknowledges that they have no idea what their data is used for and what happens with it. This sentiment is concerning as the participant should have a solid basic understanding.

P6 contends that “It gets dotted in the Cloud”. **P91** adds that, “It sits somewhere on a server. Have never really thought about specifics”.

P6 and P91 are positive that their data is uploaded online. The participants’ statements are inconclusive and neutral. This makes their opinions hard to understand. The participants have some semblance of social media data handling. However, the uncertainty exhibited by the participants is somewhat jarring, given that they can share sensitive information via the platforms.

P16 explains that “Every time someone uploads personal information on media platforms it’s not guaranteed that it’s safe from hackers even when there is a privacy statement in the terms and conditions section”.

P16 alludes that data uploaded to social media platforms are at risk of breach by malicious actors, thereby placing the social media user in harm's way. The participant exudes some data privacy awareness by remaining vigilant of threats from hackers.

P63 contends that "It gets sold to the CIA".

P63 deduces that the uploaded data is used by the Central Intelligence Agency (CIA) from the United States of America. The alleged subterfuge in the participant's response appears a little extreme. Whilst it is feasible that the CIA could obtain access to social media platforms for intelligence purposes, the various laws of countries would limit it to certain regions. The participant's response will be excluded from the study.

The participants' responses to survey question 18 are split between legitimate facts and several misconceptions. The raw facts serve as a testament to their privacy threat awareness level when interacting on a social media platform.

The Sankey diagram below in Figure 4-32 depicts the perception of the data uploaded to social media platforms at a more granular level. The researcher has drilled down to consider the mother-tongue languages of the participants.

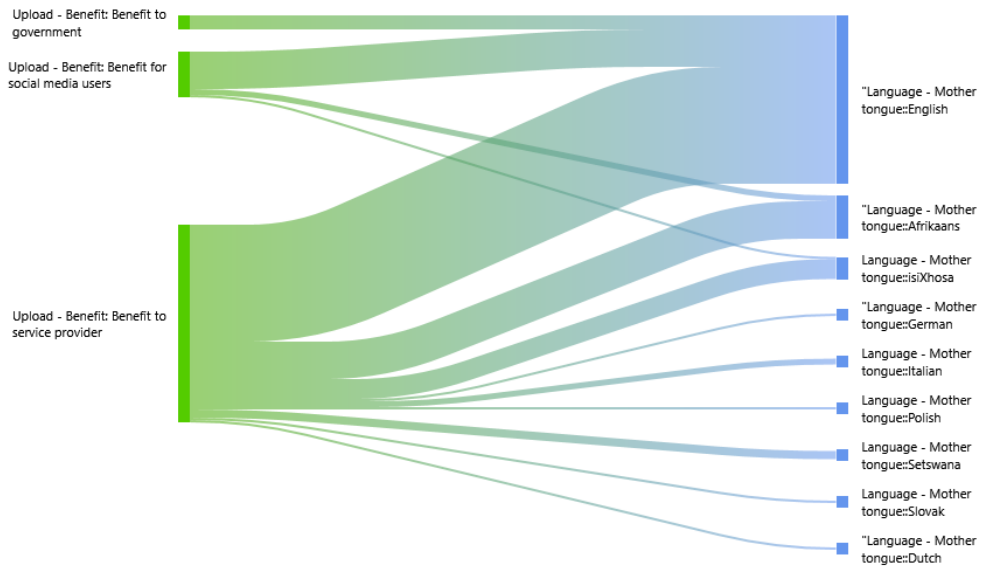


Figure 4-32: Code - Data upload benefit vs language (ATLAS.ti, 2024)

Figure 4-32 reinforces that most participants believe that social media platforms are the main beneficiaries of the uploaded data. This is evident with the broad and heavy line in the diagram denoting the participant's opinion swaying toward this fact.

Overall, English, Afrikaans and isiXhosa mother-tongue speakers account for the largest proportion of the participants in the study, as noted in Figure 4-32. Additionally, many English, Afrikaans and isiXhosa mother-tongue speakers agree with the statement, as mentioned earlier, that social media companies are the main beneficiaries of the uploaded content. There is, however, a split in opinion with a small contingent of English, Afrikaans and isiXhosa mother-tongue speakers of the opinion that the user is the primary beneficiary of the uploaded data. This fact is shown in the diagram by the slender line splitting from the respective mother-tongue speaker group to the social media users' benefit code. Lastly, some German, Italian, Polish, Setswana, Slovak and Dutch mother-tongue speakers identify the social media platform as the main beneficiary. The slender, delicate lines in Figure 4-32 confirm that these equate to a small number of participants.

The next survey question attempts to understand content ownership from the perspective of social media users to answer the perceived privacy threat awareness of participants. It is important to note that this question has been used to answer both SRQ1 and SRQ2. This is possible given the richness of the response and the identified codes linked to SRQ1 and SRQ2.

Survey Question 19: Who do you think owns the data that you upload?

Selection criterion:

Survey question 19 is selected to determine the privacy threat awareness of adult social media users when interacting on a social media platform. An open-ended question is posed to capture the rich, authentic responses of the participants to determine who they perceive as the owners of the uploaded data.

The participant's responses to the open-ended Survey Question 19 are numerous. Moreover, the core of some participant's responses is similar. Therefore, the quotations below will be limited to the most notable whilst displaying the various opinions.

P1 is of the opinion that "The social media platform". **P16** claims that "The social media platform will have your data after I have given consent they might share your data in other platforms". **P18** asserts that, "My assumption is that is that data is owned by the owners of the social media platform. I am not aware of who the actual owners of the platforms are". According to **P19,** "As soon as the data is uploaded as much as I want to believe it's owned by me, I signed it over to the company as soon as I accepted the T's & c's". **P91** states that "The platform owns the copies that I uploaded".

P1, P16, P18, P19 and **P91** report that the social media platform owns the uploaded data. The participants believe that social media platforms afford many rights to the data upon upload, and they can use the data for any means. Furthermore, some participants exhibit uncertainty regarding ownership of social media platforms. However, despite not knowing who the owners are, participants confirm that they continue to use the social media platforms.

P2 concludes that they are "The user". **P4** argues that "Photos- I own it. My personal info - probably the service provider. I really don't know". **P10** is of the opinion that "You own the data, however the social media platforms manages it. Anything unethical or x-rated the user of the social media will be blocked, taken off the platforms". According to **P73,** "You are the owner of the data however it can be used by anyone once shared or posted unless you specify differently."

P2, P4, P10 and **P73** conclude that the social media user is the owner of the uploaded data and controls how the data is used on the social media platforms. Subsequent to stating that they are the owner, **P4** resonates a little uncertainty with their “I really don’t know” assertion. **P10** adds that whilst the data belongs to the user, the social media platform has the power to moderate explicit data. **P73** contends that the data can be used by any other users after upload. The participant makes no mention of user controls to manage the data.

P20 states that “The internet owns the information as i have voluntarily uploaded it and since no one person or organization owns the internet then i am the owner of my own data”. **P36** argues that “Anyone if there is no disclaimer on it”.

P20 concludes that nobody owns the data and reinforces this idea by saying that ownership is vested with “The internet”. **P36** adds the caveat of a disclaimer but agrees that nobody owns the data. The participants’ statements are rather wide, contributing to notions that the data is available, can be used by anyone and has no data repurposing restrictions.

P49 states that they have “No clue”.

P49 surrenders and simply admits they do not know who or what owns the data. The participant also does not give any sense of restrictions to the data.

P63 reports that it is the “CIA”.

P63 is of the strong opinion that the Central Intelligence Agency (CIA) of the United States of America is the owner of the data. This is a strong opinion that is voiced by the participant. It is stated extremely concisely and provides no context.

Survey Question 20: What risk do you believe there is in using social media?

Selection criterion:

Survey question 20 is selected to determine the privacy threat awareness of adult social media users when interacting on a social media platform. The question uses a Likert scale to capture the authentic responses of the participants.

Figure 4-33: Code - Data risk perception
(ATLAS.ti, 2024)

The Sankey diagram in Figure 4-33 is generated using ATLAS.ti. Figure 4-33 shows that most participants favoured a data risk perception at the “High” level. The question provided five (5) response options, including “No risk”, “Low risk”, “Medium risk”, “High risk” and “Extreme risk”. As described in section 4.6.4.2, the researcher rationalised the codes in lieu of the closeness of their values into three (3) codes, namely: “Low”, “Medium”, and “High”. “No risk” and “Low risk” are coded as “Low” and “High risk” and “Extreme risk” are coded as “High”. Simplification of the codes from five (5) to three (3) allows for more efficient representation. The participants’ responses to survey questions are illustrated in Figure 4-33 and described in detail below.

P1, P2, P3, P5, P8, P9, P10, P11, P12, P13, P14, P15, P16, P18, P19, P22, P24, P26, P27, P28, P30, P32, P34, P35, P36, P37, P38, P41, P42, P43, P44, P50, P51, P54, P58, P59, P60,

P65, P66, P67, P70, P71, P73, P75, P79, P81, P82, P84, P86, P87, P88, P92, P93 and **P94** selected this "High" option accounting for 54 participants. This is demonstrative of the majority of participants being concerned about the risk they are confronted with. The Sankey diagram in Figure 4-33 relays these facts with a thick, heavy line.

P6, P7, P17, P20, P23, P25, P29, P31, P33, P39, P40, P45, P46, P47, P48, P49, P52, P53, P56, P57, P61, P62, P63, P64, P68, P69, P72, P74, P76, P77, P78, P80, P83, P85, P89, P90, P91 and **P95** selected a "Medium" level of data risk equalling 38 participants. This is confirmed in the Sankey diagram in Figure 4-33, where the line is less substantial than the "High" rating with the prominent line. This also constitutes a significant proportion of the participants.

Participants that toggled the low data risk option tallied to a total of three (3). This accounts for the minority that selected this option, as shown by the slender line in Figure 4-33. This included P4, P21 and P55.

The next survey question attempts to understand the importance of data privacy to social media users in answering the perceived privacy threat awareness of participants.

Survey Question 21: How important is data privacy to you?
Selection criterion: Survey question 21 is selected to determine the privacy threat awareness of adult social media users when interacting on a social media platform. The question uses a Likert scale to capture the authentic responses of the participants.

The Sankey diagram in Figure 4-34 is generated using ATLAS.ti. Figure 4-34 shows that most participants favoured a perception of data privacy importance at the "High" level. The question provided five (5) response options, including "Unimportant", "Low importance", "Medium importance", "High importance", and "Extreme importance". As described in section 4.6.4.2, the researcher rationalised the codes in lieu of the closeness of their values into three (3) codes, namely: "Low", "Medium", and "High". "Unimportant" and "Low importance" are coded as "Low", and "High importance" and "Extreme importance" are coded as "High". Simplification of the codes from five (5) to three (3) allows for more efficient representation. The participants' responses to survey questions are illustrated in Figure 4-34 and Figure 4-33, which are described in detail below.

P1, P3, P5, P6, P7, P8, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P25, P26, P28, P29, P30, P32, P35, P36, P37, P38, P39, P41, P42, P43, P44, P46, P47, P48, P50, P51, P52, P53, P54, P55, P57, P58, P59, P60, P62, P64, P65, P66, P68, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P84, P85, P86, P87, P88, P92, P93, P94 and **P95** unanimously selected the "High" option constituting 75 of the participants. This is confirmed in the Sankey diagram in Figure 4-34, where the line is the most prominent, and the "High" rating is validated with the thick, heavy line.

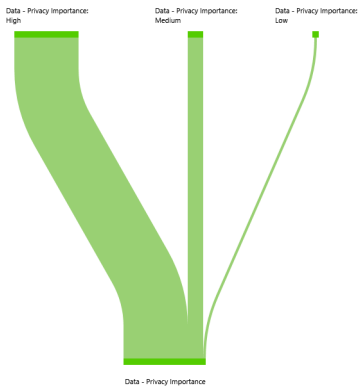


Figure 4-34: Code - Data privacy importance perception (ATLAS.ti, 2024)

17 participants, namely **P2, P15, P18, P27, P31, P34, P40, P45, P49, P56, P61, P63, P67, P69, P83, P90** and **P91** opted for a "Medium" level of data privacy importance. The line represented in the Sankey diagram in Figure 4-34 can be easily spotted but is significantly less than the "High" option.

This is in sharp contrast to the participants who felt that data privacy importance is a lower priority. This includes **P4, P33** and **P89**. The fact is acknowledged by the thin line in the Sankey diagram in Figure 4-34**.**

The next survey question further attempts to understand the importance of trust to social media users in answering the perceived privacy threat awareness of participants.

Survey Question 24: Is trust in the social media platforms you are registered with important to you?

Selection criterion:

Survey question 24 is selected to determine the privacy threat awareness of adult social media users when interacting on a social media platform. The question uses a Likert scale to capture the authentic responses of the participants.

The Sankey diagram in Figure 4-35 is generated using ATLAS.ti. Figure 4-35 shows that most participants opted for trust at the “High” level. The question provided five (5) response options, including “Unimportant”, “Low importance”, “Medium importance”, “High importance”, and “Extreme importance”. As described in section 4.6.4.2, the researcher rationalised the codes in lieu of the closeness of their values into three (3) codes, namely: “Low”, “Medium”, and “High”. “Unimportant” and “Low importance” are coded as “Low”, and “High importance” and “Extreme importance” are coded as “High”. Simplification of the codes from five (5) to three (3) allows for more efficient representation. The participants’ responses to survey questions are illustrated in Figure 4-35 and described in detail below.

Figure 4-35: Code - Data Trust Perception
(ATLAS.ti, 2024)

The Sankey diagram in Figure 4-35 shows that most participants selected data trust perception at the “High” level. **P2, P3, P5, P6, P7, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P26, P27, P30, P32, P34, P35, P37, P38, P39, P40, P41, P42, P43, P44, P45, P50, P51, P52, P53, P54, P57, P58, P60, P61, P62, P64, P65, P66, P68, P71, P72, P74, P75, P76, P77, P79, P81, P82, P83, P87, P88, P90, P92** and **P93** selected this option making up 63 of the participants. This is confirmed in the Sankey diagram in Figure

4-35**,** where the line is the most prominent, and the “High” rating is confirmed with the thick, heavy line.

28 participants, namely: **P1, P8, P15, P18, P25, P28, P29, P31, P33, P36, P46, P47, P48, P49, P59, P63, P67, P69, P70, P73, P78, P80, P84, P85, P86, P91, P94** and **P95** opted for a “Medium” level of trust reflected by the notable line in the Sankey diagram in Figure 4-35.

This is in sharp contrast to the participants who felt the trust was low. This included **P4, P55, P56 and P89**. The line in the Sankey diagram is slender, denoting that this is made up of four (4) participants.

The above-mentioned survey questions were selected to determine the privacy threat awareness level of adult social media users when interacting on a social media platform. The findings are formulated using the results from the privacy threat awareness level of adult social media users when interacting on a social media platform. The findings are presented hereunder.

Finding 5: The majority of the participants believe that the social media platform is the primary benefactor of the data uploaded where they can target marketing and monitor user activity to make social media feed recommendations. Moreover, the participants are of the opinion that the social media platform can do anything they please with the uploaded data, including sharing with and selling to third parties.

Finding 6: The participants stated that the social media platforms are the owners of the uploaded data.

Finding 7: Most of the participants attribute the highest level of risk to using a social media platform.

Finding 8: Participants predominantly consider data privacy to be of the highest importance when utilising a social media platform.

Finding 9: The participants contend that trust in a social media platform is critical. Therefore, they selected the highest level of trust when asked the question.

In summary, numerous participants are of the opinion that social media platforms have all the power. They are believed to own the uploaded data and have complete autonomy to use the uploaded data for any means they deem appropriate. Additionally, most of the participants

revealed that they consider risk, trust, and data privacy to be their top priority and attribute the highest rating levels against it.

4.7.3 Research objective 3

Research Objective 3: To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

SRQ3: What are the behavioural barriers to privacy management implementation for adult social media users?

Survey Question 29: Have the social media accounts of anyone you know been breached or hacked?

Selection criterion:

Survey question 29 is selected to determine the behaviour of adult social media users when interacting on a social media platform. The question uses a Likert scale to capture the authentic responses of the participants.

The Sankey diagram in Figure 4-36 clearly depicts that a total of 79 out of 95 study participants answered “Yes” when prompted with the aforementioned survey question. This is denoted by the broad red line that dominates Figure 4-36. This entailed **P1, P2, P3, P4, P6, P7, P8, P9, P10, P11, P12, P13, P15, P16, P19, P20, P22, P23, P24, P25, P26, P27, P28, P29, P31, P32, P33, P34, P35, P36, P38, P40, P41, P42, P43, P44, P47, P48, P49, P50, P51, P52, P53, P56, P57, P58, P59, P60, P62, P63, P65, P66, P67, P68, P69, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P83, P86, P87, P88, P89, P90, P91, P92, P93, P94** and **P95.** This fact is remarkable in conveying that so many participants are aware of other people who have experienced breaches, and it reinforces the fact that this is a persistent problem.

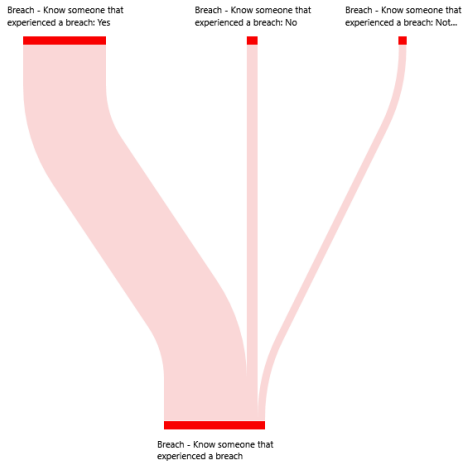


Figure 4-36: Know someone who experienced a breach (ATLAS.ti, 2024)

Very few participants submitted “Not sure” and “No” responses. Seven (7) participants selected the “Not sure” option, reflected by the slender line in the Sankey diagram in Figure 4-36. This is constituted from **P17, P21, P30, P37, P39, P55** and **P85**. Similarly, the participants that responded “No” totalled ten (10), which is also shown as a slender line in Figure 4-36. The fact is concerning and demonstrates the scale of the problem.

The next survey question further attempts to understand the importance of the behavioural barriers to privacy management of social media users to answer the overall behaviour of participants.

Survey Question 30: Has any of your social media accounts been breached or hacked? Survey Question 31: If so, how many times has your social media account been breached or hacked?
<u>Selection criterion</u>: Survey questions 30 and 31 are selected to determine the behaviour of adult social media users when interacting on a social media platform. The question uses a Likert scale to capture the authentic responses of the participants.

A total of 12 out of 95 study participants, or 12,63% of the study sample, answered “Yes” to survey question 30. This includes **P8, P20, P33, P40, P60, P67, P83, P86, P88, P90, P92** and **P93**. Although this constitutes the minority, it is interesting that 24 of the 95 participants cannot state with certainty whether they have experienced a breach. The fact that breaches still persist despite a wealth of knowledge affirms that this remains a problem.

24 participants responded “Not sure”, and 59 participants who responded “No”. **P3, P4, P10, P11, P13, P16, P17, P19, P29, P30, P31, P32, P34, P38, P42, P47, P55, P57, P66, P72, P74, P76, P80** and **P89** submitted “Not sure”. These participants could neither say that they had or had not experienced breaches. **P1, P2, P5, P6, P7, P9, P12, P14, P15, P18, P21, P22, P23, P24, P25, P26, P27, P28, P35, P36, P37, P39, P41, P43, P44, P45, P46, P48, P49, P50, P51, P52, P53, P54, P56, P58, P59, P61, P62, P63, P64, P65, P68, P69, P70, P71, P73, P75, P77, P78, P79, P81, P82, P84, P85, P87, P91, P94** and **P95** acknowledged that they had not experienced a breach. This is representative of most participants. However, it is concerning that many participants are unsure or have fallen prey to breaches. Lastly, 12 out of 12 participants admitted that their accounts were only breached once.

The next survey question considers how a personal breach and the behavioural barriers to privacy management of social media users cast an overall view of the behaviour of participants.

Survey Question 32: If so, how has the breach or hack affected your data privacy management practices?

Selection criterion:

Survey question 32 is selected to determine the behaviour of adult social media users when interacting on a social media platform. An open-ended question is posed to capture the rich, authentic responses of the participants.

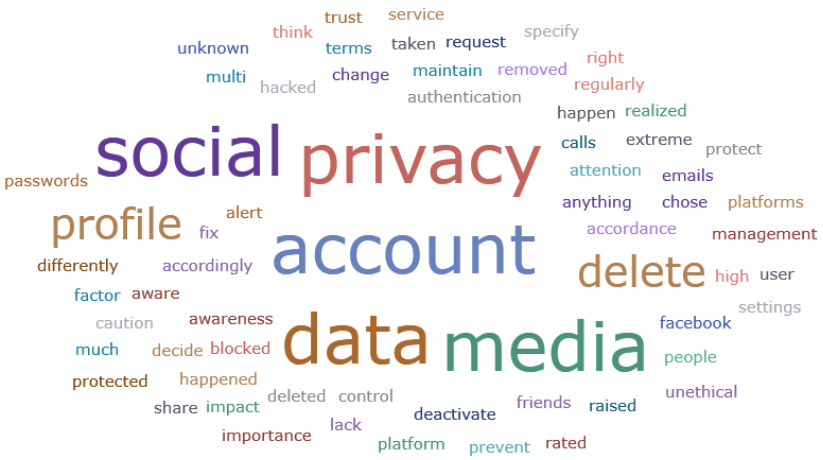


Figure 4-37: Theme 3: Behaviour word cloud (ATLAS.ti, 2024)

The ATLAS.ti generated word cloud in Figure 4-37 for the “Breach Attitude” and “Breach Behaviour” codes resonate with the sentiments of the 12 affected participants. The most notable sentiments in the word cloud pertained to “social”, “media”, “data”, “privacy”, and “account”, confirming that participants are seriously concerned about this. The next layer of the participants’ concern pertains to “profile” and “delete”. The aforementioned areas of concern for participants speak to the “Breach Attitude” and “Breach Behaviour” aspects.

The “Breach Attitude” and “Breach Behaviour” aspects illustrated in Figure 4-38, Table 4-9 and Table 4-10 are discussed further below.

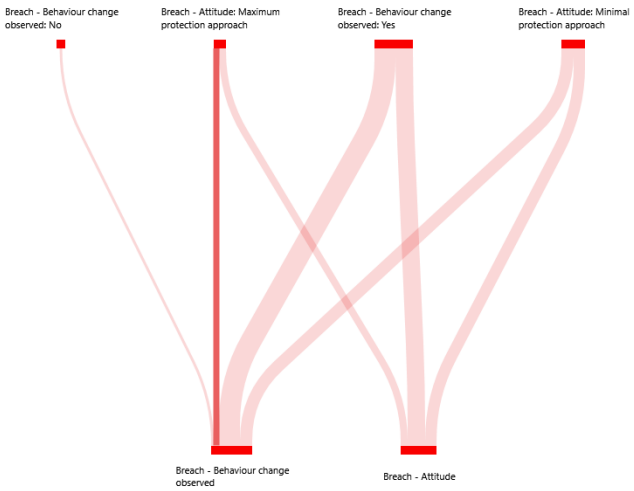


Figure 4-38: Breach attitude and behaviour (ATLAS.ti., 2024)

The Sankey diagram in Figure 4-38 illustrates the “Breach Attitude” and “Breach Behaviour” codes in combination. Table 4-9 and Table 4-10 support the Figure 4-38 by providing the details. These are responses from the 12 participants who experienced breaches on their social media accounts at least once. The affected participants are **P8, P20, P33, P40, P60, P67, P83, P86, P88, P90, P92** and **P93**.

Table 4-9: Breach attitude (ATLAS.ti., 2024)

	Participant 8	Participant 20	Participant 33	Participant 40	Participant 60	Participant 67	Participant 83	Participant 86	Participant 88	Participant 90	Participant 92	Participant 93
• **Breach - Attitude: Minimal protection approach** Gr=8		Minimum Approach			Minimum Approach			Minimum Approach	Minimum Approach	Minimum Approach	Minimum Approach	
• **Breach - Attitude: Maximum protection approach** Gr=4	Maximum Approach											

Table 4-10: Breach behaviour (ATLAS.ti., 2024)

	Participant 8	Participant 20	Participant 33	Participant 40	Participant 60	Participant 67	Participant 83	Participant 86	Participant 88	Participant 90	Participant 92	Participant 93
• **Breach - Behaviour change observed: No** Gr=2			No	No								
• **Breach - Behaviour change observed: Yes** Gr=13	Yes	Yes			Yes			Yes	Yes	Yes	Yes	

There is a notable shift in the participants’ “Breach Behaviour” after the breach, demonstrated by the thick red line gravitating to behaviour change. Participants **P8, P20, P60, P86, P88, P90** and **P92** changed their social media platform behaviour after experiencing a breach of their account. **P33** and **P40** did not change their behaviour, and P67, P83, and P93 provided responses that indicated no behavioural change.

Moreover, a shift in “Breach Attitude” is noted for the affected participants, who have adopted a minimal protection adjustment to their security practices. This is illustrated with the heavy red line in “Breach – Attitude: Minimal protection approach” in Figure 4-38. **P20, P60, P86, P88, P90** and **P92** selected a minimal protection approach, whereas **P8** selected a maximum protection approach. **P33, P40, P67, P83** and **P93** provided responses that offer no indication of attitude change.

The Sankey diagram in Figure 4-39 hereunder depicts the “Breach Attitude” and “Breach Behaviour” against ATLAS.ti Smart Groups composed of Mother-tongue, Age and Gender to

obtain a deeper perspective of the raw data. The group of participants affected predominantly consisted of seven (7) English speakers, two (2) Afrikaans speakers, and two (2) isiXhosa mother-tongue speakers. One (1) Italian mother-tongue speaker has been excluded from Figure 4-39. No participants speaking other languages were affected.

Additionally, this cohort consisted of seven (7) males and five (5) females. In general, a total of six (6) participants do not have post-senior secondary education and constitute a minute portion of the sample. Additionally, 68 of the participants spent their childhood years in Cape Town, and the data does not demonstrate any clear patterns. Therefore, the education and childhood levels have been excluded from the representation hereunder in these results.

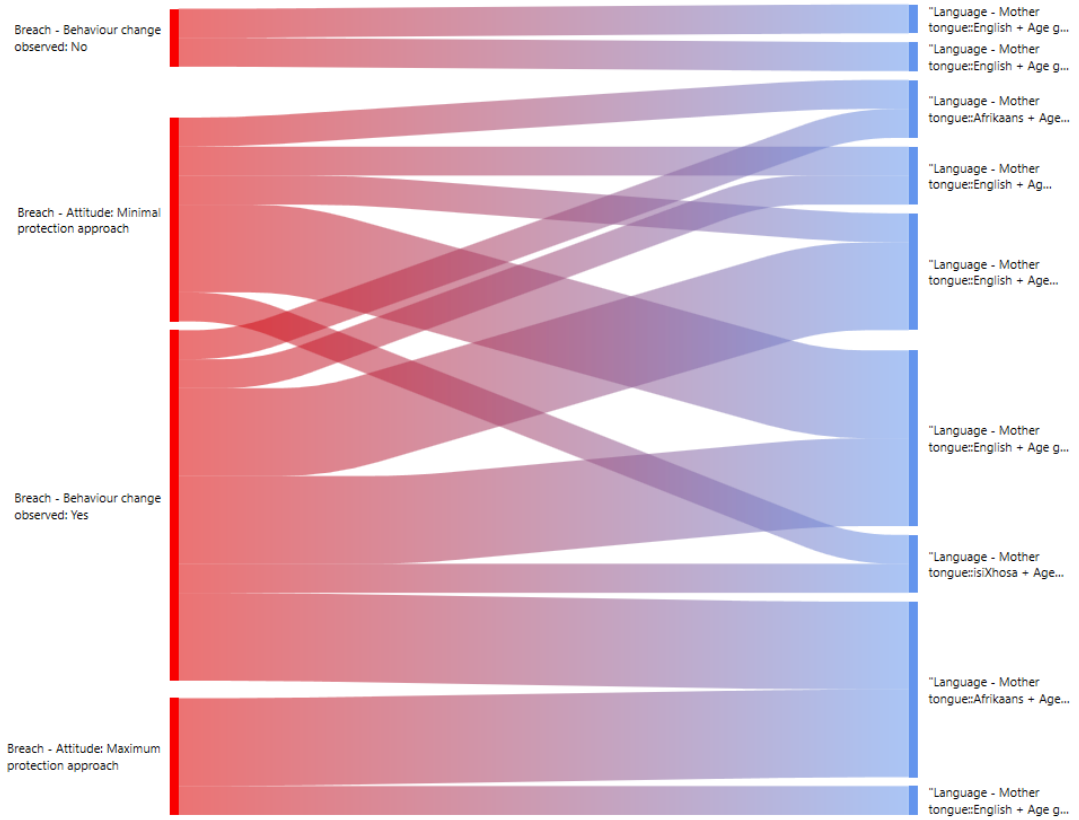


Figure 4-39: Breach attitude and behaviour with Smart Groups (ATLAS.ti., 2024)

Interestingly, despite their account breaches, no breach behaviour change was observed for one 51-55 and one 56-60-year-old English-speaking male. Furthermore, three (3) 26-30-year-old males observed a breach behaviour change and opted for maximum protection. No other groupings opted for maximum protection. The broad, heavy red lines depict the responses of the participants favouring the respective options. Figure 4-39 confirms the results presented above. It is important to note that the results of this study are not generalisable as the sample

is extremely small. It does, however, provide a clear impression of the findings resonating in the study.

The above-mentioned survey questions were selected to determine the behaviour of adult social media users when interacting on a social media platform. The findings are formulated using the results from the behaviour of adult social media users when interacting on a social media platform. The findings are presented hereunder.

Finding 10: The survey question on whether participants knew someone who experienced a breach revealed that it still poses a problem today. This is reaffirmed by the breaches several participants experienced.

Finding 11: Participants value their data privacy on social media platforms.

Finding 12: Many of the affected participants changed their data privacy management behaviour on social media platforms.

Finding 13: Predominantly, participants selected the minimal data privacy protections to safeguard themselves.

In summary, several participants experienced breaches of their social media accounts. Overall, the consequence of the breach appears to have impacted them positively in that most of them have changed their online behaviour. Numerous participants selected minimal protections to safeguard their online data presence.

4.8 Conclusion

The study is a mono-qualitative interpretivist study that explores the phenomenon of data privacy management behaviour of adult social media users in South Africa. The research problem relates to social computing and human-computer interaction (HCI) within the Information and Communication Technology (ICT) sector. Several studies have been conducted on this problem globally. However, very few studies have been conducted in the South African context.

According to Statistics South Africa (2024), the South African population amounted to 62,027,503 people in the census conducted in 2022. The report adds that the general population is comprised of diverse groups and unique communities speaking a multitude of languages throughout South Africa. Furthermore, the population is comprised of groups from

diverse cultural and socio-economic backgrounds (Statistics South Africa, 2024). Kemp (2024) estimates the South African social media user population at around twenty-six (26) million users as of January 2024. In light of these facts, the researcher believes that it is prudent to better understand the data privacy management behaviour of adult social media users in South Africa. The purpose of this chapter is to present the raw data.

The researcher employed a survey administered through Google Forms to collect the responses to answer the following questions:

RQ: What is the data privacy management behaviour of adult social media users?

> **SRQ1:** How do adult social media users manage their privacy when interacting on a social media platform?
>
> **SRQ2:** What is the perceived privacy threat awareness level of adult social media users?
>
> **SRQ3:** What are the behavioural barriers to privacy management implementation for adult social media users?

Participants were invited by the researcher via social media platforms and electronic mail. The Google Forms survey employed by the researcher garnered two rounds of responses comprised of 73 and 22 participants, respectively. The survey was limited to participants 18 years and older. No participants under the age of 18 were allowed to participate due to the legal and ethical affordances necessary to participate. The survey solicited responses from a diverse group of participants ranging in age from 18 to over 60 and differing backgrounds. The researcher ensured that participants provided consent to participate in the study. Furthermore, the researcher ensured conformance to the ethical prescripts of the study to ensure that participants were protected and that they could withdraw from the study at any time.

The study will use Communication Privacy Management (CPM) and the Theory of Planned Behaviour (TPB) in combination as the lens through which to view the participants' data privacy management behaviour. The study intends to consider the social and cultural influences of the participants to reveal any meaningful observations for their data privacy management behaviour.

The researcher opted for a simplified thematic analysis model whilst ensuring conformance to the broad steps and principles of the approach. It includes the following steps to analyse the

data: 1. Start preparations for data analysis, 2. Consider all data, 3. Codify all data, 4. Create themes, and 5. Devise a means to represent the themes. The findings are organised under the three themes that emerged from the analysis, namely: 1. Data privacy management, 2. Social media utilisation and threat perception, and 3. Behaviour outlined in Figure 4-40.

Figure 4-40: Findings (Adapted from Analysis section, 2024)

It must be noted that the survey data collected electronically using Google Forms produced a sizable repository of data, and it is not feasible to present each piece of data in this Results chapter. The researcher selected the most notable items for presentation in the analysis section, resulting in a total of 13 findings. A prioritisation logic, described at length throughout section 4.7 above, was applied to carefully select rich and complex responses.

The raw data from the survey was imported into ATLAS.ti for this interpretivist qualitative study. The researcher painstakingly read and re-read the raw data to formulate codes that were representative of the participants' responses. It was necessary to revisit the raw data and codes in subsequent coding passes to refine and ensure efficiency in the codes. Categories were formed from the codes to drive further improvements, ultimately leading to the formulation of themes. The themes, as mentioned earlier, were formed from the codes and categories identified in the participants' responses. There is a direct linkage between the research questions, objectives of the study and the respective themes, as illustrated in Table 4-11.

Table 4-11: Research questions and theme linkages

Nature	Research Questions	Research Objectives	Theme
Aim	The aim of the study is to determine the **data privacy behaviour** of adult **users of social media** residing in South Africa whilst interacting on the social media platforms.		
Main **RQ**	What is the **data privacy** management **behaviour** of adult **social media users**?		
Sub RQ1	How do adult **social media users** manage their **privacy** when interacting on a **social media** platform?	To explore the **privacy** management methods and techniques employed by adult **users of social media** residing in South Africa to manage their privacy when interacting on a **social media** platform.	**Theme 1:** Data privacy management
Sub RQ2	What is the perceived **privacy** threat awareness level of adult **social media users**?	To determine the data **privacy** threat perception of adult **social media users** residing in South Africa.	**Theme 2:** Social media utilisation and threat perception
Sub RQ3	What are the **behavioural barriers** to **privacy** management implementation for adult **social media users**?	To identify **behavioural barriers** to data **privacy** management implementation of adult **social media users** residing in South Africa.	**Theme 3:** Behaviour

Theme 1: Data privacy management

The first theme consists of the categories relating to the data privacy management aspects of uploaded data, incentivised permission for platforms to use the uploaded data, the importance of privacy, platform trust perception, risk of platform use, data protection and the beneficiary of uploaded data. These categories provide a view of the participants' data privacy management and outlook.

Theme 2: Social media utilisation and threat perception

The second theme pertains to the categories relating to social media utilisation and threat perception of ownership of uploaded data, registration reason, usage reason and understanding of the terms of service. These categories provide a view of the participants' perception of threats to social media utilisation.

Theme 3: Behaviour

The third theme consists of categories relating to social media user behaviour, such as breach awareness, breach attitude, breach behaviour, and personal experience. These categories provide a view of the participants' behaviour on social media platforms.

The presented raw data is intentionally devoid of interpretation, as this will be covered in Chapter Five: Discussion. The researcher will interpret the results of this mono-qualitative interpretivist study to reveal the patterns and meaning.

CHAPTER 5: DISCUSSION

5.1 Introduction

The chapter is organised into six (6) sections. Section One (1) provides the introduction to the study. The research objectives and synopsis are provided as a quick reference to the reader in Sections Two (2) and Three (3), respectively. Section Four (4) explains the application of the selected theories, whilst Section Five (5) delves into the respective sub-research questions and findings. Section Six (6) delivers the conclusion for this chapter. The study's title, aim, objectives, research question and sub-research questions are illustrated in Figure 5-1 below for easy reference.

Figure 5-1: Problem statement (Adapted from research proposal, 2022)

The purpose of this Chapter is to conduct and present the interpretation of the analysis performed in Chapter 4. The results are reflective of the subjective opinions of the participants. The findings and themes emanating from the data analysis will be focused on to reveal the meaning of this study. In Chapter 4, the researcher revealed three (3) themes and thirteen (13) findings as part of the analysis. The three (3) themes are represented in Table 5-1 and are linked to the respective objectives and sub-research questions. The respective themes will be outlined hereunder.

Table 5-1: Research questions and theme linkages

Nature	Research Questions	Research Objectives	Theme
Aim	The aim of the study is to determine the **data privacy behaviour** of adult **users of social media** residing in South Africa whilst interacting on the social media platforms.		
Main **RQ**	What is the **data privacy** management **behaviour** of adult **social media users**?		
Sub RQ1	How do adult **social media users** manage their **privacy** when interacting on a **social media** platform?	To explore the **privacy** management methods and techniques employed by adult **users of social media** residing in South Africa to manage their privacy when interacting on a **social media** platform.	**Theme 1:** Data privacy management
Sub RQ2	What is the perceived **privacy** threat awareness level of adult **social media users**?	To determine the data **privacy** threat perception of adult **social media users** residing in South Africa.	**Theme 2:** Social media utilisation and threat perception
Sub RQ3	What are the **behavioural barriers** to **privacy** management implementation for adult **social media users**?	To identify **behavioural barriers** to data **privacy** management implementation of adult **social media users** residing in South Africa.	**Theme 3:** Behaviour

Theme 1: Data privacy management in Table 5-1 consists of the categories relating to the data privacy management aspects of uploaded data, incentivised permission for platforms to use the uploaded data, the importance of privacy, platform trust perception, risk of platform use, data protection and the beneficiary of uploaded data. These categories provide a view of the participants' data privacy management and link to objective 1 and sub-research question 1.

Theme 2: Social media utilisation and threat perception in Table 5-1 pertains to the categories relating to the social media utilisation and threat perception of ownership of uploaded data,

registration reason, usage reason and understanding of the terms of service. These categories provide a view of the participants' threat perception of social media utilisation and link to objective 2 and sub-research question 2.

Theme 3: Behaviour in Table 5-1 encompasses the categories relating to social media user behaviour through breach awareness, breach attitude, breach behaviour and personal experience. These categories provide a view of the participants' behaviour on social media platforms and link to objective 3 and sub-research question 3.

Figure 5-3 below depicts the 13 findings organised under the three themes that emerged from the analysis, namely: 1. Data privacy management, 2. Social media utilisation and threat perception, and 3. Behaviour. The findings will be discussed in detail in section 5.5

5.2 Research objectives

The research aim and objectives are provided as a reminder and to orientate the interpretation discussion of the study. It is crucial to focus on the interpretation to ensure that the themes or patterns are revealed to further the understanding of the research problem.

5.2.1 Aim

The study aims to determine the data privacy behaviour of adult users of social media residing in South Africa whilst interacting on social media platforms. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

5.2.2 Objective

1. To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.
2. To determine the data privacy threat perception of adult social media users residing in South Africa.
3. To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

5.3 Research synopsis

The study is exploratory in nature, where the researcher will explore through survey questionnaires how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy.

Bandara et al. (2021) acknowledge that the behaviour of social computing users regarding online data privacy is not well documented. Al-Rabeeah and Saeed (2017) and Petronio and Child (2020) contend that the Communication Privacy Management (CPM) and Theory of Planned Behaviour (TPB) pertain to privacy decisions influenced by the user's cultural influences. McNealy and Mullis (2019:111) add that research involving CPM in the "social media context" is sparse and deserves attention.

The researcher intends to use embedded culture and beliefs as a lens to improve the understanding of users' behaviour. The research question and sub-research questions address the identified research problem in the study. The primary purpose of the research is to explore the data privacy management behaviours exhibited by adult social media users residing in South Africa. Furthermore, the research question seeks to understand whether the culture of social media users influences their privacy management behaviour. The research question and sub-research questions are provided below for ease of reference.

RQ: What is the data privacy management behaviour of adult social media users?

> **SRQ1:** How do adult social media users manage their privacy when interacting on a social media platform?
>
> **SRQ2:** What is the perceived privacy threat awareness level of adult social media users?
>
> **SRQ3:** What are the behavioural barriers to privacy management implementation for adult social media users?

Study essentials demand that the study be considered against an established theory. The selected theory is briefly discussed to remind the reader how the study will be interpreted.

5.4 Theory

Al-Rabeeah and Saeed (2017), Petronio and Child (2020) and Bandara et al. (2021) assert that privacy can be affected when a person initiates a privacy breach or when someone else initiates a privacy breach. The authors contend that it can be difficult to stop the latter scenario as the affected person would need to resort to legal action (Al-Rabeeah & Saeed, 2017).

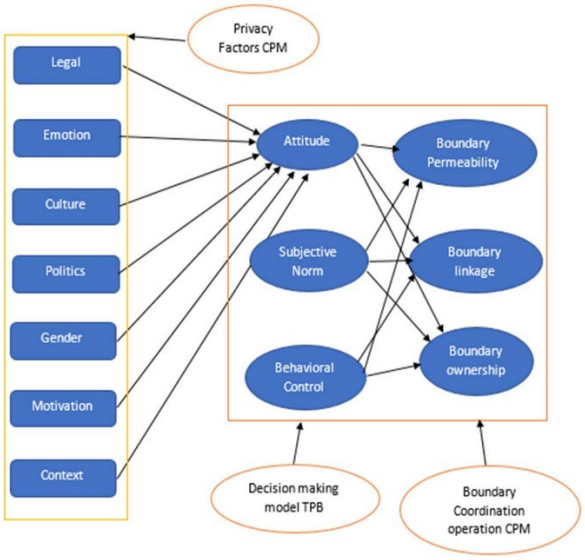


Figure 5-2: Combined model between CPM & TPB theories (Al-Rabeeah and Saeed, 2017)

Petronio and Child (2020:76) state that in Communication Privacy Management (CPM) theory, people own their data and have the freedom to share or not share their data via “privacy boundaries”. Al-Rabeeah and Saeed (2017) and Kasim et al. (2021) conclude that the privacy management behaviour of users can be pre-empted by applying the Theory of Planned Behaviour (TPB). Al-Rabeeah and Saeed (2017) propose a data privacy model consisting of an amalgam of CPM and TPB, illustrated in Table 5-2 and Figure 5-2, that can be used to rigorously scrutinise data privacy management behaviour.

Table 5-2: Components of combined CPM and TPB theories

COMBINED COMPONENTS	DECISION-MAKING MODEL TPB:	BOUNDARY COORDINATION OPERATION CPM:
• Legal • Emotion • Culture • Politics • Gender • Motivation • Context	• Attitude • Subjective norm • Behavioural control	• Boundary permeability • Boundary linkage • Boundary ownership

CPM and TPB have been used independently in previous ICT studies, notably in the IEEE Explore and the International Journal of Advanced Computer Science and Applications. The researcher employs the Al-Rabeeah and Saeed (2017)Al-Rabeeah and Saeed (2017) combined theory model as the theoretical lens for the study to reveal a deeper meaning. The researcher will attempt to differentiate this qualitative study from similar studies by considering the components listed below within the research study's context.

Petronio and Child (2020:77) explain that people use "privacy rules" to determine their privacy choices. The authors conclude that the cultural influences of people inform the logic that drives their privacy choices, with most situations having a consistent application of privacy choices (Petronio & Child, 2020). Petronio and Child (2020) add that volatile situations, stress or shock may result in erratic privacy choices as the situation, instead of the person's privacy rules, determines the decisions. The components of the combined CPM and TPB theories model in Table 5-2 against the study's research objectives will be discussed for each sub-research question and linked theme in the next section, 5.5.

5.5 Discussion

The study is exploratory in nature, where the researcher will explore through survey questionnaires how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy. The research problem relates to social computing and human-computer interaction (HCI) within the Information and Communication Technology (ICT) sector, and the proposed study envisages

detecting meaningful data privacy attitudes for adult social media users residing in South Africa. The prevailing themes, categories and codes from the data analysis are presented for interpretation against the respective research objective and theme to answer the research questions. Figure 5-3 below provides a holistic view of the researcher's approach to the data analysis. An interpretation of the analysis is necessary to answer the research question and sub-research questions listed in section 5.3.

Figure 5-3: Findings (Adapted from Analysis section, 2024)

The components of the Al-Rabeeah and Saeed (2017) combined CPM and TPB theories model in Figure 5-2 will be used independently for the interpretation discussion. These items will be discussed in more detail in the next sections in relation to the respective sub-research questions.

5.5.1 Research objective 1

Research Objective 1: To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.

SRQ1: How do adult social media users manage their privacy when interacting on a social media platform?

Sub-research question 1 (SRQ1) explores the privacy management methods and techniques of adult social media users in South Africa. The main idea revolves around fully appreciating how the users use social media, what their beliefs are and how they interact on the social media platforms from a data privacy management perspective. Categories informing Theme 1 provide a view of the participants' data privacy management. Additionally, Theme 1 is linked to objective 1 and sub-research question 1.

Al-Rabeeah and Saeed (2017) and Bandara et al. (2021) view social media utilisation as problematic, given the potential for users to place themselves in harm's way or unwittingly fall prey to malicious attacks. Therefore, the researcher will attempt to better grasp the interactions of social media users by applying the Al-Rabeeah and Saeed (2017) combined CPM and TPB theory model against the SRQ1. This is presented under the respective combined CPM and TPB components below.

Legal

Al-Rabeeah and Saeed (2017) describe the legal framework afforded to data owners and data guardians as the protection mechanism for data privacy. South Africa (2020) states that the Protection of Personal Information Act 4 of 2013 affords data privacy owners with the necessary legal instruments to protect their personal information. Furthermore, all social media platforms are obligated to provide their Terms of Service and Privacy Policy to inform users of the rights and protections afforded to them when using the social media platform. The literature review in section 2.6 evaluates the content of the Terms of Service and Privacy

Policy for Facebook, X, Instagram, TikTok, WeChat, Snapchat, LinkedIn, YouTube, WhatsApp and Telegram. Strava and Botim are two other social media platforms that were noted in the participants' responses and evaluated in section 2.6.

P2, P3, P4, P13, P18, P23, P25, P27, P30, P31, P32, P33, P36, P37, P43, P45, P47, P49, P52, P55, P56, P57, P59, P60, P61, P62, P66, P68, P71, P72, P74, P81, P82, P83, P84, P88, P89 and **P95** did not read the social media platform's Terms of Service at all. Moreover, **P1, P5, P6, P10, P11, P12, P14, P15, P16, P17, P19, P20, P22, P24, P26, P28, P29, P34, P35, P38, P39, P40, P41, P42, P46, P48, P50, P51, P54, P58, P63, P65, P67, P69, P70, P73, P75, P76, P77, P78, P79, P80, P85, P86, P87, P90, P91, P92, P93** and **P94** partly read the social media platforms' Terms of Service. This sharply contrasts with the sentiments observed in the study. Lastly, seven (7) participants, P7, P8, P9, P21, P44, P53 and P64, stated that they read the social platforms' Terms of Service in full.

However, when the sentiments mentioned earlier are compared to the social media Terms of Service facts presented in section 2.6, this is highly contradictory to most participants' responses. It is abundantly clear that most of the participants who indicated that they partly and wholly read the Terms of Service are incorrect when they state that the social media platform owns and solely benefits from the upload of users' data (Finding 1). Finding 1 agrees with the belief of Obar and Oeldorf-Hirsch (2022) that more than 75% of individuals over the age of 50 years are inclined to ignore the Terms of Service. This also holds true for users who spend less than an average of one (1) minute on the Terms of Service (Obar & Oeldorf-Hirsch, 2022). Yerby and Vaughn (2022) believe that the social media platform's Terms of Service are verbose and aim to obfuscate the information for the reader. The latter statement aligns well with Finding 1. Finding 1 is comprised of a mix of users accepting the Terms of Service without reading or reading approximately one (1) minute and accepting the conditions. It appears to be a universal sentiment that cuts across all age groups, languages, and cultures when dealing with legal documents. This speaks to the format, length and complex language of the legal instruments. Frustratingly, many of the Terms of Service are only available in English, leaving every non-English mother-tongue speaker at a significant disadvantage and more predisposed to ignorance. Additionally, in a fast-paced world, the textual format requires a lot more time to ingest. Therefore, an alternate medium like a short format video, infographic or audio would open chances of conveying the basic facts.

Finding 1 conveys that a small group of seven (7) participants read the Terms of Service in full. The group is limited to English and Afrikaans mother-tongue speakers. Additionally, the

18-25, 36-40, 56-60 and 61 and above age groups are not represented in this group. Lastly, the group consists of females in the 46-50 and 51-55 age groups and males in the 26-30, 31-35, 41-45 and 51-55 age groups. Finding 1 presents an unexpected finding where several age groups above 50 years of age indicated that they read the Terms of Service in full or in part. Participants in this cohort account for three (3) who read in full and 13 that partly read. Obar and Oeldorf-Hirsch (2022) state that more than 75% of individuals over the age of 50 years are inclined to ignore the Terms of Service. The 16 participants who read the Terms of Service, in full and in part, account for 72 per cent of the participants over the age of 50 years. This finding completely upends the findings of Obar and Oeldorf-Hirsch (2022).

The sentiments expressed in Finding 2 relay that the participants value their data privacy and believe their data is important. However, 53 per cent of the users are concerned about their uploaded information, content, and data but do not read the Terms of Service to understand the implications. Bandara et al. (2021), Chen et al. (2021), and Arzoglou et al. (2023) explain the privacy paradox where users exhibit erratic behaviour when managing their social media data privacy. The authors state that the erratic privacy practice is attributed to dissimilarities in demography, technical aptitude, general usage and the need for social recognition (Bandara et al., 2021). Interestingly, the gender count is quite even, and most languages are represented in the group. Moreover, several communities are reflected.

Findings 1 and 2 in Table 5-3 are linked to the legal component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-3 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-3: Finding for Legal component

FINDING	CATEGORY	THEME
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust	• Data privacy management
Finding 2:		

FINDING	CATEGORY	THEME
Most participants express heightened concern over their information, content and data on social media platforms.	• Risk • Data protection • Upload	

In summary, **Findings 1 and 2** are viewed through the legal component of the combined CPM and TPB theory model. The legal instruments available to the public include the Protection of Personal Information Act 4 of 2013 of South Africa and the Terms of Service and Privacy Policy of the social media platforms. There appears to be an aversion to reading the Terms of Service of social media platforms that resonates amongst the participants. Terms of Service are technically worded legal instruments that are typically difficult to comprehend. They are also lengthy textual documents. Consideration of alternate media like short format video, infographic or audio clips could be better suited to relay this critical information that seems to be misunderstood. The affected mother-tongue speakers and age groups are discussed in detail above. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Emotion

According to Petronio and Child (2020), the issues of emotion are essential to CPM, especially the impact on judgment. However, the area of emotion is currently a gap in CPM that must be addressed. The authors contend that emotion is time- and place-sensitive as it can only be observed when the emotions are expressed. Simulation is cited as the only feasible method of replicating emotion, reliving the feeling experienced, and recording is authentically observed in real time (Petronio & Child, 2020). Al-Rabeeah and Saeed (2017) note that emotion is key to understanding privacy behaviour. The authors contend that emotion has the potential to manifest unique privacy behaviour due to the nuances in personality between every individual (Al-Rabeeah & Saeed, 2017).

Emotion is difficult to discern in the participants' responses to the survey. However, Figure 4-31 uses a word cloud to represent the sentiments noted for survey question 19. The image mentioned earlier presents the participants' primary concern as "information" for their data privacy. Additionally, the words "use", "services", "content", "account", "high", "importance", "friend", "data", and "password" are presented as the secondary layer of concern. The

concerns expressed by the participants convey a glimmer of emotion for their data privacy management **(Finding 2)**.

Finding 2 is linked to the emotion aspect of the combined CPM and TPB theory model. The finding is tied to Theme 1: Data privacy management and the associated categories listed in

Table 5-4 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-4: Finding for Emotion component

FINDING	CATEGORY	THEME
Finding 2: Most participants express heightened concern over their information, content and data on social media platforms.	• Can it be used by others • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 2** is viewed through the emotion component of the combined CPM and TPB theory model. Emotion is relayed through the sentiments that resonate in the participants' responses. The most important concern is the "information" of participants' data privacy. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Culture

McNealy and Mullis (2019) state that culture delineates parameters by which data privacy is viewed and considered. The authors strongly contend that culture shapes the ground rules for data dissemination (McNealy & Mullis, 2019). Al-Rabeeah and Saeed (2017) state that culture is often cited in the broader context. The authors believe that it is important to consider the impact of culture at a more granular level of detail, as much can be overlooked or dismissed when viewing culture holistically (Al-Rabeeah & Saeed, 2017). Petronio and Child (2020) express the importance of the role of culture in sound and reliable data privacy choices. The authors allude that culture sets the foundation for dependable, values-driven data privacy decisions (Petronio & Child, 2020).

P2, P3, P4, P13, P18, P23, P25, P27, P30, P31, P32, P33, P36, P37, P43, P45, P47, P49, P52, P55, P56, P57, P59, P60, P61, P62, P66, P68, P71, P72, P74, P81, P82, P83, P84, P88,

P89 and **P95** did not read the social media platform's Terms of Service at all. Moreover, **P1, P5, P6, P10, P11, P12, P14, P15, P16, P17, P19, P20, P22, P24, P26, P28, P29, P34, P35, P38, P39, P40, P41, P42, P46, P48, P50, P51, P54, P58, P63, P65, P67, P69, P70, P73, P75, P76, P77, P78, P79, P80, P85, P86, P87, P90, P91, P92, P93** and **P94** partly read the social media platforms' Terms of Service.

The sentiments convey the importance and associated challenges expressed by participants in reading the Terms of Service. When considering the cultural component, most participants spent most of their childhood in Cape Town. The mother-tongue speaker breakdown is illustrated in Table 4-6 above against the Terms of Service, which is not read, partly read, and read in full. The contingent of the group that read the Terms of Service in full consists of only English and Afrikaans mother-tongue speakers. The bulk of the participants who did not read or partly read the Terms of Service are English, Afrikaans, isiXhosa, Setswana, Dutch, German, Italian, Polish and Slovak mother-tongue speakers. Obar and Oeldorf-Hirsch (2022) state that more than 75% of adults over the age of 50 years are inclined to completely ignore the Terms of Service without opening or reading it. The authors add that many users open the Terms of Service but spend less than an average of one (1) minute on it (Obar & Oeldorf-Hirsch, 2022). Yerby and Vaughn (2022) contend that the Terms of Service and Privacy Policy documents of social media platforms are lengthy and aim to obfuscate the information for the reader (Finding 1 and 2). Whilst these authors state that most users are likely to ignore the Terms of Service, it is interesting that the small contingent that read the Terms of Service in full do not have any other mother-tongue speaker languages represented.

Table 5-5: Finding for Culture component

FINDING	CATEGORY	THEME
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management
Finding 2: Most participants express heightened concern over their information, content and data on social media platforms.		

In summary, **Findings 1 and 2** are viewed through the culture component of the combined CPM and TPB theory model. Culture is conveyed via the participants' responses to the survey questions against their cultural backdrop gathered from the respective demographic responses. Moreover, it is noteworthy that the participants expressed their concerns about risk, data privacy, and trust when interacting on social media platforms. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Politics

Al-Rabeeah and Saeed (2017:4) define "Politics as an ideology of financial secrecy". The authors add that this outlook is tied to privacy practices to preserve intellectual property and competitive advantage. Privacy is essentially seen as currency to maintain an industry or business, leading to guaranteed success (Al-Rabeeah & Saeed, 2017).

The above-mentioned politics component is not relevant to this study. The preservation of intellectual property and competitive advantage is not needed as most participants use social media platforms in a personal capacity.

Gender

Al-Rabeeah and Saeed (2017) and Petronio and Child (2020) state that men and women view data privacy differently. The authors explain that women employ privacy logic independently, where each woman would determine their logic. This infers that no two women would necessarily apply identical privacy logic to achieve the outcome. Men are forecasted to follow a collective privacy logic. This is achieved by two or more men establishing the privacy logic and selecting it (Petronio & Child, 2020). McNealy and Mullis (2019:111) conclude that "gender and culture" play a significant role in data privacy choices. The authors add that gender influences certain data privacy behaviours where women and men would make contrasting decisions (McNealy & Mullis, 2019).

The 95 participants in the study are evenly split at 50,5% males and 48,4% females. One (1) participant chose not to disclose their gender.

Finding 1 explains the Terms of Service versus Gender and Age group for survey question 14. Most genders and age groups are represented in the "Not read at all" and "Partly read" groups. The small contingent of seven (7) participants that read the Terms of Service in full consists of females in the 46-50 and 51-55 age groups and males in the 26-30, 31-35, 41-45 and 51-55 age groups. The gender and age group cohort lack representation for most age

groups for both males and females. Petronio and Child (2020) allude that gender plays a significant role in managing data choices since males and females handle their choices differently.

Finding 1 in Table 5-6 is linked to the gender component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-6 in an attempt to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-6: Finding for Gender component

FINDING	CATEGORY	THEME
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 1** is viewed through the gender component of the combined CPM and TPB theory model. Gender is conveyed via the participants' responses to the survey questions against their gender gathered from the respective demographic responses. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Motivation

Al-Rabeeah and Saeed (2017) discuss that people's privacy logic may be linked to their motivation. The authors explain that the privacy logic may provide clues of incentives that informed their data dissemination (Al-Rabeeah & Saeed, 2017). McNealy and Mullis (2019) acknowledge motivation as one of the five drivers that compel a person to acclimate to the organisational or business culture and accepted practices.

Findings 3 and 4, relay the usage reasons for survey questions 13 and 16. The social media cases for the Family, Interests, Share Information and Other (Entertainment) groupings all

demonstrate increases, with the most notable increases being for Interests and Share Information groupings. Numerous decreases are also noted. However, Spare time usage decreases most amongst these groups.

Findings 3 and 4 in Table 5-7 are linked to the motivation component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-7 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-7: Finding for Motivation component

FINDING	CATEGORY	THEME
Finding 3: Social media platform use cases evolving demonstrate usefulness either not available or not as well implemented at the time of registration. The groupings for Interests and Share information have proven most useful.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management
Finding 4: There is a reduction in the use of groupings for Spare time, and Participate in online discussions and Communities.		

In summary, **Findings 3 and 4** are viewed through the motivation component of the combined CPM and TPB theory model. Motivation is conveyed via the participants' value attributed to using the social media platforms. An evolution of the usage driver is noted between the initial registration needs and the downstream usage needs of participants. Additionally, participants attribute significant value to data risk, privacy importance and trust in a social media platform. These concerns, when managed well by a social media platform, can motivate users to take up and keep using the solution.

Context

Al-Rabeeah and Saeed (2017) propose that the context in which a person or people find themselves may have a short- or long-term impact on their privacy logic. The authors contend that context has the most influence on data privacy logic formulation (Al-Rabeeah & Saeed, 2017). McNealy and Mullis (2019) explain that privacy logic is bound by the context. The authors further explain that a user would exhibit different privacy behaviours for a family

member and friend as opposed to a stranger. They acknowledge that the social media context is not well documented. In the social media context, the prescripts are dictated by the social media platforms and various social media groups or communities (McNealy & Mullis, 2019).

Finding 2 confirms that the context of the study is limited to social media utilisation by adults residing in South Africa. The main social media platforms acknowledged by participants include Facebook, X, Instagram, TikTok, WeChat, Snapchat, LinkedIn, YouTube, WhatsApp and Telegram. Strava and Botim are two other social media platforms noted in the participants' responses.

Finding 2 in Table 5-8 is linked to the context component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-8 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-8: Finding for Context component

FINDING	CATEGORY	THEME
Finding 2: Most of the participants express heightened concern over their information, content and data on social media platforms.	• Can it be used by others • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 2** is viewed through the context component of the combined CPM and TPB theory model. Context is conveyed by the Aim of the study and confirmed via the participants' responses. The specific social media platforms discussed are Facebook, X, Instagram, TikTok, WeChat, Snapchat, LinkedIn, YouTube, WhatsApp, Telegram, Strava and Botim. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Attitude

According to Al Halbusi et al. (2023), attitude pertains to the allure presented to a person. The authors add that attitude comprises the person's entrenched value set and principles. These values and principles have the power to influence privacy logic choices (Al Halbusi et al., 2023). Zhang et al. (2020) describe attitude as revealing the emotive state of the person. Wang et al. (2022) outline that attitude is one of the main determinants informing data privacy behaviour. Kumar (2019:380) states, "Attitude, together with Subjective Norm and Perceived Control, can have a causal impact on the behavioural intention, leading to the manifestation of behaviour".

Finding 1 presents that **P2, P3, P4, P13, P18, P23, P25, P27, P30, P31, P32, P33, P36, P37, P43, P45, P47, P49, P52, P55, P56, P57, P59, P60, P61, P62, P66, P68, P71, P72, P74, P81, P82, P83, P84, P88, P89** and **P95** did not read the social media platform's Terms of Service at all. Moreover, **P1, P5, P6, P10, P11, P12, P14, P15, P16, P17, P19, P20, P22, P24, P26, P28, P29, P34, P35, P38, P39, P40, P41, P42, P46, P48, P50, P51, P54, P58, P63, P65, P67, P69, P70, P73, P75, P76, P77, P78, P79, P80, P85, P86, P87, P90, P91, P92, P93** and **P94** partly read the social media platforms' Terms of Service. The aforementioned raw facts drawn from the participants' responses to survey question 14 sketch their attitude toward reading the Terms of Service of social media platforms.

The participants' responses to survey question 19 are depicted in a word cloud in Figure 4-31 where the sentiments "information", "use", "services", "content", "account", "high", "importance", "friend", "data" and "password" frequently recur **(Finding 2)**.

Findings 1 and 2 in Table 5-9 are linked to the attitude component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-9 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-9: Finding for Attitude component

Finding	Category	Theme
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective	• Can it be used by others? • Permission to use data for incentive • Privacy importance	• Data privacy management

Finding	Category	Theme
social media platform's Terms of Service and Privacy Policy.	• Trust • Risk • Data protection • Upload	
Finding 2: Most of the participants express heightened concern over their information, content and data on social media platforms.		

In summary, **Findings 1 and 2** are viewed through the attitude component of the combined CPM and TPB theory model. Attitude is conveyed by the participants' aversion to reading the Terms of Service, their concern for data privacy, and their approach to privacy management after experiencing a breach. Lastly, the participants selected the highest ratings for risk, data privacy importance, and trust. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Subjective norm

Zhang et al. (2020) explain that subjective norm is demonstrative of the surroundings. Kumar (2019:380) and Kasim et al. (2021:2) attribute "Attitude", "Subjective Norm", and "Perceived Control" as driving privacy behaviour. According to Kasim et al. (2021:2), subjective norm affects the behavioural "intentions" of an individual. Wang et al. (2022:5) believe that "subjective norms" influence the individual to either execute or not execute a certain behaviour.

Finding 1 describes the Terms of Service via participants' responses to survey question 14. It provides the prescript for a user to interact on the social media platform by essentially setting the tone for appropriate online behaviour. Reading the Terms of Service is essential for every user to comprehend what constitutes acceptable behaviour. Therefore, it is worrying that most of the participants expressed responses entailing "Not read at all" and "Partly read". Neubaum et al. (2023) state that "subjective norms" relate to the acceptable conduct of users. The authors contend that the acceptability of interaction is observed in the manifested exchanges between people (Neubaum et al., 2023).

Finding 1 in Table 5-10 is linked to the subjective norm component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the

associated categories listed in Table 5-10 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-10: Finding for Subject Norm component

FINDING	CATEGORY	THEME
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 1** is viewed through the subjective norms component of the combined CPM and TPB theory model. Subjective norms are outlined in the Terms of Service, and appropriate versus inappropriate user behaviour is determined. As numerous participants confirmed that they either did not read or partly read the Terms of Service of several social media platforms, a user could contravene the rules imposed by the social media platform. Offences could be minor to serious issues that would likely result in some form of user sanction. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Behavioural control

Kumar (2019:380) and Kasim et al. (2021) contend that "Behavioural Control" forms part of three conditions influencing privacy behaviour. Zhang et al. (2020) explain that behavioural control is directed by the person scanning the situation and environment to decide whether to enact the behaviour. Wiese et al. (2021) assert that behavioural control is encouraged or discouraged. The authors add that the behaviour is driven by the users' objective (Wiese et al., 2021).

Finding 1 encompasses the Terms of Service that participants submitted in response to survey question 14. Ideally, the Terms of Service would provide the user with the ground rules for interacting on the respective social media platform. It curates the accepted user behaviour to be employed on the platform.

P2, P3, P4, P13, P18, P23, P25, P27, P30, P31, P32, P33, P36, P37, P43, P45, P47, P49, P52, P55, P56, P57, P59, P60, P61, P62, P66, P68, P71, P72, P74, P81, P82, P83, P84, P88, P89 and **P95** amounting to 38 participants acknowledged that they did not read the Terms of Service of their subscribed social media platforms.

P1, P5, P6, P10, P11, P12, P14, P15, P16, P17, P19, P20, P22, P24, P26, P28, P29, P34, P35, P38, P39, P40, P41, P42, P46, P48, P50, P51, P54, P58, P63, P65, P67, P69, P70, P73, P75, P76, P77, P78, P79, P80, P85, P86, P87, P90, P91, P92, P93 and **P94** representing 50 participants partly read the Terms of Service of their subscribed social media platforms.

The bulk of the participants acknowledge partial or unread approaches to the Terms of Service. Therefore, whilst the Terms of Service is the best mechanism to relay behavioural control, it is not useful in this study's context, and participants would be prone to contravening the rules. According to Obar and Oeldorf-Hirsch (2022), over 75% of adults over the age of 50 years would not bother to read the Terms of Service. Users who open the Terms of Service are reported to spend less than an average of one (1) minute on it (Obar & Oeldorf-Hirsch, 2022).

Finding 1 in Table 5-11 is linked to the behavioural control component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-11 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-11: Finding for Behavioural Control Component

FINDING	CATEGORY	THEME
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 1** relays the behavioural control component of the combined CPM and TPB theory model. The Terms of Service provide a behavioural control mechanism to curate appropriate user behaviour. However, as most participants either did not read or partly read the Terms of Service of several social media platforms, it is ineffective as behavioural control. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Boundary permeability

McNealy and Mullis (2019) describe boundary permeability as the dissemination of variants and safeguarding of data. The authors state that this entails how much or little access is afforded to the data consumers (McNealy & Mullis, 2019). Petronio and Child (2020:77) propose that boundary permeability relates to the "thickness" of the boundary that the data owner affords the data consumer. This encompasses the volume of data shared with the data consumer and access (Petronio & Child, 2020).

Finding 2 illustrates the participants' responses to survey question 19 in a word cloud in Figure 4-31 where the sentiments "information", "use", "services", "content", "account", "high", "importance", "friend", "data" and "password" are emphasised. These sentiments convey the participants' level of concern for data privacy. In lieu of the level of concern expressed, it seems reasonable that the participants would safeguard the data and implement medium- to high-level protections.

Finding 2 in Table 5-12 is linked to the behavioural permeability component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-12 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-12: Finding for Boundary Permeability Component

FINDING	CATEGORY	THEME
Finding 2: Most of the participants express heightened concern over their information, content and data on social media platforms.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 2** conveys the boundary permeability component of the combined CPM and TPB theory model. The boundary permeability will likely result in the hardening of user defences to safeguard their information. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Boundary linkage

McNealy and Mullis (2019) discuss the boundary linkage between the data owner and the data consumer. This pertains to the connection between the two parties. A robust connection means that the data owner would ease the boundary restrictions. Alternatively, a weak connection would realise more rigorous boundary restrictions for the data consumer (McNealy & Mullis, 2019). Petronio and Child (2020) add that the boundary linkage responsibility is extended to co-owners of the data at the point that the data owner disseminates the data, including the usage rules.

Finding 2 relates to social media platform utilisation from participants' responses to survey questions 13 and 16. The participants' primary and secondary reasons for social media platform usage were Friends and Family, respectively. In this scenario, the data owner and data consumer have an amenable pre-existing relationship and establishment trust. The

strong connection between these parties means that the boundary restrictions would be significantly eased. The third and fourth highest usage reasons are Interests and Communities, respectively. In light of the generality and unfamiliarity of these groups, the participants would likely tighten the boundary restrictions.

Finding 2 in Table 5-13 is linked to the boundary linkage component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-13 to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-13: Finding for Boundary Linkage Component

FINDING	CATEGORY	THEME
Finding 2: Most of the participants express heightened concern over their information, content and data on social media platforms.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, **Finding 2** conveys the boundary linkage component of the combined CPM and TPB theory model. The boundary linkage would likely ebb and flow depending on the closeness of the data owner and data consumer. A boundary linkage for friends and family would likely be more eased. However, where the relation is less established, and there is uncertainty, the boundary linkage would be tightened. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Boundary ownership

McNealy and Mullis (2019) contend that boundary ownership is the mutual understanding delineation. Petronio and Child (2020) and McNealy and Mullis (2019) agree that boundary ownership confers ownership between the parties whilst prescribing how the data can be used and shared.

Finding 1 relays the response outcome of survey question 14 for participants who did not read, partly read, and fully read the Terms of Service for social media platforms. Most genders and age groups are represented in the “Not read at all” and “Partly read” groups. The small contingent of seven (7) participants that read the Terms of Service in full is made up of females in the 46-50 and 51-55 age groups and males in the 26-30, 31-35, 41-45 and 51-55 age groups. The gender and age group cohorts lack representation for most age groups, both male and female. The Terms of Service explain ownership of the data uploaded to social media platforms. However, since most participants did not read or partly read the Terms of Service, they would not necessarily know who the owner is. This fact resonates throughout the participants’ responses to survey question 19.

Finding 1 in Table 5-14 is linked to the boundary ownership component of the combined CPM and TPB theory model. The findings are tied to Theme 1: Data privacy management and the associated categories listed in Table 5-14 in an attempt to answer Sub-research Question 1 (SRQ1) mentioned below.

Table 5-14: Finding for Boundary Ownership Component

FINDING	CATEGORY	THEME
Finding 1: Over 50 per cent of the participants reported that they partly read the Terms of Service. In section 2.5.1 of the thesis, the researcher conducted a document review of the respective social media platform's Terms of Service and Privacy Policy.	• Can it be used by others? • Permission to use data for incentive • Privacy importance • Trust • Risk • Data protection • Upload	• Data privacy management

In summary, most of the participants did not read or did not understand the Terms of Service. Furthermore, participants do not know who the owner of the uploaded data is. In the case of the participants who partly read or read the Terms of Service in full, they do not understand what they read or misinterpreted it. The group that did not read it would not necessarily know who the owner is. It is important to note that the findings cannot be generalised due to the small size of the participants’ sample.

5.5.2 Research objective 2

Research Objective 2: To determine the data privacy threat perception of adult social media users residing in South Africa.

SRQ2: What is the perceived privacy threat awareness level of adult social media users?

Sub-research question 2 (SRQ2) evaluates the perception of data privacy threats among adult social media users residing in South Africa. Categories informing Theme 2 provide a view of the participants' data privacy management. Additionally, Theme 2 is linked to objective 2 and sub-research question 2.

Beigi and Liu (2020) assert that social media platforms have become the hunting grounds for bad actors harvesting the wealth of freely available personal information. The malicious actors can skilfully craft their attacks on social media users through a variety of means (Beigi & Liu, 2020). Moreover, Hajli et al. (2021) report concerning trends in social media companies exploiting user data, with or without consent, for a variety of use cases. The researcher will assess users' perceptions of data privacy threats to determine whether adequate data privacy management is implemented.

Therefore, the researcher will attempt to better grasp the interactions of social media users by applying the Al-Rabeeah and Saeed (2017) combined CPM and TPB theory model against the SRQ2. This is presented under the respective combined CPM and TPB components below.

Legal

Al-Rabeeah and Saeed (2017) describe the legal framework afforded to data owners and data guardians as the protection mechanism for data privacy. South Africa (2020) states that the Protection of Personal Information Act 4 of 2013 affords data privacy owners with the necessary legal instruments to protect their personal information. Furthermore, all social media platforms are obligated to provide their Terms of Service and Privacy Policy to inform users of the rights and protections afforded to them when using the social media platform. The literature review in section 2.6 evaluates the content of the Terms of Service and Privacy Policy for Facebook, X, Instagram, TikTok, WeChat, Snapchat, LinkedIn, YouTube, WhatsApp and Telegram. Strava and Botim are two other social media platforms that were noted in the participants' responses and evaluated in section 2.6.

P1, P16, P18, P19 and **P91** report that the social media platform owns the uploaded data. The participants believe that social media platforms afford many rights to the data upon upload, and they can use the data for any means. Furthermore, some participants exhibit uncertainty regarding ownership of social media platforms. However, despite not knowing who the owners are, participants confirm that they continue to use the social media platforms.

P1, P2, P3, P5, P8, P9, P10, P11, P12, P13, P14, P15, P16, P18, P19, P22, P24, P26, P27, P28, P30, P32, P34, P35, P36, P37, P38, P41, P42, P43, P44, P50, P51, P54, P58, P59, P60, P65, P66, P67, P70, P71, P73, P75, P79, P81, P82, P84, P86, P87, P88, P92, P93 and **P94** selected this "High" risk option accounting for 54 participants. This is demonstrative of the majority of participants being concerned about the risk they are confronted with.

P1, P3, P5, P6, P7, P8, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P25, P26, P28, P29, P30, P32, P35, P36, P37, P38, P39, P41, P42, P43, P44, P46, P47, P48, P50, P51, P52, P53, P54, P55, P57, P58, P59, P60, P62, P64, P65, P66, P68, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P84, P85, P86, P87, P88, P92, P93, P94 and **P95** unanimously selected the "High" option for importance of data constituting 75 of the participants.

P2, P3, P5, P6, P7, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P26, P27, P30, P32, P34, P35, P37, P38, P39, P40, P41, P42, P43, P44, P45, P50, P51, P52, P53, P54, P57, P58, P60, P61, P62, P64, P65, P66, P68, P71, P72, P74, P75, P76, P77, P79, P81, P82, P83, P87, P88, P90, P92 and **P93** selected the high option making up 63 of the participants that feel that trust in the social media platform is crucial.

It is abundantly clear that most of the participants who indicated that they partly and wholly read the Terms of Service are incorrect when they state that the social media platform owns and solely benefits from the upload of users' data **(Finding 5 and 6)**. A significant proportion of the English, Afrikaans and isiXhosa mother-tongue speaker sample either did not read or partially read the Terms of Service. This spans all age groups and genders. This infers that the participants are concerned about the trustworthiness and risk associated with social media platforms (**Findings 7 and 8)**. According to Chen et al. (2021), examining the human aspect of the data privacy management behaviour of users may provide clues to their weaknesses. Bandara et al. (2021), Chen et al. (2021) and Arzoglou et al. (2023) discuss the privacy paradox where users exhibit erratic behaviour when managing their social media data privacy. The authors state that the erratic privacy practice is attributed to dissimilarities in demography,

technical aptitude, general usage and the need for social recognition (Bandara et al., 2021). Conversely, this study's results do not align with the findings in the aforementioned authors' research. A significant proportion of English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit similar behaviours.

Findings 5, 6, 7 and 8 in Table 5-15 are also linked to the legal component of the combined CPM and TPB theory model. The findings are tied to Theme 2: Social media utilisation and threat perception and the associated categories listed in Table 5-15 to answer Sub-research Question 2 (SRQ2) mentioned below.

Table 5-15: Finding for Legal component

FINDING	CATEGORY	THEME
Finding 5: The majority of the participants believe that the social media platform is the primary benefactor of the data uploaded, where they can target marketing and monitor user activity to make social media feed recommendations. Moreover, the participants are of the opinion that the social media platform can do with the uploaded data as they please, including sharing and selling with third parties.	• Ownership • Registration reason • Usage purpose • Terms of service	• Social media utilisation and threat perception
Finding 6: The participants stated that social media platforms are the owners of the uploaded data.		
Finding 7: Most of the participants attribute the highest level of risk to using a social media platform.		
Finding 8: Participants predominantly consider data privacy to be of the highest importance when utilising a social media platform.		

In summary, **Findings 5, 6, 7 and 8** are viewed through the legal component of the combined CPM and TPB theory model. An unexpected observation shows that most English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit similar behaviours. The affected mother-tongue speakers and age groups are discussed in

detail above. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Culture

McNealy and Mullis (2019) state that culture delineates parameters by which data privacy is viewed and considered. The authors strongly contend that culture shapes the ground rules for data dissemination (McNealy & Mullis, 2019). Al-Rabeeah and Saeed (2017) state that culture is often cited in the broader context. The authors believe that it is important to consider the impact of culture at a more granular level of detail, as much can be overlooked or dismissed when viewing culture holistically (Al-Rabeeah & Saeed, 2017). Petronio and Child (2020) express the importance of the role of culture in sound and reliable data privacy choices. The authors allude that culture sets the foundation for dependable, values-driven data privacy decisions (Petronio & Child, 2020).

In **Finding 5,** the bulk of the participants convey that the data uploaded by users is stored on the social media platform and used for the organisation's benefit through targeted marketing and content recommendations. This sentiment is expressed in the quotations below.

P10 stated that "It is avaliable for all too see, at any given time. Anything uploaded to social media will always be in the backend. Can be found/traced for years to come." **P58** reports that "Others will be able to view and share the information." **P67** is of the opinion that "Any one who can see the information can download and use it".

Most participants convey that the social media platform is the owner of the data uploaded by users. The remaining groups are small and believe that the user, other company, or government is the owner of the uploaded data **(Finding 6)**. This sentiment is expressed in the quotations below.

P1 is of the opinion that "The social media platform". **P16** claims that "The social media platform will have your data after I have given consent they might share your data in other platforms". **P2** concludes that they are "The user". **P4** argues that "Photos- I own it. My personal info - probably the service provider. I really don't know".

Findings 7, 8 and 9 relate to the threat perception of social media users. The participants expressed a high level of concern for the risk, data privacy importance, and trust when interacting on social media platforms. Obar and Oeldorf-Hirsch (2022) report that users may afford higher degrees of blind trust for policies like Terms of Service or Privacy Policy endorsed

by organisational, friendship and familial connections. The authors contend that users would predominantly avoid reading the policy in these scenarios by leaning on the culture of these connections and accepting the conditions prescribed by the platform. However, they add that trust is embedded and cannot be dismissed from the process (Obar & Oeldorf-Hirsch, 2022).

P1, P2, P3, P5, P8, P9, P10, P11, P12, P13, P14, P15, P16, P18, P19, P22, P24, P26, P27, P28, P30, P32, P34, P35, P36, P37, P38, P41, P42, P43, P44, P50, P51, P54, P58, P59, P60, P65, P66, P67, P70, P71, P73, P75, P79, P81, P82, P84, P86, P87, P88, P92, P93 and **P94** selected this "High" option accounting for 54 participants. Most participants are worried about the risk when interacting on social media platforms.

P1, P3, P5, P6, P7, P8, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P25, P26, P28, P29, P30, P32, P35, P36, P37, P38, P39, P41, P42, P43, P44, P46, P47, P48, P50, P51, P52, P53, P54, P55, P57, P58, P59, P60, P62, P64, P65, P66, P68, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P84, P85, P86, P87, P88, P92, P93, P94 and **P95** unanimously selected the "High" option constituting 75 of the 95 participants.

P2, P3, P5, P6, P7, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P26, P27, P30, P32, P34, P35, P37, P38, P39, P40, P41, P42, P43, P44, P45, P50, P51, P52, P53, P54, P57, P58, P60, P61, P62, P64, P65, P66, P68, P71, P72, P74, P75, P76, P77, P79, P81, P82, P83, P87, P88, P90, P92 and **P93** selected this option making up 63 of the 95 participants.

Despite dissimilarities in the study's demography, the participants demonstrated similar concerns and behaviours. A significant proportion of English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit similar behaviours.

Findings 5, 6, 7 and 8 in

Table 5-16 are also linked to the culture component of the combined CPM and TPB theory model. The findings are tied to Theme 2: Social media utilisation and threat perception and the associated categories listed in Table 5-16 to answer Sub-research Question 2 (SRQ2) mentioned below.

Table 5-16: Finding for Culture component

FINDING	CATEGORY	THEME
Finding 5: The majority of the participants believe that the social media platform is the primary benefactor of the data uploaded, where they can target marketing and monitor user activity to make social media feed recommendations. Moreover, the participants are of the opinion that the social media platform can do with the uploaded data as they please, including sharing and selling with third parties.	• Ownership • Registration reason • Usage purpose • Terms of service	• Social media utilisation and threat perception
Finding 6: The participants stated that social media platforms are the owners of the uploaded data.		
Finding 7: Most of the participants attribute the highest level of risk to using a social media platform.		
Finding 8: Participants predominantly consider data privacy to be of the highest importance when utilising a social media platform.		
Finding 9: The participants contend that trust in a social media platform is critical. Therefore, they selected the highest level of trust when asked the question.		

In summary, **Findings 5, 6, 7, 8 and 9** are viewed through the culture component of the combined CPM and TPB theory model. Culture is conveyed via the participants' responses to the survey questions against their cultural backdrop gathered from the respective demographic responses. Moreover, it is noteworthy that the participants expressed their concerns about risk, data privacy, and trust when interacting on social media platforms. A significant proportion of English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit similar behaviours. Lastly, the behavioural sentiments raised by participants display the shift in behaviour and resonance of differing

choices against demographics. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Politics

Al-Rabeeah and Saeed (2017:4) define "Politics as an ideology of financial secrecy". The authors add that this outlook is tied to privacy practices to preserve intellectual property and competitive advantage. Privacy is essentially seen as currency to maintain an industry or business, leading to guaranteed success (Al-Rabeeah & Saeed, 2017).

The above-mentioned politics component is not relevant to this study. The preservation of intellectual property and competitive advantage is not needed as most participants use social media platforms in a personal capacity.

Motivation

Al-Rabeeah and Saeed (2017) discuss that people's privacy logic may be linked to their motivation. The authors explain that the privacy logic may provide clues of incentives that informed their data dissemination (Al-Rabeeah & Saeed, 2017). McNealy and Mullis (2019) acknowledge motivation as one of the five drivers that compel a person to acclimate to the organisational or business culture and accepted practices.

The participants' responses to survey questions 20, 21, and 22 demonstrate that they have a strong affinity to opt for the highest level of concern for risk, data privacy importance, and trust for social media platforms (Findings 7, 8, **and 9)**. Obar and Oeldorf-Hirsch (2022) and Yerby and Vaughn (2022) ascribe significant importance to trust and risk when users evaluate whether to use a social media platform.

P1, P2, P3, P5, P8, P9, P10, P11, P12, P13, P14, P15, P16, P18, P19, P22, P24, P26, P27, P28, P30, P32, P34, P35, P36, P37, P38, P41, P42, P43, P44, P50, P51, P54, P58, P59, P60, P65, P66, P67, P70, P71, P73, P75, P79, P81, P82, P84, P86, P87, P88, P92, P93 and **P94** represent the participants that selected the high option for risk **(Finding 7)**.

P1, P3, P5, P6, P7, P8, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P25, P26, P28, P29, P30, P32, P35, P36, P37, P38, P39, P41, P42, P43, P44, P46, P47, P48, P50, P51, P52, P53, P54, P55, P57, P58, P59, P60, P62, P64, P65, P66, P68, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P84, P85, P86, P87, P88, P92, P93,

P94 and **P95** encompass the participants that selected high data privacy importance **(Finding 8)**.

P2, P3, P5, P6, P7, P9, P10, P11, P12, P13, P14, P16, P17, P19, P20, P21, P22, P23, P24, P26, P27, P30, P32, P34, P35, P37, P38, P39, P40, P41, P42, P43, P44, P45, P50, P51, P52, P53, P54, P57, P58, P60, P61, P62, P64, P65, P66, P68, P71, P72, P74, P75, P76, P77, P79, P81, P82, P83, P87, P88, P90, P92 and **P93** consist of the participants that feel that trust is key to data privacy when using social media platforms **(Finding 9)**.

Participants expressed concern for the importance of their data risk, privacy, and trust in social media platforms. Arzoglou et al. (2023) discuss the privacy paradox where users exhibit erratic behaviour when managing their social media data privacy. The authors state that the erratic privacy practice is attributed to dissimilarities in demography, technical aptitude, general usage and the need for social recognition (Bandara et al., 2021). This study's results do not align with the findings of the authors, as mentioned in earlier research. A significant proportion of English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit similar behaviours.

Findings 7, 8 and 9 in Table 5-17 are linked to the motivation component of the combined CPM and TPB theory model. The findings are tied to Theme 2: Social media utilisation and threat perception and the associated categories listed in Table 5-17 to answer Sub-research Question 2 (SRQ2) mentioned below.

Table 5-17: Finding for Motivation component

FINDING	CATEGORY	THEME
Finding 7: Most of the participants attribute the highest level of risk to using a social media platform.	• Ownership • Registration reason • Usage purpose • Terms of service	• Social media utilisation and threat perception •
Finding 8: Participants predominantly consider data privacy to be of the highest importance when utilising a social media platform.		
Finding 9: The participants contend that trust in a social media platform is critical. Therefore, they selected the highest level of trust when asked the question.		

In summary, **Findings 7, 8 and 9** are viewed through the motivation component of the combined CPM and TPB theory model. Motivation is conveyed via the participants' value attributed to using the social media platforms. An evolution of the usage driver is noted between the initial registration needs and the downstream usage needs of participants. Additionally, participants attribute significant value to data risk, privacy importance and trust in a social media platform. These concerns, when managed well by a social media platform, can motivate users to take up and keep using the solution.

Attitude

According to Al Halbusi et al. (2023), attitude pertains to the allure presented to a person. The authors add that attitude comprises the person's entrenched value set and principles. These values and principles have the power to influence privacy logic choices (Al Halbusi et al., 2023). Zhang et al. (2020) describe attitude as revealing the emotive state of the person. Wang et al. (2022) outline that attitude is one of the main determinants informing data privacy behaviour. Kumar (2019:380) states, "Attitude, together with Subjective Norm and Perceived Control, can have a causal impact on the behavioural intention, leading to the manifestation of behaviour".

Findings 7, 8 and 9 are collected from the participants' responses to survey questions 20, 21 and 24 for risk, data privacy importance and trust, respectively. The majority of the participants submit high ratings for all three (3) questions and attest to the highest level of concern for the attitude component. According to Obar and Oeldorf-Hirsch (2022), the attitude of a subject is intrinsic to the data privacy behaviour expressed.

Findings 7, 8 and 9 in

Table 5-18 are linked to the attitude component of the combined CPM and TPB theory model. The findings are tied to Theme 2: Social media utilisation and threat perception and the associated categories listed in Table 5-18 to answer Sub-research Question 2 (SRQ2) mentioned below.

Table 5-18: Finding for Attitude component

FINDING	CATEGORY	THEME
Finding 7: Most of the participants attribute the highest level of risk to using a social media platform.	• Ownership • Registration reason • Usage purpose • Terms of service	• Social media utilisation and threat perception
Finding 8: Participants predominantly consider data privacy to be of the highest importance when utilising a social media platform.		
Finding 9: The participants contend that trust in a social media platform is critical. Therefore, they selected the highest level of trust when asked the question.		

In summary, **Findings 7, 8 and 9** are viewed through the attitude component of the combined CPM and TPB theory model. Attitude is conveyed by the participants' aversion to reading the Terms of Service, their concern for data privacy, and their approach to privacy management after experiencing a breach. Lastly, the participants selected the highest ratings for risk, data privacy importance, and trust. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Boundary permeability

McNealy and Mullis (2019) describe boundary permeability as the dissemination variants and safeguarding of data. The authors state that this entails how much or little access is afforded to the data consumers (McNealy & Mullis, 2019). Petronio and Child (2020:77) propose that boundary permeability relates to the "thickness" of the boundary that the data owner affords the data consumer. This encompasses the volume of data shared with the data consumer and access (Petronio & Child, 2020).

The participants' responses to survey questions 20, 21 and 24 reveal maximum concern about their risk, data privacy importance, and trust in the social media platform. It seems reasonable with the participants' expressed concerns that they would strengthen their level of protection

to safeguard **(Finding 7, 8 and 9)**. Petronio & Child (2020) believe that when levels of trust are eroded, the user would ramp up their protection and harden their defences.

Findings 7, 8 and 9 in Table 5-19 are linked to the behavioural permeability component of the combined CPM and TPB theory model. The findings are tied to Theme 2: Social media utilisation and threat perception and the associated categories listed in Table 5-19 to answer Sub-research Question 2 (SRQ2) mentioned below.

Table 5-19: Finding for Boundary Permeability Component

FINDING	CATEGORY	THEME
Finding 7: Most of the participants attribute the highest level of risk to using a social media platform.	• Ownership • Registration reason • Usage purpose • Terms of service	• Social media utilisation and threat perception
Finding 8: Participants predominantly consider data privacy to be of the highest importance when utilising a social media platform.		
Finding 9: The participants contend that trust in a social media platform is critical. Therefore, they selected the highest level of trust when asked the question.		

In summary, **Findings 7, 8 and 9** convey the boundary permeability component of the combined CPM and TPB theory model. The boundary permeability will likely result in the hardening of user defences to safeguard their information. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Boundary ownership

McNealy and Mullis (2019) contend that boundary ownership is the mutual understanding delineation. Petronio and Child (2020) and McNealy and Mullis (2019) agree that boundary ownership confers ownership between the parties whilst prescribing how the data can be used and shared.

The Terms of Service explain ownership of the data uploaded to social media platforms. However, since most participants did not read or partly read the Terms of Service, they would

not necessarily know who the owner is. This fact resonates throughout the participants' responses to survey question 19 **(Finding 6)**.

Finding 6 in Table 5-20 is linked to the boundary ownership component of the combined CPM and TPB theory model. The findings are tied to Theme 2: Social media utilisation and threat perception and the associated categories listed in Table 5-20 to answer Sub-research Question 2 (SRQ2) mentioned below.

Table 5-20: Finding for Boundary Ownership Component

FINDING	CATEGORY	THEME
Finding 6: The participants stated that social media platforms are the owners of the uploaded data.	• Ownership • Registration reason • Usage purpose • Terms of service	• Social media utilisation and threat perception

In summary, most of the participants did not read or did not understand the Terms of Service. Furthermore, participants do not know who the owner of the uploaded data is. In the case of the participants who partly read or read the Terms of Service in full, they do not understand what they read or misinterpreted it. The group that did not read it would not necessarily know who the owner is. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

5.5.3 Research objective 3

Research Objective 3: To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

SRQ3: What are the behavioural barriers to privacy management implementation for adult social media users?

Sub-research question 3 (SRQ3) delves into the behavioural barriers to data privacy management of adult social media users. Categories informing Theme 3 provide a view of the participants' data privacy management. Additionally, Theme 3 is linked to objective 3 and sub-research question 3.

Barth and de Jong (2017) and Bandara et al. (2021) discuss the privacy paradox where users exhibit erratic behaviour when managing their social media data privacy. The authors state that the erratic privacy practice is attributed to dissimilarities in demography, technical aptitude, general usage and the need for social recognition (Bandara et al., 2021). According to Han et al. (2018), examining the human aspect of data privacy management behaviour of users may provide clues to their weaknesses.

Therefore, the researcher will attempt to better grasp the interactions of social media users by applying the Al-Rabeeah and Saeed (2017) combined CPM and TPB theory model against the SRQ3. This is presented under the respective combined CPM and TPB components below.

Culture

McNealy and Mullis (2019) state that culture delineates parameters by which data privacy is viewed and considered. The authors strongly contend that culture shapes the ground rules for data dissemination (McNealy & Mullis, 2019). Al-Rabeeah and Saeed (2017) state that culture is often cited in the broader context. The authors believe that it is important to consider the impact of culture at a more granular level of detail, as much can be overlooked or dismissed when viewing culture holistically (Al-Rabeeah & Saeed, 2017). Petronio and Child (2020) express the importance of the role of culture in sound and reliable data privacy choices. The authors allude that culture sets the foundation for dependable, values-driven data privacy decisions (Petronio & Child, 2020).

Finding 11 entails the behavioural aspect of social media users. The participants expressed a high level of concern for the risk, data privacy importance, and trust when interacting on social media platforms.

Figure 4-37 uses a word cloud to represent the sentiments noted for survey question 32. The most notable sentiments in the word cloud pertained to “social”, “media”, “data”, “privacy”, and “account”, confirming that participants are seriously concerned about this. The next layer of the participants’ concern pertains to “profile” and “delete”. The responses are from the 12 participants who experienced breaches on their social media accounts at least once. The affected participants are **P8, P20, P33, P40, P60, P67, P83, P86, P88, P90, P92** and **P93**. There was a notable shift in the participants’ “Breach Behaviour” after the breach, with most participants adopting at least a minimal protection approach. No breach behaviour change is observed for 51-55 and 56-60-year-old English-speaking males. Additionally, three (3) 26-30

year old males observed a breach behaviour change and opted for maximum protection **(Finding 11)**.

Finding 11 in Table 5-21 is linked to the culture component of the combined CPM and TPB theory model. The findings are tied to Theme 3: Behaviour and the associated categories listed in Table 5-21 to answer Sub-research Question 3 (SRQ3) mentioned below.

Table 5-21: Finding for Culture component

FINDING	CATEGORY	THEME
Finding 11: Participants value their data privacy on social media platforms.	• Breach awareness • Breach attitude • Breach behaviour • Personal experience	• Behaviour

In summary, **Finding 11** is viewed through the culture component of the combined CPM and TPB theory model. Culture is conveyed via the participants' responses to the survey questions against their cultural backdrop gathered from the respective demographic responses. Moreover, it is noteworthy that the participants expressed their concerns about risk, data privacy, and trust when interacting on social media platforms. Lastly, the behavioural sentiments raised by participants display the shift in behaviour and resonance of differing choices against demographics. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Gender

Al-Rabeeah and Saeed (2017) and Petronio and Child (2020) state that men and women view data privacy differently. The authors explain that women employ privacy logic independently, where each woman would determine their logic. This infers that no two women would necessarily apply identical privacy logic to achieve the outcome. Men are forecasted to follow a collective privacy logic. This is achieved by two or more men establishing the privacy logic and selecting it (Petronio & Child, 2020). McNealy and Mullis (2019:111) conclude that "gender and culture" play a significant role in data privacy choices. The authors add that gender influences certain data privacy behaviours where women and men would make contrasting decisions (McNealy & Mullis, 2019).

The 95 participants in the study are evenly split at 50,5% males and 48,4% females. One (1) participant chose not to disclose their gender.

The participants' response to survey question 32 is split between seven (7) males and five (5) females. No breach behaviour change is observed for one (1) 51-55 and one (1) 56-60 years old English-speaking males. Furthermore, one (1) 26-30, two (2) 36-40, one (1) 41-45 and one (1) 56-60-year-old male observed a breach behaviour change. One (1) 18-25, two (2) 31-35, one (1) 56-60, and one (1) 61 and above-year-old females observed a breach behaviour change **(Finding 12)**.

Finding 12 in Table 5-22 are linked to the gender component of the combined CPM and TPB theory model. The findings are tied to Theme 3: Behaviour and the associated categories listed in Table 5-22 to answer Sub-research Question 3 (SRQ3) mentioned below.

Table 5-22: Finding for Gender component

FINDING	CATEGORY	THEME
Finding 12: Many of the affected participants changed their data privacy management behaviour on social media platforms.	• Breach awareness • Breach attitude • Breach behaviour • Personal experience	• Behaviour

In summary, **Finding 12** is viewed through the gender component of the combined CPM and TPB theory model. Gender is conveyed via the participants' responses to the survey questions against their gender gathered from the respective demographic responses. Interestingly, certain age groups and genders gravitated to behavioural change, whilst two (2) participants did not. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Motivation

Al-Rabeeah and Saeed (2017) discuss that people's privacy logic may be linked to their motivation. The authors explain that the privacy logic may provide clues of incentives that informed their data dissemination (Al-Rabeeah & Saeed, 2017). McNealy and Mullis (2019) acknowledge motivation as one of the five drivers that compel a person to acclimate to the organisational or business culture and accepted practices.

Finding 12 observes a shift in the behaviour of participants when interacting on social media platforms. **P20, P60, P86, P88, P90** and **P92** selected a minimal protection approach, whereas **P8** selected a maximum protection approach. **P33, P40, P67, P83** and **P93** provided responses that offer no indication of attitude change. Obar and Oeldorf-Hirsch (2022) mention that users ascribe significant value to their data, including risk and trust concerns, yet choose to not fulfil the basic reading requirements of the Terms of Service. Yerby et al. (2019) state that basic user competence in protecting data on social media platforms is required to service risk and trust concerns.

Finding 12 in Table 5-23 is linked to the motivation component of the combined CPM and TPB theory model. The findings are tied to Theme 3: Behaviour and the associated categories listed in Table 5-23 in an attempt to answer Sub-research Question 3 (SRQ3) mentioned below.

Table 5-23: Finding for Motivation component

FINDING	CATEGORY	THEME
Finding 12: Many of the affected participants changed their data privacy management behaviour on social media platforms.	• Breach awareness • Breach attitude • Breach behaviour • Personal experience	• Behaviour

In summary, **Finding 12** is viewed through the motivation component of the combined CPM and TPB theory model. Motivation is conveyed via the participants' value attributed to using the social media platforms. An evolution of the usage driver is noted between the initial registration needs and the downstream usage needs of participants. Additionally, participants

attribute significant value to data risk, privacy importance and trust in a social media platform. These concerns, when managed well by a social media platform, can motivate users to take up and keep using the solution. Lastly, a change in the social media platform usage behaviour of participants is noted after participants experience account breaches, thereby motivating the behavioural shift. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Attitude

According to Al Halbusi et al. (2023), attitude pertains to the allure presented to a person. The authors add that attitude comprises the person's entrenched value set and principles. These values and principles have the power to influence privacy logic choices (Al Halbusi et al., 2023). Zhang et al. (2020) describe attitude as revealing the emotive state of the person. Wang et al. (2022) outline that attitude is one of the main determinants informing data privacy behaviour. Kumar (2019:380) states, "Attitude, together with Subjective Norm and Perceived Control, can have a causal impact on the behavioural intention, leading to the manifestation of behaviour".

Finding 11 reveals the breach attitude expressed in response to survey question 32. Figure 4-37 shows the high recurrence of "social", "media", "data", "privacy", and "account" through the relative size compared to less concerning sentiments. The sentiment discloses that participants have placed significant emphasis on it. Moreover, the participants' attitudes shifted toward applying information security protocols after their data breach. **P8, P20, P60, P86, P88, P90** and **P92** changed their social media platform behaviour after experiencing a breach of their account. This contrasts with **P33** and **P40,** who do nothing differently after their data breach. Notably, no breach behaviour change is observed for 51-55 and 56-60-year-old English-speaking males.

Table 5-24 is linked to the attitude component of the combined CPM and TPB theory model. The findings are tied to Theme 3: Behaviour and the associated categories listed in Table 5-24 to answer Sub-research Question 3 (SRQ3) mentioned below.

Table 5-24: Finding for Attitude component

FINDING	CATEGORY	THEME
Finding 11: Participants value their data privacy on social media platforms.	• Breach awareness • Breach attitude • Breach behaviour • Personal experience	• Behaviour

In summary, **Finding 11** is viewed through the attitude component of the combined CPM and TPB theory model. Attitude is conveyed by the participants' aversion to reading the Terms of Service, their concern for data privacy, and their approach to privacy management after experiencing a breach. Lastly, the participants selected the highest ratings for risk, data privacy importance, and trust. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Boundary permeability

McNealy and Mullis (2019) describe boundary permeability as the dissemination variants and safeguarding of data. The authors state that this entails how much or little access is afforded to the data consumers (McNealy & Mullis, 2019). Petronio and Child (2020:77) propose that boundary permeability relates to the "thickness" of the boundary that the data owner affords the data consumer. This encompasses the volume of data shared with the data consumer and (Petronio & Child, 2020) access (Petronio & Child, 2020).

Findings 11, 12 and 13 account for the privacy breaches experienced by 12 out of 95 participants. Eight (8) participants adopted minimal protection, and two (2) participants adopted maximum protection to safeguard their data privacy. Two (2) participants, 51-55 and 56-60-year-old English-speaking males, confirmed that they are doing nothing differently and have not adopted any form of security. **Finding 10** illustrates that most of the participants are aware of someone who experienced a breach. The awareness of breach incidents and information security implemented means that participants are aware of the problem. Therefore, the participants' protection will likely mitigate attacks and potential data losses.

Findings 10, 11, 12 and 13 are linked to the behavioural permeability component of the combined CPM and TPB theory model. The findings are tied to Theme 3: Behaviour and the associated categories listed in Table 5-25 to answer Sub-research Question 3 (SRQ3).

Table 5-25: Finding for Boundary Permeability Component

FINDING	CATEGORY	THEME
Finding 10: The survey question on whether participants knew someone who experienced a breach revealed that it still poses a problem today. This is reaffirmed by the breaches several participants experienced.	• Breach awareness • Breach attitude • Breach behaviour • Personal experience	• Behaviour
Finding 11: Participants value their data privacy on social media platforms.		
Finding 12: Many of the affected participants changed their data privacy management behaviour on social media platforms.		
Finding 13: Predominantly, participants selected minimal data privacy protections to safeguard themselves.		

In summary, **Findings 10, 11, 12 and 13** convey the boundary permeability component of the combined CPM and TPB theory model. The boundary permeability will likely result in the hardening of user defences to safeguard their information. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

5.6 Conclusion

Chapter Five (5) presents the interpretation of the analysis performed in Chapter 4. Interpretation of the findings is important as it attempts to deliver on the research aim and objectives of the study to answer the research questions. The research question and sub-research questions are provided below for easy reference.

RQ: What is the data privacy management behaviour of adult social media users?

SRQ1: How do adult social media users manage their privacy when interacting on a social media platform?

SRQ2: What is the perceived privacy threat awareness level of adult social media users?

SRQ3: What are the behavioural barriers to privacy management implementation for adult social media users?

Furthermore, the research aim and objectives are provided as a reminder and to orient the interpretation discussion of the study.

5.6.1 Aim and objectives

5.6.1.1 Aim

The study aims to determine the data privacy behaviour of adult users of social media residing in South Africa whilst interacting on social media platforms. The researcher intends to explore the reasons for the behaviour to contribute to the design of future data privacy awareness initiatives, identify potential data privacy threats and inform incremental information security improvement of social media platforms.

5.6.1.2 Objectives

1. To explore the privacy management methods and techniques employed by adult users of social media residing in South Africa to manage their privacy when interacting on a social media platform.
2. To determine the data privacy threat perception of adult social media users residing in South Africa.
3. To identify behavioural barriers to data privacy management implementation of adult social media users residing in South Africa.

The study is exploratory, with the researcher exploring through survey questionnaires how adult social media users residing in South Africa interact on social media platforms. This specifically relates to the treatment or management of their data privacy. The researcher uses the participants' embedded culture and beliefs as a lens to foster understanding of this phenomenon.

The following themes revealed in Chapter 4 are summarised below.

5.6.2 Themes

Focus on the interpretation is necessary to ensure that the themes or patterns are revealed to comprehend and reveal deep insights into the research problem. The researcher concentrated on the findings and the themes emanating from the data analysis to reveal meaning for this study. The researcher revealed three (3) themes and thirteen (13) findings as part of the analysis in Chapter 4. The three (3) themes are represented in Table 5-1 with linkages to the respective objectives and sub-research questions.

Theme 1: Data privacy management in Table 5-1 consists of the categories relating to the data privacy management aspects of uploaded data, incentivised permission for platforms to use the uploaded data, the importance of privacy, platform trust perception, risk of platform use, data protection and the beneficiary of uploaded data.

Theme 2: Social media utilisation and threat perception in Table 5-1 pertains to the categories relating to the social media utilisation and threat perception of ownership of uploaded data, registration reason, usage reason and understanding of the terms of service.

Theme 3: Behaviour encompasses the categories relating to social media user behaviour through breach awareness, breach attitude, breach behaviour, and personal experience.

5.6.3 Theory

Al-Rabeeah and Saeed (2017) assert that privacy can be affected when a person experiences a privacy breach and usually requires intervention to remediate the situation. The researcher employs the Al-Rabeeah and Saeed (2017) combined theory model illustrated in Figure 5-2 as the theoretical lens for the study to reveal a deeper meaning. The researcher will attempt to differentiate this qualitative study from similar studies by considering the components listed in Table 5-26 within the study's context.

Table 5-26: Components of combined CPM and TPB theories

PRIVACY FACTORS CPM:	DECISION-MAKING MODEL TPB:	BOUNDARY COORDINATION OPERATION CPM:
• Legal • Emotion • Culture • Politics • Gender • Motivation • Context	• Attitude • Subjective norm • Behavioural control	• Boundary permeability • Boundary linkage • Boundary ownership

5.6.4 Discussion

The study is exploratory in nature, where the researcher will explore through survey questionnaires how adult social media users residing in South Africa interact on social media platforms, specifically the treatment or management of their data privacy. The research problem relates to social computing and human-computer interaction (HCI) within the ICT sector, and the proposed study envisages detecting meaningful data privacy attitudes for adult social media users residing in South Africa.

The results are discussed at length in section 5.5 above. Several notable takeaways and one unexpected finding are described below.

5.6.4.1 Notable takeaways

The notable takeaways are extracted from the main body of text in the discussion and are reflected against the components of combined CPM and TPB theories.

Legal

Many of the study's participants responded that they did not read the Terms of Service of the social media platforms. This accounts for 88 out of 95 participants that fall into these groups. This fact is rather curious when reviewing the participants' concern for risk, data privacy importance and trust. The seven (7) participants who read the Terms of Service in full were

limited to English and Afrikaans mother-tongue speakers. Additionally, the 18-25, 36-40, 56-60 and 61 and above age groups are not represented in this group.

The Terms of Service for most social media platforms are only available in English. An inference for the participants included in the study can be made that the language of the Terms of Service is a determinant of whether it will be read. However, the former groups also have English mother-tongue speakers therein and debunk the inference. In closing, language usage, wording complexity, length and format are key factors that determine whether it will be read.

Emotion

The study's participants demonstrate significant concern for their risk, data privacy importance and trust when interacting on social media platforms. Emotion is relayed through the sentiments that resonate in the participants' responses. The most important concern is the "information" of participants' data privacy.

Culture

The impact of culture on the study is revealed in the participants' responses to the survey questions against their cultural backdrop. This is gathered from their respective demographic responses. Study participants expressed their concerns about risk, data privacy, and trust when interacting on social media platforms. The behavioural sentiments raised by participants display the shift in behaviour and resonance of differing choices against demographics.

Politics

The politics component is not relevant to the study. It relates to the preservation of intellectual property and competitive advantage. Since most of the participants use it in a personal capacity, there is no competitive aspect.

Gender

The 95 participants in the study are evenly split at 50,5% males and 48,4% females. One (1) participant chose not to disclose their gender. The gender component is quite interesting. Men and women are predisposed to different data privacy management behaviours driven by the unique privacy logic exhibited by each gender. Additionally, in the small group of participants who experienced breaches on their social media accounts, all participants, barring two (2) men, changed their data privacy management behaviour.

Motivation

Motivation is conveyed via the participants' value attributed to using the social media platforms. A shift from the initial registration needs to the downstream usage needs of participants is observed. The usage shift of the platform can be attributed to evolving user needs. Participants further tendered to extreme concern for their data risk, privacy importance, and trust in a social media platform. Lastly, a change in the social media platform usage behaviour of participants is noted after participants experienced account breaches, thereby motivating the behavioural shift.

Context

The main social media platforms acknowledged by participants include Facebook, X, Instagram, TikTok, WeChat, Snapchat, LinkedIn, YouTube, WhatsApp and Telegram. Strava and Botim are two other social media platforms noted in the participants' responses. Additionally, social media platforms ascribe their Terms of Service and Privacy Policy to provide usage ground rules. The fact that most participants do not read or do not adequately understand these rules places them at risk of rule contravention.

Attitude, Subjective norm and Behavioural control

The participants' attitude is conveyed by their aversion to reading the Terms of Service. Their concern expressed for data privacy and their approach to privacy management after experiencing a breach do not match their outlook concern. Numerous participants confirmed that they either did not read or partly read the Terms of Service of several social media platforms. A user could contravene the rules imposed by the social media platform due to ignorance, with offences receiving serious to nil repercussions issued by the platform. The Terms of Service provide a behavioural control mechanism to curate appropriate user

behaviour. However, as most participants either did not read or partly read the Terms of Service of the social media platforms, it is ineffective as behavioural control.

Boundary permeability, Boundary linkage and Boundary ownership

Boundary permeability will likely result in the hardening of user defences to safeguard their information. The prevalent threat and risk climate will have a natural impact on the behaviour of users. For boundary linkage, users make the determination based on their familiarity with the person or entity they are sharing with and the environment in which they are operating. The boundary ownership is recognised by the social media platform's Terms of Service statements. Users upload data routinely to social platforms. Most of the participants in this study do not know that they are the owners of the data.

5.6.4.2 Unexpected finding

The researcher conducted a comprehensive literature review in Chapter 2. The literature revealed some concerns regarding older adults not being amenable to reading the Terms of Service of social media platforms. However, the researcher did not anticipate the extent and permeation of the problem resonating throughout the study's participants. It encompasses a wide demographic of varying genders, age groups, mother-tongue speakers and communities.

The study's interpretation revealed some interesting revelations. Chapter Six: Conclusion provides a summary of the findings and an account of the contributions to the study. Furthermore, it casts the limitations observed in the study and potential opportunities for future research.

CHAPTER 6: CONCLUSION

6.1 Introduction

The chapter is organised into eight (8) sections. Section One (1) presents the Introduction, in which the researcher opens the final chapter of the study. A summary of the analysis is provided in Section Two (2), whereas Section 3 provides the discussion of the findings. Section Four (4) covers the implications of the research. Section Five (5) explains the limitations, and Section Six (6) provides the recommendations. The contribution is presented in Section Seven (7), and Section Eight (8) delivers the conclusion for this chapter.

This chapter provides an account of the research journey by providing a synopsis of the key findings. It realises the goal of the multi-year research by addressing the research gaps identified in Chapter 2. In the key findings section, the purpose of the study is briefly revisited to orientate the reader and thread together all the aspects to form a cohesive picture. Discussion of the themes and distinct trends are recapped whilst offering unexpected findings detected in the research. These themes and trends are associated with the research aim, objectives and questions formulated in Chapter 3 of the study. The implications and limitations sections shed light on the value offered by the findings and the scope of the research, respectively. A recommendations section attempts to list the research opportunities for future undertakings that would add value to the body of knowledge to support the improved management of data privacy on social media platforms in South Africa. The section on the contribution casts the theoretical, methodological and practical offerings that the research provides in a bid to add value to the research domain. In the conclusion, the final section threads all the research facts together to close out the chapter of an enthralling and humbling research journey.

Statistics South Africa (2024) notes that the South African population, amounting to 62,027,503 people in the census conducted in 2022, represents diverse groups and unique communities that speak a multitude of languages. Jamalova and Constantinovits (2020) assert that the smartphone and telecommunications industries are experiencing rampant growth, thereby lowering costs and removing barriers to entry. This extends the capability of accessing the internet beyond traditional personal computers (Jamalova & Constantinovits, 2020). Nyoni and Velempini (2018) attribute the convenience of access to mobile devices coupled with the social value aspect of social media platforms as a significant driver in the popularity of the platforms for South African social media users. According to Kemp (2024), the South African

social media user population is estimated at approximately twenty-six (26) million users as of January 2024. In light of these facts, the researcher believes that there is research value in understanding the data privacy management behaviour of adult social media users in South Africa. Whilst several studies have been conducted on this problem globally, very few studies have been conducted in the South African context.

The study is a mono-qualitative interpretivist study. It explores the phenomenon of data privacy management behaviour of adult social media users in South Africa. The research problem relates to social computing and human-computer interaction (HCI) within the Information and Communication Technology (ICT) sector.

Figure 6-1: Findings (Adapted from Analysis section, 2024)

The study uses the combined Communication Privacy Management (CPM) and the Theory of Planned Behaviour (TPB) as the lens through which to view the participants' data privacy management behaviour. The study considers the social and cultural influences of the participants to reveal any meaningful observations for their data privacy management behaviour.

The researcher opted for a simplified thematic analysis model whilst ensuring conformance to the broad steps and principles of the approach. It includes the following steps to analyse the data: 1. Start preparations for data analysis, 2. Consider all data, 3. Codify all data, 4. Create

themes, and 5. Devise a means to represent the themes. The findings are organised under the three themes that emerged from the analysis, namely: 1. Data privacy management, 2. Social media utilisation and threat perception, and 3. Behaviour depicted in Figure 6-1.

The purpose of this chapter is to provide a summary of the analysis and discuss the findings. Moreover, the chapter intends to convey the implications, limitations, recommendations and contributions of the study. The next section provides a synopsis of the data analysis conducted for the study.

6.2 Summary of the analysis

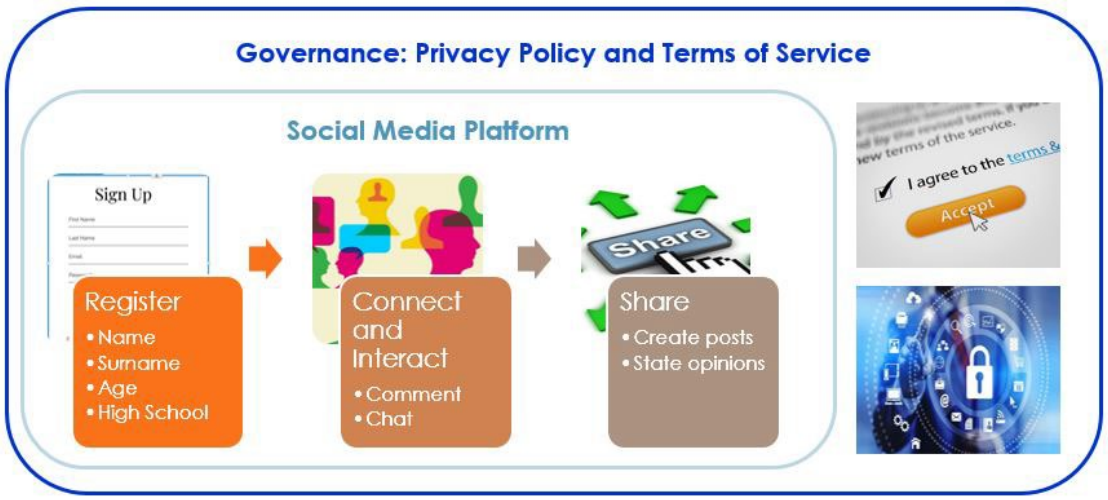


Figure 6-2: Social media platform utilisation (Adapted from research proposal, 2022)

Figure 6-2 above depicts a generic social media utilisation lifecycle. The typical South African privacy management behaviour exhibited is determined by an array of user privacy management decisions, as illustrated in Figure 6-3. Usage incentives encourage users to override their privacy management decision-making logic despite the risks. The privacy management decisions of South African social media users are heavily influenced by their language, age, gender, culture and community.

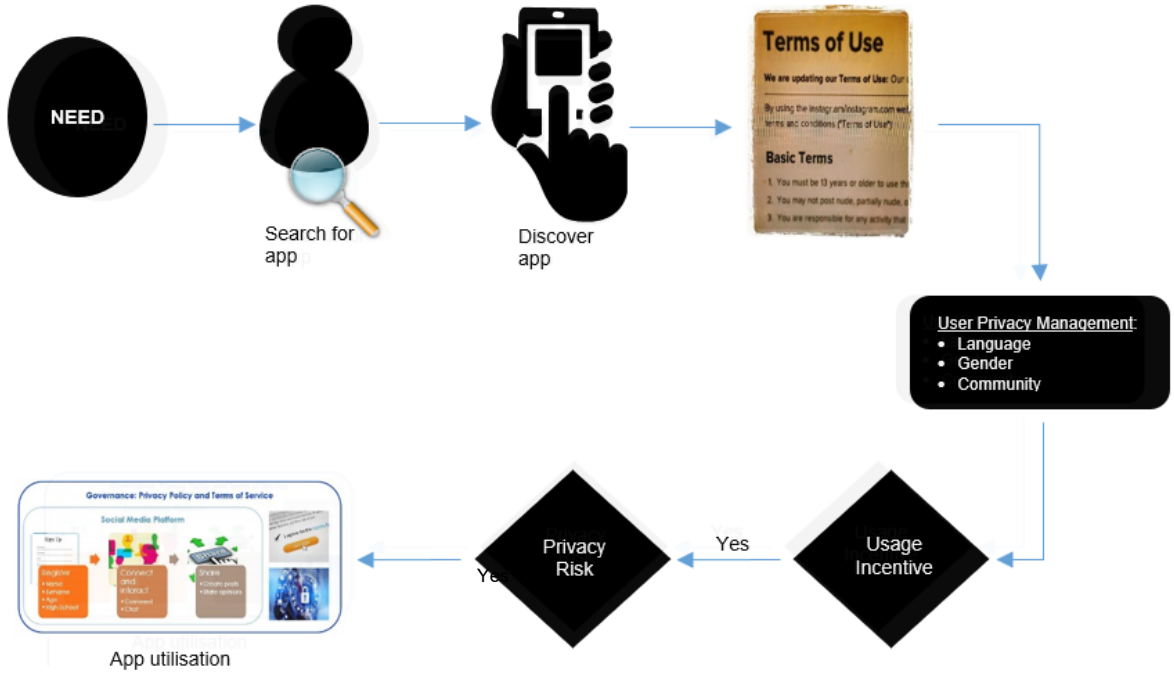


Figure 6-3: Privacy behaviour workflow (Adapted from research proposal, 2022)

Figure 6-4 illustrates the Integrated Framework for the research. Linkages of the Research Objectives and Research Questions to the respective Themes and Categories in the findings are plotted using the broken line arrows.

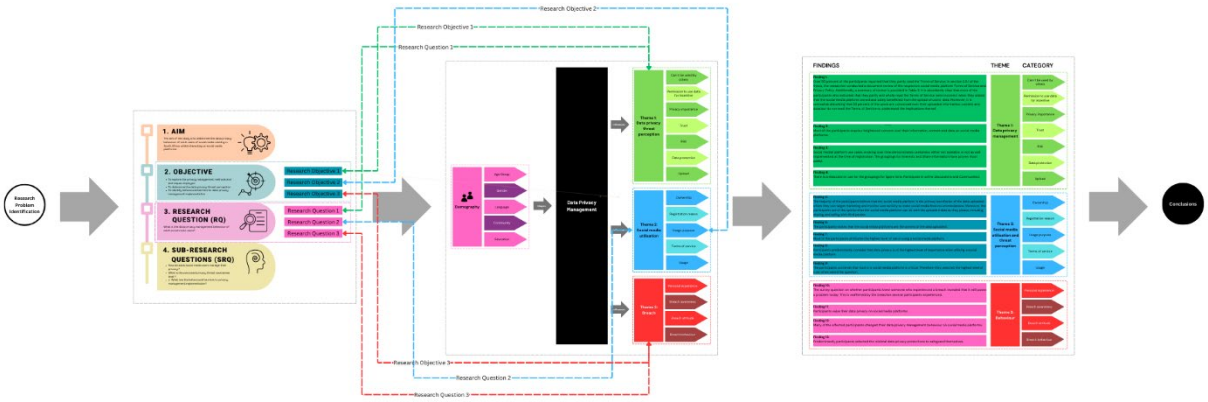


Figure 6-4: Integrated framework (Adapted from thesis, 2024)

Table 6-1 below provides an alternate view of the Aim, Research Question, Sub-Research Question and the linked themes presented in the analysis for ease of reference.

Table 6-1: Research questions and theme linkages

Nature	Research Questions	Research Objectives	Theme
Aim	The aim of the study is to determine the **data privacy behaviour** of adult **users of social media** residing in South Africa whilst interacting on the social media platforms.		
Main **RQ**	What is the **data privacy** management **behaviour** of adult **social media users**?		
Sub RQ1	How do adult **social media users** manage their **privacy** when interacting on a **social media** platform?	To explore the **privacy** management methods and techniques employed by adult **users of social media** residing in South Africa to manage their privacy when interacting on a **social media** platform.	**Theme 1:** Data privacy management
Sub RQ2	What is the perceived **privacy** threat awareness level of adult **social media users**?	To determine the data **privacy** threat perception of adult **social media users** residing in South Africa.	**Theme 2:** Social media utilisation and threat perception
Sub RQ3	What are the **behavioural barriers** to **privacy** management implementation for adult **social media users**?	To identify **behavioural barriers** to data **privacy** management implementation of adult **social media users** residing in South Africa.	**Theme 3:** Behaviour

The analysis utilises thematic analysis with several themes revealed from the associated codes and categories. Three (3) themes are observed, namely: Theme 1: Data privacy management, Theme 2: Social media utilisation and threat perception and Theme 3: Behaviour. A summary of themes is provided below.

Theme 1: Data privacy management

The first theme consists of the categories relating to the data privacy management aspects of uploaded data, incentivised permission for platforms to use the uploaded data, the importance of privacy, platform trust perception, risk of platform use, data protection and the beneficiary of uploaded data. These categories provide a view of the participants' data privacy management and outlook, thereby linking the theme to Research Objective 1 and Sub-research Question 1.

The findings related to Sub-research Question 1 allude that privacy management methods are affected by Theme 1: Data Privacy Management.

Theme 2: Social media utilisation and threat perception

The second theme pertains to the categories relating to social media utilisation and threat perception of ownership of uploaded data, registration reason, usage reason and understanding of the terms of service. These categories provide a view of the participants' threat perception of social media utilisation, thereby linking the theme to Research Objective 2 and Sub-research Question 2.

The findings related to Sub-research Question 2 allude that privacy management methods are affected by Theme 2: Social media utilisation and threat perception.

Theme 3: Behaviour

The third theme consists of categories relating to social media user behaviour, such as breach awareness, breach attitude, breach behaviour, and personal experience. These categories provide a view of the participants' behaviour on social media platforms, thereby linking the theme to Research Objective 3 and Sub-research Question 3.

The findings related to Sub-research Question 3 allude that privacy management methods are affected by Theme 3: Behaviour.

In summary, the study revealed that social media users do not read the Terms of Service and Privacy Policy of the platforms. Alternatively, users read these statements without understanding the content. These statements further appear to be designed to discourage the user from reading them. Users perceive a high degree of risk, and data importance and trust for social media platforms are necessary, but their actions do not support this outlook. Breaches of user accounts drive the adoption of information and privacy security principles to safeguard their interests.

The findings of the study will be covered in the next section. This section seeks to reveal any notable trends or patterns in the findings.

6.3 Discussion of findings

A focus on the interpretation is necessary to ensure that the themes or patterns are revealed to comprehend and reveal deep insights into the research problem. The researcher centres on the findings and the themes emanating from the data analysis to reveal meaning for this study.

The researcher reveals three (3) themes and thirteen (13) findings as part of the analysis in Chapter 4. The three (3) themes are represented in Table 6-1 with linkages to the respective objectives and sub-research questions.

The researcher employs the Al-Rabeeah and Saeed (2017) combined CPM and TPB theory model illustrated in Figure 5-2 as the theoretical lens for the study to reveal a deeper meaning. The researcher differentiates this qualitative study from similar studies by considering the components listed in Table 6-2 within the study's context.

Table 6-2: Components of combined CPM and TPB theories

PRIVACY FACTORS CPM:	DECISION-MAKING MODEL TPB:	BOUNDARY COORDINATION OPERATION CPM:
• Legal • Emotion • Culture • Politics • Gender • Motivation • Context	• Attitude • Subjective norm • Behavioural control	• Boundary permeability • Boundary linkage • Boundary ownership

The notable takeaways are extracted from the main body of text in the discussion and are reflected against the components of combined CPM and TPB theories. The next section discusses Sub-research Question 1, Theme 1: Data privacy management and the findings. It further explores the linkage to Research Objective 1.

6.3.1 Sub-research question 1

SRQ1: How do adult social media users manage their privacy when interacting on a social media platform?

There appears to be an aversion to reading the Terms of Service of social media platforms that resonates amongst the participants. Consideration of alternate media like short format video, infographic or audio clips could be better suited to relay this critical information that seems to be misunderstood. A small group of seven (7) participants read the Terms of Service in full. The group is limited to English and Afrikaans mother-tongue speakers. Additionally, the

18-25, 36-40, 56-60 and 61 and above age groups are not represented in this group. Lastly, the group consists of females in the 46-50 and 51-55 age groups and males in the 26-30, 31-35, 41-45 and 51-55 age groups.

An unexpected finding was that several age groups above 50 years of age indicated that they read the Terms of Service in full or in part. Obar and Oeldorf-Hirsch (2022) state that more than 75% of individuals over the age of 50 years are inclined to ignore the Terms of Service. The participants who read the Terms of Service, in full and in part, account for 72 per cent of the participants over the age of 50 years. This finding completely upends the findings of Obar and Oeldorf-Hirsch (2022).

The sentiments of participants convey that they value their data privacy and believe their data is important. However, 53 per cent of the users are concerned about their uploaded information, content, and data but do not read the Terms of Service to understand the implications. Bandara et al. (2021), Chen et al. (2021), and Arzoglou et al. (2023) explain the privacy paradox where users exhibit erratic behaviour when managing their social media data privacy. The authors state that the erratic privacy practice is attributed to dissimilarities in demography, technical aptitude, general usage and the need for social recognition (Bandara et al., 2021). Interestingly, the gender count is quite even, and most languages are represented in the group.

It is noteworthy that the participants expressed their concerns about risk, data privacy, and trust when interacting on social media platforms. Moreover, emotive sentiments resonate with participants' responses, citing their most important concern, which is the "information" of participants' data privacy.

6.3.2 Sub-research question 2

SRQ2: What is the perceived privacy threat awareness level of adult social media users?

An unexpected observation shows that most English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit similar behaviours. The affected mother-tongue speakers and age groups are discussed in detail above.

Participants' responses noted their risk concerns, data privacy importance, and trust when interacting on social media platforms. A significant proportion of English, Afrikaans, and isiXhosa mother-tongue speakers from all age groups, genders, and communities exhibit

similar behaviours. Lastly, the behavioural sentiments raised by participants display the shift in behaviour and resonance of differing choices against demographics.

An evolution of the usage driver is noted between the initial registration needs and the downstream usage needs of participants. Additionally, participants attribute significant value to data risk, privacy importance and trust in a social media platform. These concerns, when managed well by a social media platform, can motivate users to take up and keep using the solution.

Participants do not know who the owner of the uploaded data is. In the case of the participants who partly read or read the Terms of Service in full, they do not understand what they read or misinterpreted it. The group that did not read it would not necessarily know who the owner is. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

6.3.3 Sub-research question 3

SRQ3: What are the behavioural barriers to privacy management implementation for adult social media users?

Interestingly, certain age groups and genders gravitated to behavioural change, whilst two (2) participants did not.

Participants attribute significant value to data risk, privacy importance and trust in a social media platform. A change in the social media platform usage behaviour of participants is noted after participants experience account breaches, thereby motivating the behavioural shift. It is important to note that the findings cannot be generalised due to the small size of the participants' sample.

Breaches of the participants' social media accounts illustrate a hardening of users' defences to safeguard their information. Whilst users indicate that they value privacy, the practices do not match their privacy outlook.

6.3.4 Unexpected findings

A few unexpected findings are listed above in sections 6.3.1 and 6.3.2.

However, a finding where most participants knew someone who experienced a social media platform breach was unexpected. The researcher anticipated that at least a few participants would know of someone who had experienced it. Moreover, the researcher did not realise that participants would continue to exhibit risky privacy behaviours despite being armed with this knowledge. Several participants accounted for risky privacy management decisions driven by incentives and app functionality. The behaviour is likely driven by “emotion” and “motivation” aspects of the theoretical framework. The “emotion” aspect is especially difficult to determine without actual observation of the behaviour.

6.4 Implications

The study has culminated in numerous findings that have some practical implications associated. These implications are the outcome of applying the research aim, objectives and questions to the study to generate themes and findings. They have the potential to practically assist in improving the data privacy management of social media users and other online users.

The study has the potential to influence the medium used to relay information contained in legal instruments like the Terms of Service and Privacy Policy of social media platforms. Participants in the study predominantly do not read or understand the content of these statements. This has the potential for users to contravene the rules of the social media platform or broader legislation. Adopting alternative media to relay the information means that users can ingest the information more effectively. Moreover, these options have the advantage of using a more visual-based approach as opposed to heavy textual statements.

Theoretical Contribution: Language plays a key role in comprehending the information. Language importance in boundary coordination conveys the potential for CPM and TPB to be enhanced to add value for South African social media users.

Opportunities are created through the identification of research gaps that can be taken up to add to the body of knowledge. In the event the opportunity, as mentioned earlier, is addressed, the researcher can conduct a study to evaluate the efficacy and uptake of the new media. Additionally, the creation of frameworks to tailor social and enterprise awareness for various cultural groups presents another opportunity for research.

Practical Contribution: The findings reveal that each demographic has specific needs. Therefore, focused interventions that further address these needs are essential to get the

message across. Moreover, the delivery medium must also be considered to ensure the optimal impact of the message.

Lastly, the study provides gaps in legislation that legislators can address to improve data privacy management and accountability by social media platforms.

Legal Contribution: Government policymakers must heed the loopholes in the regulatory environment and tighten policy to ensure that social media platforms write their legal instruments, including Terms of Service, in simple and concise language.

The next section on limitations outlines the constraints and scope of the study.

6.5 Limitations

The study is a mono-qualitative interpretivist study using surveys to examine the data privacy behaviour of adult social media users. It attempts to capture the authentic perceptions, practices, experiences, behaviours, attitudes, and general outlook of social media users regarding their data privacy management behaviour. Children are excluded from the study in lieu of the ethical affordances necessary for inclusion. Moreover, the study is delineated to the confines of South Africa as the researcher resides in the Western Cape in South Africa. This is manageable due to the size, complexity, and time constraints of the study. The study's limitation to South Africa is to understand the influence of diverse cultures and communities on data privacy management. It would be pertinent to extend the study to a mixed-method study to improve the management of bias and confirm the qualitative results through quantitative means.

A cross-sectional approach focuses the study on the period that the data was collected. This means it will not provide the benefit that a longitudinal study delivers by observing the baseline and monitoring potential change over time. Conversely, the study is limited to gathering the data over a specific six (6) week duration, capturing the participant inputs at the time of collection. Employing a longitudinal study would prove interesting as the researcher would be able to evaluate and measure change over time. For example, the researcher could establish a baseline, conduct some interventions and re-evaluate post-intervention.

The research population in South Africa is estimated at 26 million social media users. The study garnered 95 responses through convenience sampling. This sampling method was selected due to the researcher's part-time student and full-time employment status, as

resources were limited. Although the study obtained a response rate of less than one (1) per cent of the population, it represents a fair participation level for a small study. Due to the exceptionally small sample with unique characteristics, the findings are not generalisable. A future study with more resources could be conducted on a significantly larger sample to ensure that the findings are generalisable.

A combined Communication Privacy Management (CPM) and the Theory of Planned Behaviour (TPB) are the lenses through which to view the participants' data privacy management behaviour. The social and cultural influences of the participants are considered to reveal any meaningful observations for their data privacy management behaviour.

The following sections list the In-scope and Out-of-scope items.

In-scope

The study is limited to the following parameters:

- Data privacy behaviour of adult social media users.
- The research population will be limited to adult social media users 18 years of age and older residing in South Africa.
- The study will be conducted within the confines of South Africa.
- Combined CPM and TPB theories will be employed.
- Influence of participants' age, language, education and community.

Out-of-scope

The study excludes the following:

- Social media users under 18 years of age.
- Legislation and policy instruments for managing data privacy, specifically the Protection of Personal Information Act 4 of 2013 of South Africa and global privacy legislation.
- Information security.
- Cyber security.
- Encryption and decryption.

6.6 Recommendations

McNealy and Mullis (2019:111) add that research involving CPM in the “social media context” is sparse and deserves attention. The authors tender that this is fertile ground for future research. This is supported by the gaps revealed in the study.

Given the limited sample size in this study, it is not possible to generalise the findings. However, this presents an opportunity to conduct a follow-up study armed with more resources to obtain a representative sample that can be generalised.

Furthermore, the fact that the Terms of Service, Privacy Policies, and other legal instruments are generally not read by individuals or users presents several opportunities.

Firstly, research should be done to formulate a framework to address the problem through other media, such as short-format videos, infographics, or audio clips. These media have the potential to present the information in a visual, image or audio format that may be more palatable. A short format video ranging between one and two minutes can convey multiple pieces of information. Similarly, still images combined with small pieces of text can relay numerous concepts on a single page. An audio file allows someone to listen to it whilst they are performing another task. The formulation of a framework to stimulate engagement in the information through other media may yield significant benefits, including apprising users of their rights.

Secondly, the findings can be considered when formulating a framework to tailor social and enterprise awareness content to better reach specific demographics. Social media service providers can better reach their users by providing content in languages they are comfortable reading and speaking. These acts promote inclusivity by considering the needs of non-Western demographics. Moreover, the consideration of language, personal beliefs, culture and community of the diverse South African population when tailoring training and awareness initiatives may drive user knowledge. The formulation of these initiatives has the potential to stimulate engagement in the information and apprise users of their rights. Educators must tailor their privacy training programmes per targeted demographic to ensure optimal delivery.

Thirdly, a framework can be developed for social media service providers to improve the reach of the Terms of Service and Privacy Policy. Options for a social media service provider can include blocking usage until content is consumed. However, this approach would necessitate a more effective means for users to ingest the information. Additionally, a social media service

provider could stimulate interaction through incentives like limited use of a premium function or a competition. This stimulates interest and excitement, driving users to ingest the information. Government policymakers must obligate social media platforms to avail their Terms of Service and Privacy Policy in all official South African languages by default.

Lastly, research can be done to highlight the legislative shortcomings so that legislators can tighten the law through amendment. It would allow legislators to identify the problem areas and determine where effort should be expended to obtain maximum value. Social media platforms must be mandated to foster transparency in their privacy settings and user education tools.

The recommendations, as mentioned earlier, have the potential to make a positive difference by implementing one or a combination of the recommendations. The conclusion is presented in the next section to close out the chapter and the study.

6.7 Conclusion

This chapter provides an account of the research journey by providing a synopsis of the key findings. In the key findings section, the purpose of the study is briefly revisited to orientate the reader and thread together all the aspects to form a cohesive picture. Discussion of the themes and distinct trends are recapped whilst offering unexpected findings detected in the research.

The researcher reveals three (3) themes and thirteen (13) findings. The three (3) themes are represented with linkages to the respective objectives and sub-research questions. The researcher employs the Al-Rabeeah and Saeed (2017) combined CPM and TPB theory model as the theoretical lens for the study to reveal a deeper meaning.

The themes and findings are derived to respond to the research aim, objectives and questions. The main research question and sub-research questions are provided for ease of reference.

RQ: What is the data privacy management behaviour of adult social media users?

> **SRQ1:** How do adult social media users manage their privacy when interacting on a social media platform?
>
> **SRQ2:** What is the perceived privacy threat awareness level of adult social media users?

SRQ3: What are the behavioural barriers to privacy management implementation for adult social media users?

SRQ1 is directly linked to Theme 1: Data privacy management. It seeks to answer Research Objective 1. The study reveals that social media users do not read or do not understand the Terms of Service and Privacy Policy of the platforms. These legal instruments are accused of deliberately obfuscating information to discourage the user from reading it. Additionally, users perceive a high degree of risk, and data importance and trust for social media platforms are necessary.

SRQ2 is directly linked to Theme 2: Social media utilisation and threat perception, and seeks to answer Research Objective 2. Users convey that over time, their use cases for social media platforms evolve. This means what they previously valued or considered important may no longer be viewed in the same light.

SRQ3 is directly linked to Theme 3: Behaviour and seeks to answer Research Objective 3. Breaches of user accounts drive the adoption of information and privacy security principles to safeguard their interests. This behaviour is interesting, considering that most users know someone who experienced a breach and initially do not do much to protect themselves. It takes their own account being breached to drive change in behaviour.

In short, what users say they do does not match their actions. Moreover, the legal instruments implemented by social media platforms are largely ineffective and discourage engagement. The lack of language diversity, gender appropriateness, and cultural considerations do not promote inclusivity. This places users at risk of contravening the rules of social media platforms and legislation.

This study bridges the gap in understanding how cultural factors influence data privacy behaviour, a topic underexplored in the South African context.

REFERENCES

Abdelaziz, Y., Napoli, D. & Chiasson, S. 2019. End-Users and Service Providers: Trust and Distributed Responsibility for Account Security. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*.

Adams, R. 2023. New BMWs to combat crime with innovative technology. *Paarl Post*. https://paarlpost.co.za/new-bmws-to-combat-crime-20230913-2/#:~:text=recognition%20(ANPR)%20cameras-,Ricardo%20Mackenzie%2C%20MEC%20for%20Mobility%20in%20the%20Western%20Cape%2C%20on,of%20just%20over%20R63%20million. 13 April 2025.

Ali, Z. 2023. Social Media Phishing – The 2023 Cybersecurity Threat. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/next-gen-infosec/social-media-phishing-threat/ 13 April 2025.

Al-Rabeeah, A.A.N. & Saeed, F. 2017. Data privacy model for social media platforms. In *2017 6th ICT International Student Project Conference (ICT-ISPC)*. IEEE: 1–5. https://ieeexplore.ieee.org/document/8075361/.

Alwafi, G. & Fakieh, B. 2024. A machine learning model to predict privacy fatigued users from social media personalized advertisements. *Scientific Reports*, 14(1).

Anti-Phishing Working Group. 2024. *Phishing Activity Trends Report: 2nd Quarter 2024*. http://www.apwg.org,.

Arzoglou, E., Kortesniemi, Y., Ruutu, S. & Elo, T. 2023. The Role of Privacy Obstacles in Privacy Paradox: A System Dynamics Analysis. *Systems*, 11(4).

Ayaburi, E.W. & Treku, D.N. 2020. Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 50: 171–181.

Azad, M.S., Khan, S.S., Hossain, R., Rahman, R. & Momen, S. 2023. Predictive modeling of consumer purchase behavior on social media: Integrating theory of planned behavior and machine learning for actionable insights. *PLoS ONE*, 18(12 December).

Babbie, E. 2016. *The Practice of Social Research*. www.cengagebrain.com.

Bandara, R.J., Fernando, M. & Akter, S. 2021. Construing online consumers' information privacy decisions: The impact of psychological distance. *Information and Management*, 58(7).

Barth, S. & de Jong, M.D.T. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7): 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013.

Becker, M. 2019. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology*, 21(4): 307–317.

Beigi, G. & Liu, H. 2020. A Survey on Privacy in Social Media. *ACM/IMS Transactions on Data Science*, 1(1): 1–38.

BenRhouma, O., AlZahrani, A., AlKhodre, A., Namoun, A. & Bhat, W.A. 2022. To sell, or not to sell: social media data-breach in second-hand Android devices. *Information and Computer Security*, 30(1): 117–136.

Biggs, R., Preiser, R., de Vos, A., Schlüter, M., Maciejewski, K. & Clements, H. 2022. *The Routledge Handbook of Research Methods for Social-Ecological Systems*. London: Routledge. https://www.taylorfrancis.com/books/9781003021339.

Blaxter, L., Hughes, C. & Tight, M. 2018. How to Research Trends. In *Menswear Trends*. Bloomsbury Publishing Plc: 130–165. https://www.bloomsburyfashioncentral.com/encyclopedia-chapter?docid=b-9781474227322&tocid=b-9781474227322-chapter5.

Botim. 2024. BOTIM Terms of Service. *Botim*. https://botim.me/home/ 15 April 2024.

Boukoros, S. & Katzenbeisser, S. 2017. Measuring privacy in high dimensional microdata collections. *ACM International Conference Proceeding Series*, Part F1305.

Braun, V., Clarke, V., Boulton, E., Davey, L. & McEvoy, C. 2021. The online survey as a qualitative research tool. *International Journal of Social Research Methodology*, 24(6): 641–654.

Chen, L., Huang, Y., Ouyang, S. & Xiong, W. 2021. The Data Privacy Paradox and Digital Demand. *SSRN Electronic Journal*. https://www.ssrn.com/abstract=3856834.

Creswell, J.W. & Creswell, J.D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fifth Edition. Los Angeles: Sage Publishing.

Delport, J. 2021. 14.3 Million South African Facebook Users Implicated by Data Breach. *IT News Africa*.

Delport, J. 2024. 14.3 Million South African Facebook Users Implicated by Data Breach. *IT News Africa.com*. https://www.itnewsafrica.com/2021/04/14-3-million-south-africa-facebook-users-implicated-by-data-breach/ 9 November 2024.

Espinosa, D.F. & Xiao, L. 2020. Twitter users' privacy concerns: What do their accounts' first names tell us? *Journal of Data and Information Science*, 3(1): 40–53.

Facebook. 2024. Facebook - Terms of service. *Facebook*. www.facebook.com 15 April 2024.

Farnell, C., Huff, P. & Cox, W. 2024. *Human Privacy in Virtual and Physical Worlds*. 1st Edition. M. C. Lacity & L. Coon, eds. Cham: Springer Nature Switzerland. https://link.springer.com/10.1007/978-3-031-51063-2.

Fazeldehkordi, E., Owe, O. & Noll, J. 2019. Security and Privacy Functionalities in IoT. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*.

Fung, B.C.M., Wang, K., Chen, R. & Yu, P.S. 2010. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, 42(4).

Fyke, Z., Griswold-Steiner, I. & Serwadda, A. 2019. Prying into Private Spaces Using Mobile Device Motion Sensors. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*.

Gilbert, P. 2018. Social media becomes biggest data breach threat. *IT Web*.

Hajli, N., Shirazi, F., Tajvidi, M. & Huda, N. 2021a. Towards an Understanding of Privacy Management Architecture in Big Data: An Experimental Research. *British Journal of Management*, 32(2): 548–565.

Hajli, N., Shirazi, F., Tajvidi, M. & Huda, N. 2021b. Towards an Understanding of Privacy Management Architecture in Big Data: An Experimental Research. *British Journal of Management*, 32(2): 548–565. https://onlinelibrary.wiley.com/doi/10.1111/1467-8551.12427.

Al Halbusi, H., Soto-Acosta, P. & Popa, S. 2023. Analysing e-entrepreneurial intention from the theory of planned behaviour: the role of social media use and perceived social support. *International Entrepreneurship and Management Journal*, 19(4): 1611–1642.

Hammons, R.L. & Kovac, R.J. 2019. *Fundamentals of Internet of Things for Non-Engineers*.

Han, K., Jung, H., Jang, J.Y. & Lee, D. 2018. Understanding Users' Privacy Attitudes through Subjective and Objective Assessments: An Instagram Case Study. *Computer*, 51(6): 18–28. https://ieeexplore.ieee.org/document/8395111/.

Hanlon, A. & Jones, K. 2023. Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions? *Journal of Strategic Marketing*.

Hollenbaugh, E.E. 2019. Privacy Management Among Social Media Natives: An Exploratory Study of Facebook and Snapchat. *Social Media and Society*, 5(3).

Hosken, G. 2020. Data from huge Experian breach found on the internet. *TimesLive*: 13–15.

Hu, H.F., Chang, Y.P., Lin, C. & Yen, C.F. 2019. Quality of life of gay and bisexual men during emerging adulthood in Taiwan: Roles of traditional and cyber harassment victimization. *PLoS ONE*, 14(2).

Illidge. 2024a. Legal warning about smartphones and social media in South Africa. *MyBroadband*.

Illidge. 2024b. Popular South African online store hit by data breach. *MyBroadband*.

Instagram. 2024. Instagram - Terms of use. *Instragram*. www.instragram.com 15 April 2024.

Iyamu, T. & Ngqame, Y. 2017. Towards a conceptual framework for protection of personal information from the perspective of act. *South African Journal of Information Management*, 19(1): 1–7. https://doi.org/.

Jamalova, M. & Constantinovits, M.G. 2020. Smart for development: Income level as the element of smartphone diffusion. *Management Science Letters*, 10(5): 1141–1150.

Kandeh, A.T., Botha, R.A. & Futcher, L.A. 2018. Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *SA Journal of Information Management*, 20(1): 1–9.

Kasim, K.O., Winter, S.R., Liu, D., Keebler, J.R. & Spence, T.B. 2021. Passengers' perceptions on the use of biometrics at airports: A statistical model of the extended theory of planned behavior. *Technology in Society*, 67.

Kemp, S. 2021. Digital 2021 - South Africa. https://datareportal.com/reports/digital-2021-south-africa 3 April 2024.

Kemp, S. 2024. Digital 2024 - South Africa. https://datareportal.com/reports/digital-2024-south-africa 3 April 2024.

Knight, M. 2023. An Epidemic in Enforceability: A Growing Need for Individual Autonomy in Health Care Data-Privacy Protection in an Era of Digital Tracking. *Vanderbilt journal of entertainment and technology law*, 25(4): 749–781. https://perma.cc/4KTF-8SB3].

Kshetri, N. & DeFranco, J.F. 2020. Is Privacy Dead? *IT Professional*, 22(5): 4–12.

Kuenzler, A. 2022. On (some aspects of) social privacy in the social media space. *International Data Privacy Law*, 12(1): 63–73. https://academic.oup.com/idpl/article/12/1/63/6403924.

Kumar, A. 2019. Exploring young adults' e-waste recycling behaviour using an extended theory of planned behaviour model: A cross-cultural study. *Resources, Conservation and Recycling*, 141: 378–389.

Kumar, R. 2011. *Research Methodology: A step-by-step guide for beginners*. 3rd ed. Los Angeles: Los Angeles : SAGE.

Kuşkonmaz, E.M. 2021. Right to Privacy and Right to Protection of Personal Data under the ECHR and the Charter. In *Privacy and Border Controls in the Fight against Terrorism*. Brill | Nijhoff: 60–116. https://brill.com/view/book/9789004439498/BP000003.xml.

Lacity, M.C. & Coon, L. 2024. *Human Privacy in Virtual and Physical Worlds*. 1st Edition. M. C. Lacity & L. Coon, eds. Cham: Springer Nature Switzerland. https://link.springer.com/10.1007/978-3-031-51063-2.

LinkedIn. 2024. LinkedIn - Pages terms. *LinkedIn*. https://www.linkedin.com/ 15 April 2024.

Liu, Y., Tse, W.K., Kwok, P.Y. & Chiu, Y.H. 2022. Impact of Social Media Behavior on Privacy Information Security Based on Analytic Hierarchy Process. *Information (Switzerland)*, 13(6).

Malinga, S. 2024. Data breaches affect over 1bn users in 2018. *IT Web*.

Mastrobattista, L., Muñoz-Rico, M. & Cordón-García, J.A. 2024. Optimising textual analysis in higher education studies through Computer-Assisted Qualitative Data Analysis (CAQDAS) with ATLAS.ti. *Journal of Technology and Science Education*, 14(2): 622–632.

McNealy, J. & Mullis, M.D. 2019. Tea and turbulence: Communication privacy management theory and online celebrity gossip forums. *Computers in Human Behavior*, 92: 110–118.

Messing, J., Bagwell-Gray, M., Brown, M.L., Kappas, A. & Durfee, A. 2020. Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. *Journal of Family Violence*, 35(7): 693–704.

Millard, D. & Bascerano, E.G. 2016. Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal*, 19(19).

Moodley, N. 2022. TransUnion data breach leaves 54 million South Africans exposed. *Daily Maverick*. https://www.dailymaverick.co.za/article/2022-03-19-transunion-union-data-breach-leaves-54-million-south-africans-exposed/ 3 November 2024.

Mzekandaba, S. 2023. Cape Town advances digitally-driven law enforcement. *IT Web*. https://www.itweb.co.za/article/cape-town-advances-digitally-driven-law-enforcement/mQwkoM6Yp8e73r9A 29 November 2024.

Mzekandaba, S. 2024. Data breaches rising at alarming rate, says InfoReg. *IT Web*.

Nemakonde, V. 2024. Saps 'ready' to advertise for police body cameras, but infrastructure still needs upgrades. *The Citizen*.

Nemmaoui, S., Baslam, M. & Bouikhalene, B. 2023. Privacy conditions changes' effects on users' choices and service providers' incomes. *International Journal of Information Management Data Insights*, 3(1).

Nene, N. 2024. City of Cape Town's 'eye in the sky' on the hunt for criminals. *EWN*. https://www.ewn.co.za/2024/05/06/city-of-cape-towns-eye-in-the-sky-on-the-hunt-for-criminals 29 November 2024.

Neubaum, G., Metzger, M., Krämer, N. & Kyewski, E. 2023. How Subjective Norms Relate to Personal Privacy Regulation in Social Media: A Cross-National Approach. *Social Media and Society*, 9(3).

Nind, M. 2023. *Handbook of Teaching and Learning Social Research Methods*. Cheltenham: Edward Elgar Publishing. https://www.ebsco.com/terms-of-use.

Nyoni, P. & Velempini, M. 2018. Privacy and user awareness on Facebook. *South African Journal of Science*, 114(5–6): 1–5.

Obar, J.A. & Oeldorf-Hirsch, A. 2022. Older Adults and 'the Biggest Lie on the Internet': From Ignoring Social Media Policies to the Privacy Paradox. *International Journal of Communication*, 16: 4779–4800. http://ijoc.org.

Ochoa, I., Calbusch, L., Viecelli, K., De Paz, J., Leithardt, V. & Zeferino, C. 2019. Privacy in the Internet of Things: A Study to Protect User's Data in LPR Systems Using Blockchain. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*.

Petronio, S. & Child, J.T. 2020. Conceptualization and operationalization: utility of communication privacy management theory. *Current Opinion in Psychology*, 31: 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009.

Primault, V., Boutet, A., Mokhtar, S. Ben & Brunie, L. 2019. The Long Road to Computational Location Privacy: A Survey. *IEEE Communications Surveys and Tutorials*, 21(3): 2772–2793.

Qureshi, S.F., Abbasi, M. & Shahzad, M. 2020. Cyber Harassment and Women of Pakistan: Analysis of Female Victimization. *Journal of Business and Social Review in Emerging Economies*, 6(2): 503–510. www.publishing.globalcsrc.org/jbsee.

Saunders, C.H., Sierpe, A., von Plessen, C., Kennedy, A.M., Leviton, L.C., Bernstein, S.L., Goldwag, J., King, J.R., Marx, C.M., Pogue, J.A., Saunders, R.K., Van Citters, A., Yen, R.W., Elwyn, G. & Leyenaar, J.K. 2023. Practical thematic analysis: a guide for multidisciplinary health services research teams engaging in qualitative analysis. *BMJ*: e074256. https://www.bmj.com/lookup/doi/10.1136/bmj-2022-074256.

Saunders, M.N.K., Lewis, Philip. & Thornhill, Adrian. 2019. *Research methods for business students*. Eighth. Harlow: Pearson.

Schubert, K.D. & Barrett, D. 2024. *Human Privacy in Virtual and Physical Worlds*. 1st Edition. M. C. Lacity & L. Coon, eds. Cham: Springer Nature Switzerland. https://link.springer.com/10.1007/978-3-031-51063-2.

Shokri, R., Theodorakopoulos, G., Le Boudec, J.Y. & Hubaux, J.P. 2011. Quantifying location privacy. *Proceedings - IEEE Symposium on Security and Privacy*: 247–262.

Snapchat. 2024. SnapChat - Terms of service. *Snapchat*. https://web.snapchat.com/ 15 April 2024.

Soratto, J., de Pires, D.E.P. & Friese, S. 2020. Thematic content analysis using ATLAS.ti software: Potentialities for researchs in health. *Revista Brasileira de Enfermagem*, 73(3).

South Africa. 2020. *Commencement of certain sections of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013)*.

Statistics South Africa. 2024. *Census 2022 in Brief*. Academic Press. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.statssa.gov.za/publications/Census2022inBrief/Census2022inBriefJune2024.pdf 30 October 2024.

Strava. 2024. Strava - Terms of use. *Strava*. www.strava.com 15 April 2024.

Telegram. 2024. Telegram - Terms of service. *Telegram*. https://web.telegram.org/ 15 April 2024.

Thorne, S. 2024. Cybercrime warning in South Africa. *Business Tech*. https://businesstech.co.za/news/technology/794744/cybercrime-warning-in-south-africa/ 9 November 2024.

TikTok. 2024. TikTok - Terms of service. *TikTok*. www.TikTok.com 15 April 2024.

Triga, V. & Manavopoulos, V. 2019. Does mode of administration impact on quality of data? Comparing a traditional survey versus an online survey via a voting advice application. *Survey Research Methods*, 13(2): 181–194.

Tsou, Y.T., Alraja, M.N., Chen, L.S., Chang, Y.H., Hu, Y.L., Huang, Y., Yu, C.M. & Tsai, P.Y. 2021. (k, ε, δ)-Anonymization: privacy-preserving data release based on k-anonymity and differential privacy. *Service Oriented Computing and Applications*, 15(3): 175–185. https://doi.org/10.1007/s11761-021-00324-2.

Wang, Y.Y., Wang, Y.S. & Wang, Y.M. 2022. What drives students' Internet ethical behaviour: an integrated model of the theory of planned behaviour, personality, and Internet ethics education. *Behaviour and Information Technology*, 41(3): 588–610.

WeChat. 2024. WeChat - Terms of service. *WeChat*. https://www.wechat.com/ 15 April 2024.

WhatsApp. 2024. WhatsApp - Terms of service. https://www.whatsapp.com/ 15 April 2024.

White, P. 2009. *Developing Research Questions: A guide for social scientists*.

Wiese, A., Galvin, E., O'Farrell, J., Cotter, J. & Bennett, D. 2021. Doctors' maintenance of professional competence: a qualitative study informed by the theory of planned behaviour. *BMC Health Services Research*, 21(1).

Wisse, M. & Roeland, J. 2022. Building blocks for developing a research question: The ABC-model. *Teaching Theology and Religion*, 25(1): 22–34.

X. 2024. X - Terms of service. *X*. www.x.com 15 April 2024.

Xue, J., Macropol, K., Jia, Y., Zhu, T. & Gelles, R.J. 2019. Harnessing big data for social justice: An exploration of violence against women-related conversations on Twitter. *Human Behavior and Emerging Technologies*, 1(3): 269–279.

Yerby, J., Koohang, A. & Paliszkiewicz, J. 2019. Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, 7(1): 1–13. http://www.iiakm.org/ojakm/articles/2019/OJAKM_Volume7_1pp1-13.php.

Yerby, J. & Vaughn, I. 2022. Deliberately confusing language in terms of service and privacy policy agreements. *Issues in Information Systems*, 23(2): 138–149.

YouTube. 2024. YouTube - Terms of service. *YouTube*. www.youtube.com 15 April 2024.

Zhang, X., Liu, S., Wang, L., Zhang, Y. & Wang, J. 2020. Mobile health service adoption in China: Integration of theory of planned behavior, protection motivation theory and personal health differences. *Online Information Review*, 44(1): 1–23.

Zuboff, S. 2019. *The Age of Surveillance Capitalism*. http://dx.doi.org/10.1016/j.ecolecon.2013.05.006.

APPENDICES

APPENDIX A: SURVEY QUESTIONNAIRE

QUESTIONS:

RESEARCH QUESTION (RQ)	SUB-RESEARCH QUESTIONS (SRQ)	CODE
What is the data privacy management behaviour of adult social media users?	1. How do adult social media users manage their privacy when interacting on a social media platform?	SRQ1
	2. What is the perceived privacy threat awareness level of adult social media users?	SRQ2
	3. What are the behavioural barriers to privacy management implementation for adult social media users?	SRQ3

TERMS:

#	TERM	DEFINITION/DESCRIPTION/EXPLANATION
1.	Social media platform	It is the information and communication technology platforms that allow for the formulation of social networks to share and interact.
2.	Terms of Usage	The Terms of Usage, commonly referred to as Terms of Service, relates to the usage of a service or product. It is further extended to rights of ownership and conditions of service by both the service provider and the user.

3.	Data privacy	Data privacy involves the concealment of personal information from persons not privy to the information. Disclosure of private data must be driven by consent of the owner or legal basis.

BIOGRAPHICAL QUESTIONS:

#	QUESTION
1.	<<< CONSENT QUESTIONS AS PER CONSENT FORM – Appendix B >>>
2.	Please select the age group you are in. • < 18 {questionnaire will not allow the child (under 18 years) to participate} • 18 – 25 • 26 – 30 • 31 – 35 • 36 – 40 • Etc.
3.	Select your gender. • Male • Female • Prefer not to say
4.	Select your highest level of education. • Primary school (Grades 1 – 7) • Secondary school (Grades 8 – 11) • Secondary school (Grade 12 / Matric)

#	QUESTION
	• Diploma • National Diploma • Advanced Diploma/ BTech Degree/ Honours Degree • Masters Degree/ MTech Degree • Doctorate/DTech Degree • No formal schooling • Prefer not to say • Other: _____
5.	Which of the following best describes your current employment status. • Employed • Not currently employed • Full-time student • Prefer not to say
6.	Which city do you live in?
7.	What languages do you read and speak? Select all that apply. • English • Afrikaans • Sepedi • Sesotho • Setswana

#	QUESTION
	• isiZulu • isiXhosa • isiSwati • isiNdebele • tshiVenda • xiTsonga • Other: _____
8.	What is your mother-tongue/first language? • English • Afrikaans • Sepedi • Sesotho • Setswana • isiZulu • isiXhosa • isiSwati • isiNdebele • tshiVenda • xiTsonga • Other: _____
9.	Select the Province you spent most of your childhood. • Western Cape • Gauteng • Kwazulu-Natal • Limpopo

#	QUESTION
	• Other: _____ • Etc.
10.	Which town or city did you spend most of your childhood?

POTENTIAL QUESTIONS:

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
11.	Please select the social media platforms that you use? • Facebook • Twitter • Instagram • TikTok • WeChat • SnapChat • LinkedIn • Etc.	Multi-select list	SRQ1
12.	On a scale from 1 to 10, rate how frequently you access any one of these social media platforms? For example: 1 = Rarely (once a month) TO 10 = Very often (several times a hour)	Likert scale	SRQ1

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
13.	Why did you register for a social media platform? Select all that apply. • Connect with friends • Connect with family • Connect with communities • Follow trends • Follow your interests • Share information • Participate in online discussions • Post photographs or video • It is something to do in your spare time • Marketing of my business • Classifieds: Selling of new or used good in personal capacity • Classifieds: Buying new or used goods • Other: _____	Multi-select list	SRQ1
14.	When you registered with a social media platform, did you read the “Terms of Usage” for the social media platform? • Not at all • Does not matter, it is all the same • Skimmed over it • Partly read it • Read in full	Single-select Likert scale	SRQ1

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
15.	What you think the “Terms of Usage” states/entails? Select all that apply. • It protects the social media user • It protects the social media platform service provider • It states how the data you post will be used • It states where the data will be hosted and how it will be protected • It states how the data will be handled or shared • Other: _____	Multi-select list	SRQ1
16.	How do you use social media? Select all that apply. • Connect with friends • Connect with family • Connect with communities • Follow trends • Follow your interests • Share information • Participate in online discussions • Post photographs or video • It is something to do in your spare time • Marketing of my business • Classifieds: Selling of new or used good in personal capacity • Classifieds: Buying new or used goods • Other: _____	Multi-select list	SRQ1

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
17.	Do you use social media in your personal capacity, business/work capacity or both? • Personal use • Business or work use • Both	Single-select list	SRQ1
18.	Please explain in your own words what you think happens with the data/information you upload to a social media platform?	Open ended	SRQ1
19.	Who do you think owns the data that you upload?	Open ended	SRQ1
20.	What risk do you believe there is in using a social media? • No risk • Low risk • Medium risk • High risk • Extreme risk	Single-select Likert scale	SRQ2
21.	How important is data privacy to you? • Unimportant • Low importance • Medium importance	Single-select Likert scale	SRQ2

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
	• High importance • Extreme importance		
22.	Do you protect your data on social media platforms? • Not at all • Take basic precautions • Take every precaution possible	Single-select Likert scale	SRQ2
23.	How do you protect your data? Select all that apply. • Do not protect my data • Change default account setting to private • Use a strong alphanumeric password combination (consists of upper and lowercase letters of alphabet, numbers, special characters and password length longer than 8 characters) • Use multi-factor or 2-factor authentication • Use different passwords for different social media accounts • Change passwords routinely • Do not accept friend requests unless you are sure they are a legitimate friend • Try not to check-in with location • Do not click on miscellaneous links • Use anti-virus software	Multi-select list	SRQ2

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
24.	Is trust of the social media platforms you are registered with important to you? • Unimportant • Low importance • Medium importance • High importance • Extreme importance	Single-select Likert scale	SRQ2
25.	Would you use a social media platform that you do not trust? • Yes • No • Not sure	Single-select Likert scale	SRQ2
26.	Would you use a social media platform that you do not trust if you received something for free e.g. discount code for a product? • Yes • No • Not sure	Single-select Likert scale	SRQ2

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
27.	Do you believe that the data (e.g. text, photo, video, etc.) you upload can be used by anyone else? • Not at all • No, my account is set to private and my friends would not share anything without my permission • Maybe, I have many friends and have not verified them all prior to accepting friend requests • Yes, my account is set to public and anyone can see what I have posted	Single-select Likert scale	SRQ2
28.	Would you allow the social media service provider to use your data if they allow you to use their app for free? • Not at all • Maybe. I would consider signing up for a free Facebook in exchange for user behaviour tracking e.g. using an algorithm to monitor what I view and how much time I spend on it to build a user behaviour profile of me • Yes. I would sign up for a free email account in exchange full monitoring of my emails	Single-select Likert scale	SRQ2
29.	Has the social media accounts of anyone you know been breached or hacked? • Yes • No	Single-select Likert scale	SRQ3

#	QUESTION	QUESTION TYPE	QUESTION LINKAGE CODE
	• Not sure		
30.	Has any of your social media accounts been breached or hacked? • Yes • No • Not sure	Single-select Likert scale	SRQ3
31.	If so, how many times has your social media account been breached or hacked? • At least once • Between 2 – 3 times • More than 3 times	Single-select Likert scale	SRQ3
32.	If so, how has the breach or hack affected your data privacy management practices?	Open ended	SRQ3

APPENDIX B: INDIVIDUAL CONSENT

FID/REC/ICv0.1

FACULTY OF INFORMATICS AND DESIGN

Individual Consent for Research Participation

Title of the study: **Data privacy management behaviour of social media users in South Africa**

Name of researcher: Ierefaan Batchelor

Contact details: email: ierefaan.bachelor@gmail.com Phone: 078 175 0830

Name of supervisor: Dr Errol Francke

Contact details: email: FranckeE@cput.ac.za Phone: 082 494 7851

Purpose of the Study: The purpose of this study is to better understand the data privacy management behaviour of adult social media users residing in South Africa. The research problem relates to social computing and human-computer interaction (HCI) within the Information and Communication Technology (ICT) sector with the proposed study envisaged to detect meaningful data privacy attitudes for adult social media users residing in South Africa.

Participation: This study will include participants via a survey study method. It is limited to collecting the views, ideas, preferences and opinions of the research participants using open-ended questions. Participants will be recruited via social media platforms e.g. LinkedIn and

Facebook. Participation in the study will be voluntary and the participant will be afforded an opportunity to withdraw at any stage of the study.

Confidentiality: The identities, personal information and data collected of the participants will be safeguarded against unauthorised access. Strict confidentiality will be observed.

Anonymity: The data collected will be aggregated for the study and all participants will remain anonymous. The identities, personal information and data collected of the participants will be safeguarded against unauthorised access.

Conservation of data: The data collected for the study will be safeguarded against unauthorised access. In lieu of the POPI Act, the data will only be used for the purposes explained to research participants and only kept for the duration required.

Voluntary Participation: Participation in the study will be voluntary and participants will be afforded an opportunity to withdraw at any stage of the study.

Additional consent: I make the following stipulations (please tick as appropriate):

	In thesis	**In research publications**	**Both**	**Neither**
My image may be used:				
My name may be used:				

My exact words may be used:				
Any other (stipulate):				

Acceptance: I, (print name) _____

agree to participate in the above research study conducted by Ierefaan Batchelor of the Faculty of Informatics and Design in the Department of Information Technology at the Cape Peninsula University of Technology, whose research is under the supervision of Dr Errol Francke.

If I have any questions about the study, I may contact the researcher or the supervisor. If I have any questions regarding the ethical conduct of this study, I may contact the Secretary of the Faculty Research Ethics Committee at 021 469 1012, or email naidoove@cput.ac.za.

Participant's signature: _____ Date: _____

Researcher's signature: _____ Date: _____

APPENDIX C: ETHICAL CLEARANCE

PO Box 1906, Bellville,7535 Symphony Way, Bellville, Cape Town, South Africa
+ 27 (0)21 959 6767 www.facebook.com/cput.ac.za info@cput.ac.za www.cput.ac.za

Office of the Research Ethics Committee
Faculty of Informatics and Design
Room 2.09
80 Roeland Street
Cape Town
Tel: 021-469 1012
Email: ndedem@cput.ac.za
Secretary: Mziyanda Ndede

22 September 2022

Mr Ierefaan Batchelor
c/o Department of Information Technology
CPUT

Reference no: 208006818/2022/23

Project title: Data privacy management behaviour of social media users in South Africa

Approval period: 22 September 2022 – 31 December 2023

This is to certify that the Faculty of Informatics and Design Research Ethics Committee of the Cape Peninsula University of Technology approved the methodology and ethics of Mr Ierefaan Batchelor (208006818) for MICT: IT (Magister Technologiae: Information and Communication Technology).

Any amendments, extension or other modifications to the protocol must be submitted to the Research Ethics Committee for approval.

The Committee must be informed of any serious adverse event and/or termination of the study.

Dr Blessing Makwambeni
Acting Chair: Research Ethics Committee
Faculty of Informatics and Design
Cape Peninsula University of Technology

Cape Peninsula
University of Technology
creating futures

PO Box 1906, Bellville,7535 Symphony Way, Bellville, Cape Town, South Africa
+ 27 (0)21 959 6767 www.facebook.com/cput.ac.za info@cput.ac.za www.cput.ac.za

Office of the Research Ethics Committee
Faculty of Informatics and Design
Room 2.09
80 Roeland Street
Cape Town
Tel: 021-469 1012
Email: ndedem@cput.ac.za
Secretary: Mziyanda Ndede

06 June 2024

Mr Ierefaan Batchelor
c/o Department of Information Technology
CPUT

Reference no: 208006818/2022/23

Project title: Data privacy management behaviour of social media users in South Africa

Approval period: 22 September 2022 – 30 June 2025 (Extension)

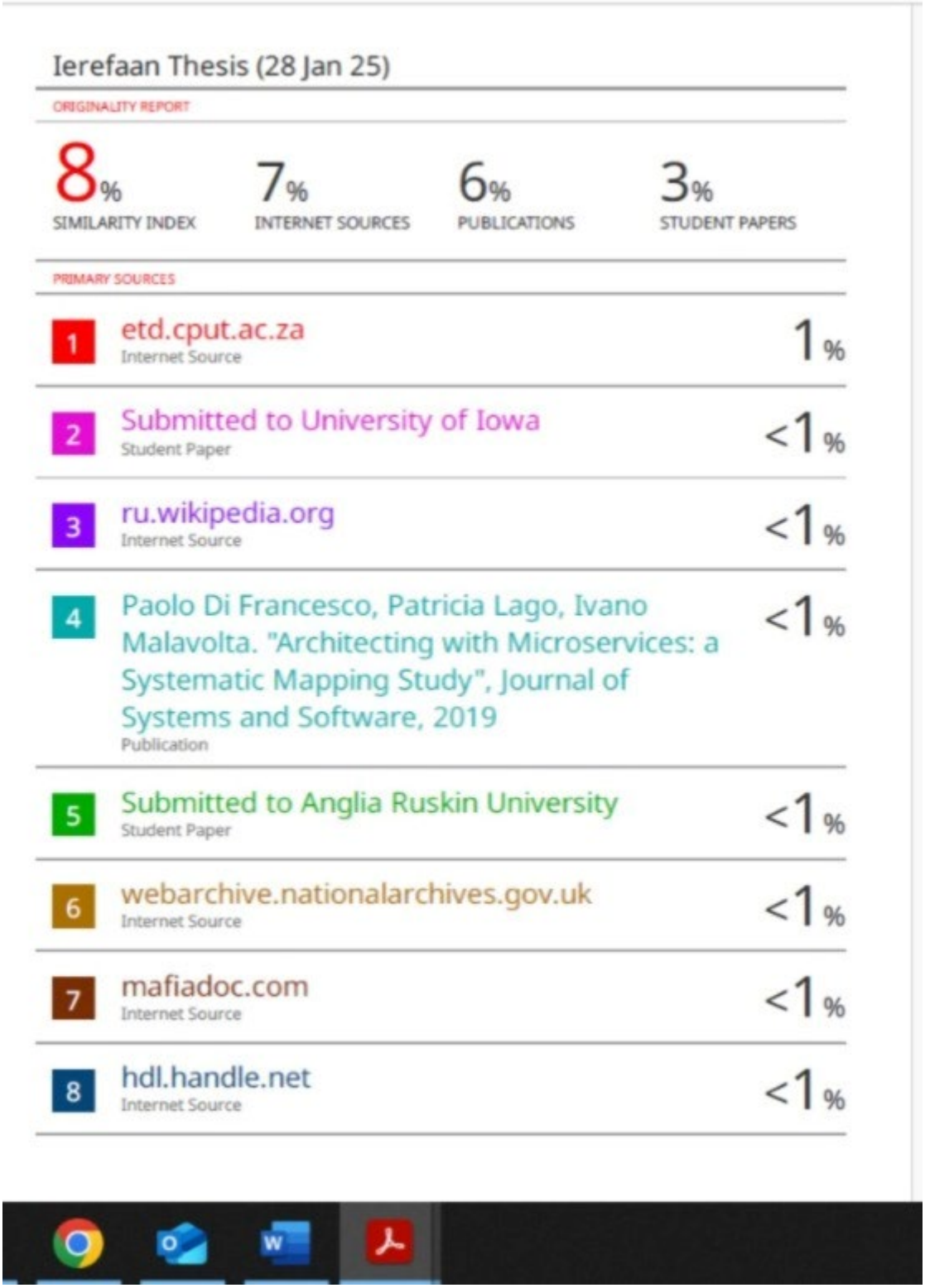
This is to certify that the Faculty of Informatics and Design Research Ethics Committee of the Cape Peninsula University of Technology approved the methodology and ethics of Mr Ierefaan Batchelor (208006818) for MICT: IT (Magister Technologiae: Information and Communication Technology).

Any amendments, extension or other modifications to the protocol must be submitted to the Research Ethics Committee for approval.

The Committee must be informed of any serious adverse event and/or termination of the study.

Prof L.J. Theo
Chair: Research Ethics Committee
Faculty of Informatics and Design
Cape Peninsula University of Technology

APPENDIX D: TURNITIN REPORT



Ierefaan Thesis (28 Jan 25)

ORIGINALITY REPORT

8%	7%	6%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	etd.cput.ac.za Internet Source	1%
2	Submitted to University of Iowa Student Paper	<1%
3	ru.wikipedia.org Internet Source	<1%
4	Paolo Di Francesco, Patricia Lago, Ivano Malavolta. "Architecting with Microservices: a Systematic Mapping Study", Journal of Systems and Software, 2019 Publication	<1%
5	Submitted to Anglia Ruskin University Student Paper	<1%
6	webarchive.nationalarchives.gov.uk Internet Source	<1%
7	mafiadoc.com Internet Source	<1%
8	hdl.handle.net Internet Source	<1%

APPENDIX E: EDITING CERTIFICATE

DR PATRICIA HARPUR

B.Sc Information Systems Software Engineering, B.Sc Information Systems (Hons)
M.Sc Information Systems, D.Technology Information Technology

Editing Certificate

---

19 Keerweder Street
Vredelust
Bellville
7945

083 7308540
doc@getthatresearchdone.com

To Whom It May Concern

This document certifies I have copy-edited the following dissertation by Ierefaan Batchelor:

DATA PRIVACY MANAGEMENT BEHAVIOUR OF SOCIAL MEDIA USERS IN SOUTH AFRICA

Please note this certificate does not cover any content, conceptual organisation, or textual changes made after the editing process.

Best regards

Dr Patricia Harpur

7 February 2025
