

**Development of a diagnostic instrument and privacy
model for student personal information privacy
perceptions at a Zimbabwean university**

By

**Kudakwashe Maguraushe
(61945218)**

submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY

in the subject

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Professor Adéle da Veiga

CO-SUPERVISOR: Professor Nico Martins

2021

DEDICATION

This thesis is dedicated to my parents and family, without whose support and motivation, this would not have been possible.

DECLARATION

I hereby declare that this document, **Development of a diagnostic instrument and privacy model for student personal information privacy perceptions at a Zimbabwean university**, submitted for evaluation towards the requirements of the subject: **INFORMATION SYSTEMS**, as part of the Doctor of Philosophy qualification at the University of South Africa, is my own original work and has not previously been submitted to any other institution of higher learning or subject for evaluation. All sources used or quoted in this document are indicated and acknowledged by means of a comprehensive list of references.

Surname, Initials: **Maguraushe K.**

Student Number: **61945218**

Signature



Date: **17/05/2021**

ACKNOWLEDGEMENTS

Thank you, Lord, for granting me the strength, peace and knowledge to conduct and complete this study. I don't remember you disappointing me!

I would also like to express my deepest gratitude towards my supervisors, Prof Adéle da Veiga and Prof Nico Martins. Thank you for your profound guidance, encouragement and motivation, all which cannot be expressed through any metaphorical words. It was a privilege to be regarded your student. You were always by my side throughout this academic journey.

Secondly, I am grateful to the UNISA M+D bursary department for the financial support during my PhD journey. Execution of the research activities became less of a burden due to their financial backup. To Dr. Ellen and Organisation Diagnostics, I am grateful for the successful hosting of my survey. I am also grateful to Dr. Liezel Korf and Liezel Korf Associates for their assistance in data analysis. You all made the journey less stressing.

Thirdly, I would like to thank my family. I am grateful to my wife Loice, who had to endure my long working hours. She tolerated and cooperated by giving me the spinal support during my 4-year journey. To my three kids: Tanaka, Laura and Layla, I thank God for you and for understanding that dad was working. You kept me motivated and you are the reason behind my smile. May the Almighty grant you wisdom to rule and conquer in all spheres of your lives. My parents, Edson and Precious have been the main driving force behind my educational journey. I thank you. I do not forget my young brother Kudzanai; I am grateful for the financial support throughout the course of my journey.

Last, but definitely not the least, I am appreciative to my workmates and colleagues. Many thanks to my coordinator Dr. Meshack Muderedzwa for the moral support and advice during the journey. I am also grateful to these colleagues: Tafadzwa Joseph Dube, Khesani R. Chilumani, Lario Malungana, Emmanuel Freeman, Belinda Mutunhu Ndlovu, Paul Nemashakwe and Dr. Sydney Machokoto for their moral support and encouragement. Your words were sources of energy for continuity.

To God be the glory! Great things He has done!

ABSTRACT

Orientation: The safety of any natural being with respect to the processing of their personal information is an essential human right as specified in the Zimbabwe Data Protection Act (ZDPA) bill. Once enacted, the ZDPA bill will affect universities as public entities. It will directly impact how personal information is collected and processed. The bill will be fundamental in understanding the privacy perceptions of students in relation to privacy awareness, privacy expectations and confidence within university. These need to be understood to give guidelines to universities on the implementation of the ZDPA.

Problem Statement: The current constitution and the ZDPA are not sufficient to give organisations guidelines on ensuring personal information privacy. There is need for guidelines to help organisations and institutions to implement and comply with the provisions of the ZDPA in the context of Zimbabwe. The privacy regulations, regarded as the three concepts (awareness, expectations and confidence), were used to determine the student perceptions. These three concepts have not been researched before in the privacy context and the relationship between the three concepts has not as yet been established.

Research purpose: The main aim of the study was to develop and validate an Information Privacy Perception Survey (IPPS) diagnostic tool and a Student Personal Information Privacy Perception (SPIPP) model to give guidelines to universities on how they can implement the ZDPA and aid universities in comprehending student privacy perceptions to safeguard personal information and assist in giving effect to their privacy constitutional right.

Research Methodology: A quantitative research method was used in a deductive research approach where a survey research strategy was applied using the IPPS instrument for data collection. The IPPS instrument was designed with 54 items that were developed from the literature. The preliminary instrument was taken through both the expert review and pilot study. Using the non-probability convenience sampling method, 287 students participated in the final survey. SPSS version 25 was used for data analysis. Both descriptive and inferential statistics were done. Exploratory factor analysis (EFA) was used to validate the instrument while confirmatory factor analysis (CFA) and the structural equation modelling (SEM) were used to validate the model.

Main findings: diagnostic instrument was validated and resulted in seven new factors, namely university confidence (UC), privacy expectations (PE), individual awareness (IA), external awareness (EA), privacy awareness (PA), practice confidence (PC) and correctness expectations (CE). Students indicated that they had high expectations of the university on privacy. The new factors showed a high level of awareness of privacy and had low confidence in the university safeguarding their personal information privacy. A SPIPP empirical model was also validated using structural equation modelling (SEM) and it indicated an average overall good fit between the proposed SPIPP conceptual model and the empirically derived SPIPP model

Contribution: A diagnostic instrument that measures the perceptions (privacy awareness, expectations and confidence of students) was developed and validated. This study further contributed a model for information privacy perceptions that illustrates the relationship between the three concepts (awareness, expectations and confidence). Other universities can use the model to ascertain the perceptions of students on privacy. This research also contributes to improvement in the personal information protection of students processed by universities. The results will aid university management and information regulators to implement measures to create a culture of privacy and to protect student data in line with regulatory requirements and best practice.

Keywords: confirmatory factor analysis; correctness expectations; diagnostic instrument; exploratory factor analysis; external awareness; individual awareness; practice confidence; perceptions; personal information; privacy; privacy education; privacy expectations; instrument; structural equation modelling; university confidence

TABLE OF CONTENTS

DEDICATION.....	ii
DECLARATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT.....	v
TABLE OF CONTENTS.....	vii
TABLE OF FIGURES.....	xv
LIST OF TABLES	xvi
LIST OF ABBREVIATIONS	xviii
CHAPTER ONE: SCIENTIFIC ORIENTATION OF THE RESEARCH.....	1
1.1 INTRODUCTION	2
1.2 BACKGROUND	2
1.3 PROBLEM STATEMENT.....	5
1.4 RESEARCH QUESTIONS AND OBJECTIVES	8
1.4.1 Main research question	8
1.4.2 Theoretical research questions.....	8
1.4.3 Empirical research questions.....	8
1.5 AIMS.....	9
1.5.1 Main research aim	9
1.5.2 Literature review aims.....	9
1.5.3 Empirical study aims.....	10
1.6 RESEARCH METHODOLOGY.....	10
1.6.1 Research paradigm	11
1.6.2 Research method	11
1.6.3 Research strategy.....	11
1.6.4 Research instruments and sampling.....	12
1.6.5 Reliability and validity	12
1.6.6 Data management	13
1.6.7 Data analysis	13
1.6.8 Ethical considerations.....	13
1.7 SIGNIFICANCE AND CONTRIBUTION OF THE STUDY	14

18 SCOPE	15
1.9 ORGANISATION OF THE THESIS	16
1.10 CHAPTER SUMMARY	17
CHAPTER TWO: PRIVACY, PRIVACY PRINCIPLES AND PRIVACY REGULATIONS ...	18
2.1 INTRODUCTION	18
2.2 OVERVIEW OF CHAPTER TWO	18
2.3 SCOPING REVIEW	20
2.3.1 Stages in the scoping review	21
2.3.2 Overview of existing research.....	24
2.3.2.1 Related privacy models.....	24
2.3.2.2 Privacy models in academia	26
2.3.2.3 Privacy awareness influence in compliance	27
2.3.2.4 Student privacy awareness, expectations and confidence	28
2.4 BACKGROUND OF PRIVACY AND PRIVACY PRINCIPLES	29
2.4.1 Privacy definitions.....	29
2.4.2 Personal information.....	32
2.4.3 Personal information processing.....	33
2.4.4 Privacy concerns	35
2.4.5 Privacy breaches	37
2.4.6 Privacy paradox.....	40
2.4.7 Privacy compliance.....	41
2.5 INTERNATIONAL PRIVACY REGULATIONS AND GUIDELINES.....	43
2.5.1 The Fair Information Practice Principle (FIPPs).....	43
2.5.2 The Organisation for Economic Cooperation and Development (OECD) Protection of Privacy and Transborder Flows of Personal Data	47
2.5.3 The General Data Protection Regulation (GDPR)	50
2.6.1 Aims of the GDPR.....	50
2.6.2 Relevance of GDPR in this study.....	51
2.6 ZIMBABWE DATA PROTECTION ACT (ZDPA).....	52
2.6.1 The Data Protection Authority of Zimbabwe	53
2.6.2 Principles of the Data Protection Act bill.....	53
2.6.3 Roles of the data controller.....	54
2.6.4 Rights of data subjects	54

2.7 Comparison of the ZDPA bill with the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data and the GDPR	55
2.7.1 FIPPs as the baseline for privacy model formulation	57
2.8 CHAPTER SUMMARY	59
CHAPTER THREE: INFORMATION PRIVACY PERCEPTION CONCEPTUAL MODEL..	60
3.1 INTRODUCTION	60
3.2 CHAPTER OVERVIEW	60
3.3 INFORMATION PRIVACY PERCEPTIONS	62
3.3.1 Overview of information privacy perceptions	62
3.3.2 The social contract theory on privacy	64
3.4 PRIVACY WITHIN UNIVERSITY – STUDENT CONTEXT (THE THREE CONCEPTS)	
65	
3.4.1 Student privacy awareness.....	66
3.4.2 Student privacy expectations.....	70
3.4.3 Student confidence in the university	72
3.5 PRIVACY COMPONENTS	76
3.5.1 Notice/ Openness	76
3.5.2 Information quality	78
3.5.3 Purpose specification.....	78
3.5.4 Use limitation	79
3.5.5 Collection limitation.....	80
3.5.6 Individual participation / choice	81
3.5.7 Additional components	83
3.5.7.1 Privacy policy	84
3.5.7.2 Privacy education.....	86
3.5.7.3 Consent.....	87
3.6 CONSOLIDATED PRIVACY COMPONENTS FOR THE MODEL.....	89
3.6.1 Inclusion criterion into the SPIPP conceptual model.....	91
3.6.2 Measurement perspective	91
3.7 THE STUDENT PERSONAL INFORMATION PRIVACY PERCEPTION (SPIPP) MODEL.....	94
3.8 THE INFORMATION PRIVACY PERCEPTION INSTRUMENT	96
3.9 CHAPTER SUMMARY	100

CHAPTER FOUR: RESEARCH METHODOLOGY.....	101
4.1 INTRODUCTION	101
4.2 CHAPTER OVERVIEW	101
4.3 DEFINITION OF RESEARCH METHODOLOGY.....	103
4.4 RESEARCH PHILOSOPHY.....	104
4.5 RESEARCH APPROACHES.....	106
4.6 RESEARCH DESIGN	107
4.7 RESEARCH STRATEGY.....	109
4.8 TIME HORIZON.....	112
4.9 POPULATION AND SAMPLING.....	112
4.9.1 Sample design.....	112
4.9.2 The sample and population	113
4.9.3 The sample size.....	113
4.9.4 Sampling technique	114
4.10 DATA COLLECTION: SURVEY DEVELOPMENT PROCESS	116
4.10.1 Data collection instrument	116
4.10.2 Instrument design and construction	117
4.10.3 Instrument refinement process	120
4.10.4 Structure of the IPPS survey instrument.....	122
4.10.4.1 Section 1: Biographical information.....	122
4.10.4.2 Section 2: Personal information privacy perception statements	124
4.10.4.3 Description of the scale.....	126
4.10.4.4 General information for survey completion.....	127
4.10.5 Instrument finalisation.....	127
4.10.5.1 Expert review	128
4.10.5.2 Pilot study	135
4.10.6 Data collection and administering the survey	137
4.10.7 Reliability	138
4.10.8 Validity	140
4.11 DATA ANALYSIS.....	142
4.11.1 Data management	142
4.11.2 Descriptive statistics	143
4.11.3 Inferential statistics	143

4.11.3.1 The t-test.....	144
4.11.3.2 The Analysis of Variance	144
4.11.3.3 Correlation analysis.....	145
4.11.3.4 Spearman's correlation	146
4.11.4 Factor analysis.....	147
4.11.4.1 Exploratory factor analysis (EFA).....	147
4.11.4.2 Confirmatory factor analysis (CFA)	150
4.11.5 Structural equation modelling (SEM)	153
4.12 RESEACH HYPOTHESES FORMULATION	153
4.13 ETHICAL CONSIDERATIONS.....	156
4.14 CHAPTER SUMMARY	158
CHAPTER FIVE: RESEARCH RESULTS	159
5.1 INTRODUCTION	159
5.2 BIOGRAPHICAL STATISTICS	161
5.2.1 Survey responses.....	161
5.2.2 Gender distribution	162
5.2.3 Nationality distribution.....	162
5.2.4 Mode of study distribution.....	163
5.2.5 Year of study distribution	164
5.2.6 Programme distribution.....	165
5.3 EXPLARATORY FACTOR ANALYSIS (EFA).....	166
5.3.1 Communalities.....	166
5.3.2 Sample adequacy and sphericity.....	167
5.3.3 Determining the internal consistency of scale.....	171
5.3.4 Adoption of new factors	173
5.3.4.1 Final factors.....	173
5.3.5 Reliability of the instrument.....	175
5.3.6 Means and standard deviations of the factors' interpretation.....	177
5.4 INFERENCEIAL STATISTICS.....	180
5.4.1 Confirmatory factor analysis (CFA).....	180
5.4.2 Structural equation modelling (SEM)	192
5.4.3 Pearson product moment correlation coefficient between variables	195
5.4.4 Testing for group mean differences	199

5.4.4.1 Gender	199
5.4.4.2 Age.....	199
5.4.4.3 Mode of study.....	200
5.4.4.4 Programme of study.....	200
5.4.4.5 Year of study	202
5.5 CONCLUSION ON RESEARCH HYPOTHESES	203
5.6 CHAPTER SUMMARY	205
CHAPTER SIX: CONCLUSION, LIMITATIONS AND RECOMMENDATIONS	207
6.1 INTRODUCTION	208
6.2 REFLECTION OF THE STUDY	208
6.2.1 Discussion of research aims relating to literature review:	208
6.2.1.1 <i>To conceptualise privacy awareness of students from a theoretical perspective.....</i>	209
6.2.1.2 <i>To conceptualise privacy expectations of students from a theoretical perspective.....</i>	210
6.2.1.3 <i>To conceptualise student confidence in academic institutions from a theoretical perspective.</i>	211
6.2.1.4 <i>To develop a conceptual model of privacy awareness, expectations and confidence of students from a theoretical perspective.</i>	212
6.2.2 Discussion of research aims relating to empirical study:	213
6.2.2.1 <i>Research objective 1: To develop a privacy perception instrument measuring privacy awareness, expectations and confidence of students.....</i>	213
6.2.2.2 <i>Research objective 2: To validate the instrument using factor and item analysis.....</i>	214
6.2.2.3 <i>Research objective 3: To determine the expectations of students when the university processes their personal information.</i>	214
6.2.2.4 <i>Research objective 4: To determine the privacy awareness levels of students when the university processes their personal information.....</i>	215
6.2.2.5 <i>Research objective 5: To determine the privacy confidence levels of students in the university observing privacy of their personal information.</i>	216
6.2.2.6 <i>Research objective 6: To determine the relationship between the 3 concepts (expectations, awareness and confidence) using correlation analysis.....</i>	216

6.2.2.7 <i>Research objective 7: To validate the model using structural equation modelling (SEM).</i>	218
6.2.2.8 <i>Research objective 8: To determine whether different biographical variables influence privacy awareness, expectations and confidence of students.</i>	222
6.2.2.9 <i>Research objective 9: To make recommendations to improve the information privacy perceptions on the basis of the findings of this research.</i>	224
6.2.3 Conclusions regarding the hypotheses	225
6.3 LIMITATIONS	226
6.3.1 Literature review limitations	226
6.3.2 Empirical study limitations	227
6.4 RECOMMENDATIONS	228
6.4.1 Recommendations for universities	228
6.4.2 Recommendations for future research	230
6.5 CONTRIBUTIONS	231
6.5.1 Theoretical level contribution	231
6.5.2 Empirical contribution	232
6.5.3 Practical contribution	233
6.6 CHAPTER SUMMARY	234
REFERENCE LIST	236
INDEX OF APPENDICES	264
Appendix A: Ethical clearance approval	264
A1: Humans Ethical Clearance	264
A2: Non-Humans Ethical Clearance	266
Appendix B: Approval letter for research	268
Appendix C: Participation information sheet:	270
C1: Expert panel participation information sheet	270
C2: Pilot group participation information sheet	274
Appendix D: Consent to participate form	278
D1: Expert panel consent form	278
D2: Pilot study participation form	279
Appendix E: Questionnaires	280
E1: Expert review information privacy perceptions questionnaire	280
E2: Pilot study information privacy perceptions questionnaire	291
E3: Final questionnaire for the survey (HTML format)	300

Appendix F: Initial communalities for the 54 items.....	320
Appendix G: Summarised rotated pattern matrix for the eight-factors	324
Appendix H: Correlation results	326
Appendix I: Independent t-test for gender.....	327
Appendix J: ANOVA test for age	328
Appendix K: ANOVA test for mode of study	330
Appendix L: Spearman's rho for year of study	332
Appendix M: ANOVA test for programme of study	333
Appendix N: Author's publications	335
N1: Validation of an information privacy perception instrument at a Zimbabwean university.....	336
N2: A conceptual framework for student personal information privacy culture in Zimbabwe universities.....	351
Appendix O: Editors Certificate.....	365

TABLE OF FIGURES

Figure 1.1: Chapter Overview	1
Figure 2.1: Chapter summary	19
Figure 2.2: Search phases on student privacy awareness, expectations and confidence .	23
Figure 2.3: Different privacy definitions.....	31
Figure 2.4: Fundamental FIPPs	44
Figure 3.1: Chapter summary flow chart.....	61
Figure 3.2: Conceptual model for privacy concepts	66
Figure 3.3: Privacy components of the SPIPP	93
Figure 3.4: The SPIPP conceptual model for a university	95
Figure 4.1: Chapter summary flowchart diagram	102
Figure 4.2: The research onion	104
Figure 4.3: Instrument design and sampling.....	121
Figure 4.4: Error detection rates	129
Figure 5.1: Chapter summary flowchart diagram	160
Figure 5.2: Scree plot graph	168
Figure 5.3: Mean values for the factors.....	178
Figure 5.4: Model fit for university confidence.....	180
Figure 5.5: Model fit for privacy expectations.....	182
Figure 5.6: Model fit for individual awareness.....	184
Figure 5.7 Model fit for individual awareness.....	186
Figure 5.8 Model fit for correction expectation	188
Figure 5.9 Model fit for external awareness.....	190
Figure 5.10: Model fit for privacy education	191
Figure 5.11: Model fit for information privacy perceptions.....	193
Figure 6.1: Chapter summary flowchart diagram	207
Figure 6.2: Final validated information privacy model	219

LIST OF TABLES

Table 2.1: Examples of personal information that universities process.....	34
Table 2.2: Summary of the ZDPA bill sections in alignment with FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data and GDPR sections	56
Table 2.3: Summary of privacy components grounded on FIPPs guidelines	58
Table 3.1: Consolidated privacy components	89
Table 3.2: Summary of information privacy perceptions questions	97
Table 4.1: Components and allocated items	125
Table 4.2: Expert panel participants	130
Table 4.3: Summary of expert review.....	132
Table 4.4: CFA model fit measurements, descriptions and acceptable fit of variables	151
Table 4.5: Research hypotheses	154
Table 5.1: Age categories	161
Table 5.2: Gender distribution.....	162
Table 5.3: Nationality distribution.....	163
Table 5.4: Mode of study distribution	163
Table 5.5: Year of study distribution	164
Table 5.6: Programme distribution.....	165
Table 5.7: Sample adequacy and significance.....	167
Table 5.8: Total variance with Eigenvalues.....	169
Table 5.9: Rotated pattern matrix for the 8-factor model.....	171
Table 5.10: Cronbach alpha values and inter-item correlations per factor	176
Table 5.11: Descriptive statistics	177
Table 5.12: Model fit indices for university confidence.....	181
Table 5.13: Model fit indices for privacy expectations.....	183
Table 5.14: Model fit indices for individual awareness.....	185
Table 5.15: Model fit indices for practice confidence	187
Table 5.16: Model fit indices for correction expectation	189
Table 5.17: Summary of information privacy perception model fit indices	191
Table 5.18: Model fit for information privacy perceptions.....	194
Table 5.19: Summary of practically significant factors using the Pearson correlation.....	196
Table 5.20: ANOVAs and post hoc test for program of study	201
Table 5.21: Spearman correlation for year of study	202

Table 5.21: Summary of research hypotheses203

LIST OF ABBREVIATIONS

ABBREVIATION	TERMS IN FULL
CFA	Confirmatory Factor Analysis
CE	Correctness Expectations
EFA	Exploratory Factor Analysis
EA	External Awareness
FIPPs	Fair Information Privacy Principles
GDPR	General Data Protection Regulation
IA	Individual Awareness
IPPS	Information Privacy Perception Survey
OECD	Organisation of Economic Cooperation and Development
PC	Practice Confidence
PA	Privacy Awareness
PE	Privacy Expectations
SPIPP	Student Personal Information Privacy Perception
SEM	Structural Equation Modelling
UC	University Confidence
ZDPA	Zimbabwe Data Protection Act bill

For citations and references, **APA 6** referencing style was used throughout this thesis.

CHAPTER ONE: SCIENTIFIC ORIENTATION OF THE RESEARCH

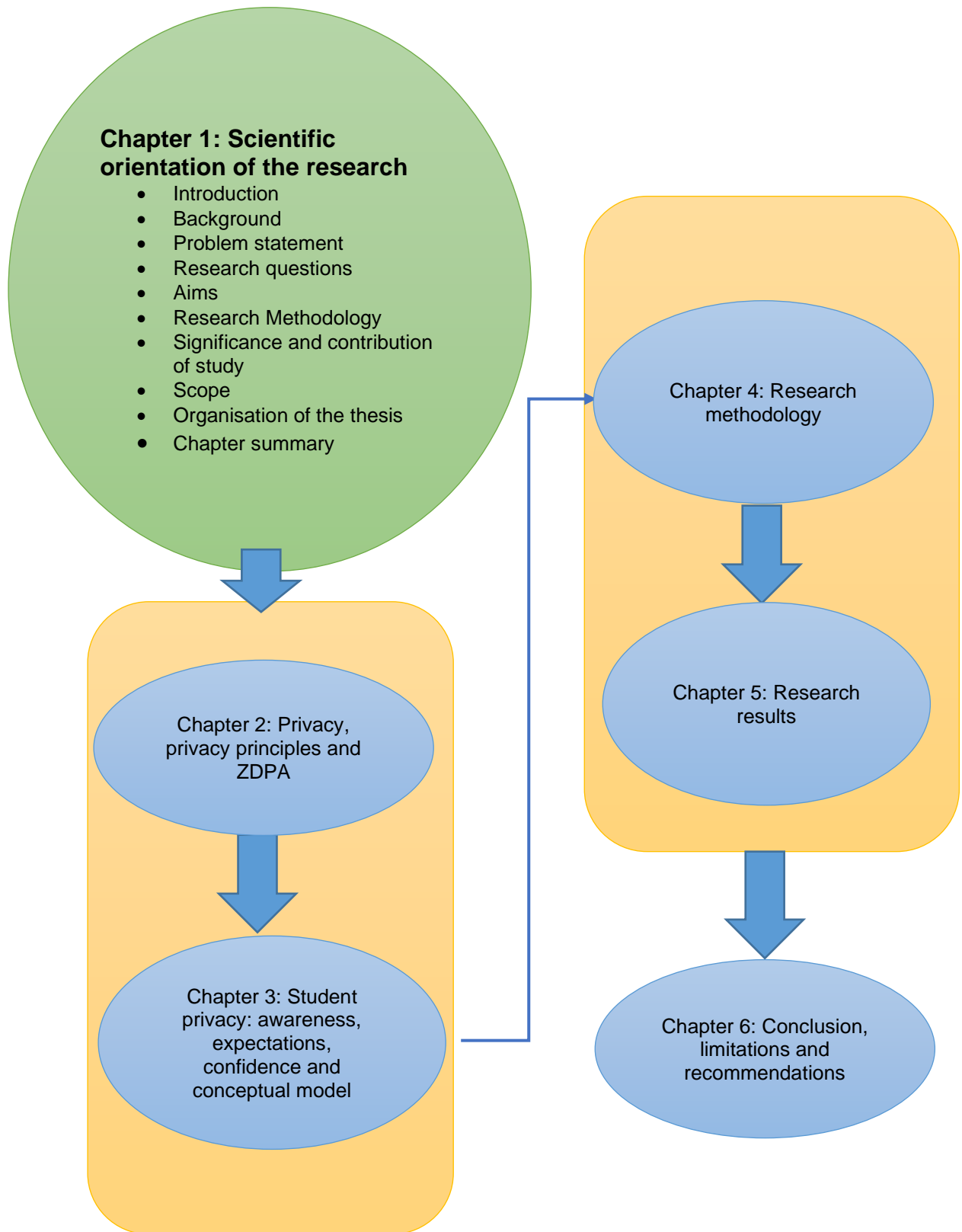


Figure 1.1: Chapter Overview (Source: Researcher's compilation)

1.1 INTRODUCTION

This research focused on developing a diagnostic instrument and model for information privacy perceptions of students in Zimbabwean universities. In this study, privacy perceptions refers to perceptions about student privacy awareness, privacy expectations and the confidence levels of students regarding universities' capability to uphold privacy. Privacy is a major issue in information systems. Information systems looks at the components used for the collection, storage, processing and dissemination of data to provide information and eventually knowledge, in an organisational setting, according to Boell and Cecez-Kecmanovic (2015). The privacy of such data/ information is critical within an organisation and failure by the organisation to prioritise privacy will result in privacy breaches and consequently, litigations. With the need to protect personal data, an organisation must come up with control measures on how they will use personal information as part of their organisational goals in information systems (Chen & Ismail, 2013).

This chapter provides the background of the study, leading to the problem statement, research questions and associated research objectives and related deliverables. It also provides an outline of the relevance of the study, together with its contribution to the body of knowledge. A summary of the research model that include the research philosophy, approach, design, strategy, together with a summary of the data gathering techniques used in this research and ethical considerations of the research are done in this chapter. The chapter concludes by giving an overview of the thesis outline and a chapter summary.

1.2 BACKGROUND

Perceptions on information privacy differ from one country to the other (Chua, Herbland, Wong & Chang, 2017). In the Zimbabwean context, the protection that is afforded to a natural person with respect to the their personal information processing is perceived to be an essential human right (Zimbabwe Constitution, 2013). The right to privacy is treasured in the Zimbabwean Constitution (Clause 57, part 2 of Chapter 4), which declares that, *"Every person has the right to privacy, which includes the right not to have a) their home, premises or property entered without permission; b) their person, home, premises or property searched; c) their possession seized; d) the*

privacy of their communication infringed; or e) their health condition disclosed (Zimbabwe Constitution, 2013 p.30). Unfortunately, it does not state how the privacy of personal information will be enforced. There are existing pieces of legislation in Zimbabwe that have an influence on the right to privacy and the personal information protection, but these are limited to specified data types, or specific activities.

Zimbabwe is in the progression of enacting the Zimbabwe Data Protection Act (ZDPA) as a specific legal document to guide and protect privacy of personal information for individuals, institutions, organisations and people. However, the law has not yet taken effect. The ZDPA is particular on how public and private entities process personal information while safeguarding against the unlawful collection and the subsequent use of personal information (Chetty, 2013).

Universities are examples of public entities and therefore the ZDPA will apply to how they process personal information. They will require guidance to implement the conditions of the ZDPA, which guidance has not been issued as yet in Zimbabwe. A stakeholder report review by the Digital Society of Zimbabwe, the Zimbabwe Human Rights NGO Forum, the Privacy International and the International Human Rights Clinic at the Harvard Law, bemoans the lack of data protection legislation in Zimbabwe (Stakeholder Review, 2016). In fact, Ncube (2016) is of the opinion that the current legislative pieces on privacy in Zimbabwe do not meet the regional and international expectations on data protection principles. The absence of such legislation and of a precise guideline on data protection mechanisms is deemed a threat to the right to privacy (OpenNet Africa, 2016). To reduce such potential threats to information privacy, a data privacy model can guide universities, an example being the privacy model for e-learning implementation (Ivanova, Grosseck & Holotescu, 2015). Therefore, a privacy model could be helpful within the university context to foster positive perceptions on privacy.

It is also imperative that organisations prioritise meeting customers' privacy expectations and that they do so in line with the minimum accepted privacy requirements (Da Veiga & Ophoff, 2020). Either meeting or violating the privacy expectations of customers by the organisation will greatly impact on trust (and hence confidence) by the customers (Martin, 2018). In situations where consumers (students) develop perceptions that their personal information has been compromised

negatively, they tend to also respond in a negative manner (Schwaig et al., 2013). The negative perceptions of students about privacy of their personal information can be addressed by increasing their awareness through education and sensitising them of their personal data protection (Chen & Ismail, 2013). Failure to comprehend students' perceptions on their personal data privacy can be one of the causes of mayhem in personal data protection. Therefore, awareness and training are elementary to the accomplishment of any information privacy initiative and in creating positive privacy perceptions. Martin's (2018) study indicated that meeting the privacy expectations results in positive perceptions. Students will develop positive perceptions with a university when it processes their personal information in line with their expectations, which reduces privacy breaches.

If an organisation (or a university) complies with the requirements of the regulations and protect the personal information of their customers (students), trust can be developed (Da Veiga, 2017). A follow up research by Da Veiga (2018b) concluded that South African consumers (students) have low confidence in the organisations (institutions) complying with regulatory and privacy guidelines and that trust is key in confidence build-up. In terms of expectations, not only does observing the privacy expectations of consumers (students) increase their buying intentions and the consumers' (students') possibility of transacting with an organisation (Eastlick, Lotz & Warrington, 2006; Fortes & Rita, 2016), but also trust in the organisation (McKnight, Choudhury, & Kacmar, 2002; Martin, 2015).

In a society, there are certain mutually beneficial agreements that communities naturally develop about how to use and share their personal information (Kruikemeier et al., 2020; Martin, 2015). This phenomenon is termed the social contract theory. Martin (2015) indicates that social contracts can be so powerful that they can never be understood by an outsider. Evidently, people attach privacy expectations based on these social contracts and the organisations will have to adequately manage such privacy expectations from their stakeholders (Bandara, Fernando & Akter, 2020; Casman, 2011; Martin, 2015). The reasonable expectations about privacy (social contract) emerge when people socialise, make relationships or trade based on some norms (Bandara et al., 2020). It is imperative to understand if organisations are adequately managing the expectations on privacy of their stakeholders (Martin, 2015), which are students in this study. People (in this case students) have high confidence

(positive perceptions) with the social contract theory in the safe handling and usage of their personal information, but once they develop any privacy concern, they can withdraw from sharing (Kruikemeier et al., 2020).

Since the social contract theory can be used to ascertain if organisations are meeting the expectations perceptions of students, one can use the same to analyse their awareness perceptions. Meeting customers' privacy expectations can propagate trust, which will ultimately lead to positive privacy confidence perceptions on the organisation as posited by Martin (2015). Therefore, in acknowledging the social contracts approach to privacy of information, people's (students') perceptions will be grounded on what they know pertaining to privacy (**awareness**), what they reasonably expect from the organisations (institutions) pertaining to personal information privacy (**expectations**) and these will stimulate trust (Huang & Bashir, 2016) and hence **confidence** in the organisation. These are the three concepts that formulate the privacy perceptions under study in this research.

The three concepts are analysed alongside the research aim in determining if these have an impact on the information privacy perceptions. The impact of perceptions on privacy is such that they can alter individuals' behaviour and attitude (Schwaig et al., 2013). Schwaig et al. (2013) submit that consumers' (students') perceptions are likely to be negative if they develop a feeling that the privacy of their personal information has been invaded and infringed in any way. While the ZDPA is not in effect yet, individuals have privacy perceptions about how their personal information should be protected. A privacy model can aid and guide privacy perceptions and compliance (Kyobe, 2010b).

1.3 PROBLEM STATEMENT

The increasing reliance on technology in storing and communicating personal information in this digital age has subsequent led to an increase in privacy breaches and the economic and social impact of these cannot be ignored (Aghasian, Garg & Montgomery, 2020; Feri, Giannetti & Jentzsch, 2016; Kokolakis, 2017; Mamonov & Benbunan-fich, 2018; Mikhed & Vogan, 2018; Okazaki, Eisend, Plangger, Ruyter & Grewal, 2020; Patsakis, Charemis, Papageorgiou, Mermigas & Pirounias, 2018; Wheatley, Hofmann & Sornette, 2019). Unfortunately, this might also affect

universities. As reported by Feri et al. (2016), there are many reports of disclosure without consent of a person's personal information, which is a direct violation of their privacy rights and consequently a breach of privacy.

Using the Zimbabwean context, universities lack a diagnostic instrument and an information privacy perception model to measure privacy perceptions on how personal information has to be processed and stored. There are no privacy guidelines as yet to help organisations and institutions in implementing and complying with the provisions of the privacy regulation. The current constitution and the ZDPA are not sufficient to give organisations guidelines on the implementation of personal information privacy. As indicated earlier, universities are considered public entities and the ZDPA will be applicable to them in students' personal information processing, to help restrain the increasing privacy breaches.

The privacy breaches can be ascribed to the use of many sophisticated tools, techniques and equipment in the digital age (Mamonov & Benbunan-Fich, 2015). Privacy breaches need better safeguarding ways and require the development of incident response plans in order to protect privacy (OECD, 2013b). The privacy breaches are also regarded as an obligation of those who must be safeguarding the data (Iachello & Hong, 2007; Okazaki et al., 2020). In this research, the university is the safeguarding establishment and it responsible for implementing the ZDPA. Universities fail to follow proper privacy procedures, resulting in data breaches, and this happens when universities fail to put in place proper training and awareness for their employees. Breaches are also a result of lack of adequate rules to govern personal data access and over-collection of data among other causes (OECD, 2013b). Some breaches are due to the organisation lacking internal controls on how personal information should be used (Ackerman & Mainwaring, 2005; Martin et al., 2020).

Various researchers have conducted several empirical studies focusing on privacy concepts, for example privacy in the online context (Miltgen, 2009; Mohamud, Saidin & Zeki, 2017; Salleh, Hussein, Mohamed & Aditiawarman, 2013), privacy in the student expectations context (Ivanova et al., 2015; Kumaraguru & Cranor, 2005; Talib et al., 2014), privacy in the student awareness context (Chen & Ismail, 2013; Lawler & Molluzzo, 2011; Malandrino et al., 2013) or regulatory compliance with the laws on privacy (Almadhoun, Dominic & Woon, 2011; Chua et al., 2017). From the literature,

there appears to be no research pointing to focus on the university-student context assimilating the three concepts proposed in this study based on the social contract theory on privacy perceptions. These are privacy expectations, privacy awareness and confidence in the university to meet privacy expectations to aid in complying with privacy regulatory requirements. Research indicates lack of models that consider all the three concepts.

In summary, in reviewing current literature on student personal information privacy perceptions in Zimbabwe, the following research problems are highlighted;

- The ZDPA does not give guidance on how to implement the conditions of the privacy of personal information but focusses on privacy principles and regulations (Chetty, 2013; Ncube, 2016; Zimbabwe Data Protection Act Bill, 2013). Indeed, it is not the role of legislation to give guidance on how it might be implemented in an organisational setting but having a model that aid in privacy practice would be more ideal for privacy compliance.
- Research has shown that consumers (students) do not always trust nor have confidence in organisations processing their personal information in line with privacy principles and guidelines (Chua et al., 2017; Da Veiga & Ophoff, 2020; Fortes & Rita, 2016; Huang & Bashir, 2016; Kruikemeier et al., 2020). Similarly, students might not trust or have confidence in universities protecting their privacy, especially where there are no implementation guidelines.
- The presence and increase of privacy breaches in the digital environment (Anjum et al., 2018; Bush, 2016; Chua et al., 2017; Kafali et al., 2017; Mamonov & Benbunan-Fich, 2015; Martin et al., 2020; Ruyter & Grewal, 2020) is a cause for concern and a threat to the privacy of students' personal information. In fact, privacy is considered a fundamental problem that has to be addressed, especially in this growing digital world (Fatima et al., 2019; Kokolakis, 2017).
- Universities do not know what students expect from the institution on privacy (Callanan, Jerman-Blažič & Blažič, 2016; Degroot & Vik, 2017; Dwyer & March, 2016; Krzych & Ratajczyk, 2013; Schumacher & Ifenthaler, 2018). A privacy model can give guidelines to universities on privacy implementation and can aid universities to better understand student privacy perceptions.

1.4 RESEARCH QUESTIONS AND OBJECTIVES

The main research question, theoretical and empirical questions are highlighted below.

1.4.1 Main research question

The main research question that guided this study is:

- *What are the key components that constitute the personal information privacy perceptions in the Zimbabwean university context?*

To answer this question, some sub-questions needed to be explored and investigated. These were divided into theoretical research questions and empirical research questions. The questions were centred on elucidating the three main concepts i.e., the student **awareness**, their **expectations** and their **confidence** on the university upholding their personal information privacy.

1.4.2 Theoretical research questions

The following research questions were articulated based on the literature review:

- i. Based on the literature, how can privacy awareness of students be conceptualised?
- ii. Based on the literature, how can privacy expectations of students be conceptualised?
- iii. Based on the literature, how can student confidence in academic institutions be conceptualised?
- iv. Based on the literature review, can a theoretical model of privacy awareness, expectations and confidence of students be developed?

1.4.3 Empirical research questions

The following research questions were formulated in terms of the empirical study:

- i. How can an instrument that measures privacy awareness, expectations and confidence of students be developed?
- ii. How can the privacy perception instrument be validated?
- iii. What are the privacy expectations of students when the university processes their personal information?
- iv. What are the privacy awareness levels of students when the university processes their personal information?
- v. What are the privacy confidence levels of students in the university processing their personal information?
- vi. What is the empirical relationship between privacy awareness, expectations and confidence of students?
- vii. How is the information privacy perception model validated?
- viii. Do different biographical variables influence privacy awareness, expectations and confidence of students?
- ix. What recommendations can be made to improve the information privacy perceptions of Zimbabwean students in universities?

1.5 AIMS

Based on the research questions above, the following research aims were formulated – main research aim, literature review aims and empirical study aims:

1.5.1 Main research aim

The main aim of the study was to develop a diagnostic instrument and privacy model for student personal information privacy perceptions (awareness, expectations and confidence) in Zimbabwe

1.5.2 Literature review aims

This was considered as Phase 1: theoretical aims based on literature. The following aims were articulated for the literature review:

- i. To conceptualise privacy awareness of students from a theoretical perspective.

- ii. To conceptualise privacy expectations of students from a theoretical perspective.
- iii. To conceptualise student confidence in academic institutions from a theoretical perspective.
- iv. To develop a conceptual model of privacy awareness, expectations and confidence of students from a theoretical perspective.

1.5.3 Empirical study aims

In relation to the empirical study, the following research aims were formulated:

- i. To develop a privacy perception instrument measuring privacy awareness, expectations and confidence of students.
- ii. To validate the instrument using factor and item analysis.
- iii. To determine the expectations of students when the university processes their personal information.
- iv. To determine the privacy awareness levels of students when the university processes their personal information.
- v. To determine the privacy confidence levels of students in the university observing privacy of their personal information.
- vi. To determine the relationship between the three concepts (expectations, awareness and confidence) using correlation analysis.
- vii. To validate the model using structural equation modelling (SEM).
- viii. To determine whether different biographical variables influence privacy awareness, expectations and confidence of students.
- ix. To make recommendations to improve the information privacy perceptions on the basis of the findings of this research.

1.6 RESEARCH METHODOLOGY

In this section, a research methodology overview is discussed. The discussion is on the research paradigm, research method, research strategy, research instruments and sampling used, reliability and validity assessments and data collection. The data management, data analysis and also the ethical considerations in the research

process are also discussed in this section. The research methodology will further be expanded on in Chapter 4.

1.6.1 Research paradigm

The researcher used the *positivism* research paradigm. The main concern of this research is knowledge gaining through statistical inquiry to arrive at conclusions, based on the empirical results, i.e., uncovering of truth and presenting it by empirical means. Data analysis conclusions are used to provide evidence to dispel or support hypotheses (Greener, 2008; Riley-Tillman & Reinke, 2011). This is in line with the description of positivism in Kumar (2011) and Saunders et al. (2016).

1.6.2 Research method

A *quantitative research* method, using the survey method was also used. This is synonymous with a positivist method. Positivistic think-tanks adopt scientific procedures and systematise the process of generating knowledge with the aid of quantification to properly augment precision in the parameter description and all the relationships amongst them (Greener, 2008; Riley-Tillman & Reinke, 2011). The measurement and assessment of student privacy perceptions were done using quantitative means and the results were analysed statistically, as advocated by Creswell and Creswell (2018) and Gerber and Hall (2017).

1.6.3 Research strategy

Research strategy is considered a methodological connection between the philosophy and the choice of methods used in collecting and analysis of data (Neuman, 2014; Saunders et al., 2016) that gives the plan of action for achieving the objectives (Greener, 2008). Used in this study was a *survey*, which is defined as a scientific method for studying people's behaviour that would be difficult to experiment or observe directly (Davidson, 2004; Guerin & Dohr, 2005). A survey enabled the researcher to gather data about opinions, circumstances or practices.

1.6.4 Research instruments and sampling

Using *questionnaires (instruments)* as a data collection technique in the survey, at least 270 university students from various departments of one institution were invited to participate using a non-probability sampling technique of *convenience sampling* and were chosen based on their convenience and availability as sources of data (Cohen, Manion & Morrison, 2011; Salkind, 2017; Saunders et al., 2016; Tracy, 2013). The researcher also adopted the *purposive sampling* method for the expert review panel and the convenience sampling technique for piloting in the study. Instruments are ideal because they are developed based on some theoretical knowledge, as suggested by Muller (2014) and this was the circumstance in this study. After collecting data using the instruments during piloting, a survey was deployed in the electronic format using SurveyTracker software for a stipulated period.

1.6.5 Reliability and validity

Also ensured in this research were reliability and validity. As Tricco, Tetzlaff and Moher (2011) suggest, the reliability of the data can be increased by expert panel and pilot testing, and these were applied in this research. Cronbach alpha was applicable for calculating the internal consistency reliability for the study. Using the Cronbach alpha coefficients for an exploratory research like this, reliability is considered good for values above 0.8, considered acceptable for values between 0.6 and 0.8 and, finally, considered unacceptable for the values below 0.6 (Gerber and Hall, 2017).

Validity according to Kazi and Khalid (2012) and Gerber and Hall (2017), is the degree to which an assessment measures what it has to measure in relation to the investigation being made. In this research, face validity, content and construct validity were used. In addition, considering the fact that a new instrument was developed, content and construct validity were very important. In this research, pilot testing of the instrument increased the internal validity, leading to less ambiguity in the instrument (Oats, 2012). More so, face validity was achieved through expert reviews, which led to some adjustments being made. The instrument's validity was ensured by means of factor analysis.

1.6.6 Data management

According to Scantron (2018), the primary reason for using SurveyTracker is that it has an online tracking system and therefore data can easily be uploaded into an excel sheet or SPSS (and being imported into other formats like CSV, PDF, queXML). This data was stored electronically after its collection and SurveyTracker summarised data responses for every category, and this is used for data analysis.

1.6.7 Data analysis

After capturing the data using SurveyTracker, it was imported to SPSS for statistical analysis. Statistical reporting methods in this study include the use of descriptive statistical analysis of the mean, standard deviation, frequency and percentages among other methods. (Taylor-Powell & Hermann, 2000). Both the ANOVA and t-test analyse the spread of the data values (variance) between and within data by making comparison of a certain descriptive statistical feature i.e. the means of populations (Saunders et al., 2016). In addition, Saunders et al. (2016) suggested that a t-test can be used to test whether two categories or groups are different and ANOVA can be used to test the differences of the categories or groups if they are three or more.

To measure the strength of relationships that exist between the two variables, Pearson product moment correlation coefficient was used in this study (Saunders et al., 2016). It was used for the analysis of the variables' inter-factor association and for testing if the correlated variables are numeric and relatively symmetric (Rossiter, 2017; Saunders et al., 2016). For testing the group mean differences for the year of study, the Spearman correlation was used (Cohen et al., 2011). To do the validation of the model, the structural equation modelling (SEM) was used (Kline, 2011; Weston, 2018) and it is discussed in section 4.11.5 in Chapter Four.

1.6.8 Ethical considerations

Ethics are norms for conduct that differentiate acceptable and also unacceptable behaviour (Israel & Hay, 2006). Israel and Hay (2006) also suggest that an acceptable code of ethical conduct should be drawn before the commencement of any research work. Ethics were ensured in this research through getting an ethical clearance from

the University of South Africa (UNISA) before commencing the study, permitting the researcher to carry out the survey. Permission was also obtained from the university under study, granting the researcher permission to conduct the survey. The participant information letter was availed to the expert panel and pilot group to add more clarity on the nature of study, the participation requirements, anonymity, confidentiality and use of information. In turn, the expert panel and pilot group agreed with the informed consent for participation. Students were also given the option to consent to participate in the survey, with an option of signing out from participation without being compelled to give any reason.

1.7 SIGNIFICANCE AND CONTRIBUTION OF THE STUDY

The first contribution is the development of an Information Privacy Perception Survey (IPPS) diagnostic tool and a Student Personal Information Privacy Perception (SPIPP) model. The diagnostic instrument (IPPS) and the proposed model (SPIPP) can assist universities as a guideline package on how the university can implement the ZDPA and to understand student perceptions towards privacy and how they perceive the university in meeting privacy requirements. Student expectations and concerns can be addressed when the university uses the outcome to identify action plans in line with the developmental constructs identified. Student awareness will improve if the university conducts awareness programs that focus on the aspects identified in the survey, which the students were not aware of initially. The IPSS diagnostic instrument and SPIPP privacy model developed in the study can be re-validated and be used in other contexts or countries. This research provides the first validation of the instrument which would enable further research and use in other universities.

The second contribution is through suggestions and recommendations which are useful within the university domain in improving the privacy of student personal information. The information derived from the instrument can be used to understand expectations and areas where the university can improve privacy and the protection of student personal information. The instrument can be used to measure how aware of privacy students are and what their expectations are on privacy. The outcome can then be used by the university to develop action plans in line with the developmental constructs identified. This will enable the university to make students aware of their privacy rights and to align processing of their personal information with legal

requirements, as well as with students' privacy expectations. In addition, one of the most useful and unique contributions of this research is a SPIPP privacy model for the three constructs i.e., **student privacy awareness**, **student privacy expectations** and **student confidence in the university**. The SPIPP model will give privacy guidelines on the implementation of the ZDPA, based on the student perceptions.

The third significance of this research is its contribution towards student privacy literature body of knowledge on awareness, expectations and confidence boosting. Available literature shows research studies in either awareness, expectations or confidence, and to the best knowledge of the researcher, none is shown for the three concepts all in one study. This study is therefore the first of its kind, which incorporates the OECD privacy design guidelines, integrating them with the ZDPA privacy guidelines. This makes it easy to be adopted in Zimbabwe. The instrument can be used in future to ascertain what the privacy expectations are and how aware students are of the privacy requirements or conditions. These recommendations are meant to improve student personal information privacy in universities, which benefits both the university and students themselves.

Another crucial contribution of this study is the results from the correlations of the three concepts in the model and how the university could make use of the benefit from them. The university can use such feedback to focus on the weak relationships and use them as areas of improvement. The positive relationships will also be in need of consolidation, to maintain them so that positive perceptions are realised. More so, the privacy model developed can be adopted and be used by other academic institutions to understand student expectations and to meet them in practice. They will have to validate it to suit their scope and context. Even organisations and industries are bound to benefit from the provisions of the model. They could use the model as a guideline when processing their employee personal information to assist them to comply with the ZDPA.

18 SCOPE

This scope of the study is recognised as follows:

- The study measures the students' perceptions regarding how the university upholds their privacy. In this study, perceptions refer to perceptions about the concepts of awareness, expectations and confidence of the students in the university on personal information processing.
- Only one university is included in the fieldwork in this research and the scope was limited to students in one university. However, it is feasible to deploy the developed questionnaire in other universities in Zimbabwe, Africa or even the world at large. This can be done by validating the instrument in other universities.
- The study was grounded on the data protection regulations and principles that were limited to the FIPPs, the 2013 OECD Protection of Privacy and Transborder Flows of Personal Data privacy guidelines, the GDPR and the ZDPA bill.

This study was carried out at one private university in Zimbabwe. It is a religious institution although they do not discriminate based on one's religion, they accept all diverse students, from diverse backgrounds and with diverse religions and beliefs. The institution is multi-compartmented, all campuses are in towns and cities. Of particular importance is the fact that the students came from different backgrounds, some originate from urban cities and towns while others from the rural areas. This background information is vital as it gives an insight on what could influence the students' perceptions on the privacy of their personal information.

1.9 ORGANISATION OF THE THESIS

The overall structure of this thesis is as follows:

Chapter 1: Scientific orientation of the research - This includes the introduction of the research topic, the problem statement, the research aim and objectives, the research questions and the research significance and its contribution. Several other aspects of research are dealt with in this chapter.

Chapter 2: Privacy, privacy principles and privacy regulations - This chapter gives an overview of scoping review in analysing privacy as a concept, personal information,

privacy principles and guidelines and the ZDPA in the design of the information privacy conceptual model.

Chapter 3: Information privacy perception conceptual model - this chapter emphasizes the scoping review pertaining to the three concepts of this study (awareness, expectations and confidence), the social contract theory and finally concludes with student personal information privacy perception conceptual model.

Chapter 4: Research methodology – instrument design, research paradigm, research instruments, how data is collected and ethical considerations.

Chapter 5: Research results – includes the analysis of data, statistical methods, validation and reliability of the instrument. The results stemming from the research are presented and also discussed.

Chapter 6: Conclusion, limitations and recommendations - Concludes the research, cites the limitations and contributions of the study as well as giving some suggestions on future research recommendations.

1.10 CHAPTER SUMMARY

This chapter gave an introduction of the research topic. It explained the background of this research and highlighted the problem statement. This led to the different research questions, which were aligned to the study objectives. A brief summary of the research methodology was outlined, focusing on how the research was conducted, the tools, instruments and design adopted to answer the research questions. The chapter further discussed how to ensure reliability and validity in this study, together with the relevant ethical considerations made. The research significance and its contributions were outlined and the research scope was presented. The chapter concludes by giving the overview of the structure of the thesis. Chapter 2 focusses on privacy, privacy principles, global privacy legislation, the Fair Information Practice Principles, the OECD privacy principles, the General Data Protection Regulation and the ZDPA.

CHAPTER TWO: PRIVACY, PRIVACY PRINCIPLES AND PRIVACY REGULATIONS

2.1 INTRODUCTION

This chapter presents the scoping review, and discusses how it is adoptable in this study. It focuses on the background of the research, starting with the definition of privacy concepts and principles. It then discusses internationally adopted legislations and privacy principles like the Fair Information Practice Principles (FIPPs), the Organisation for Economic Cooperation and Development (OECD) Protection of Privacy and Transborder Flows of Personal Data as well as the General Data Protection Regulation (GDPR). It concludes by discussing the ZDPA, which is integrated in the conceptual model development. The chapter serves as the background to the study.

2.2 OVERVIEW OF CHAPTER TWO

The chapter is segmented into six main parts. These are:

- First Part (Section 2.3) - discusses the use and adoption of the scoping review in this study. Also discussed is an overview of existing research.
- Second Part (Section 2.4) - focuses on the privacy concepts and the definition of privacy, personal information, personal information processing, privacy concerns, privacy breaches, privacy paradox and privacy compliance.
- Third Part (Section 2.5) - it discusses international privacy principles i.e., Fair Information Practice Principles (FIPPs) and guidelines of the Organisation for Economic Cooperation and Development (OECD) Protection of privacy and Transborder flows of personal data. It also discusses the recently adopted regulations on privacy, and of particular interest is the newly adopted General Data Protection Regulation.
- Fourth Part (Section 2.6) – overview of the ZDPA.
- Fifth Part (Section 2.7) – Presents a comparison of the ZDPA with the FIPPs as the baseline, the OECD privacy guidelines and the GDPR.
- Sixth Part (Section 2.8) - this last section summarises the chapter.

A summarised snippet of the discussions in this chapter is shown in Figure 2.1.

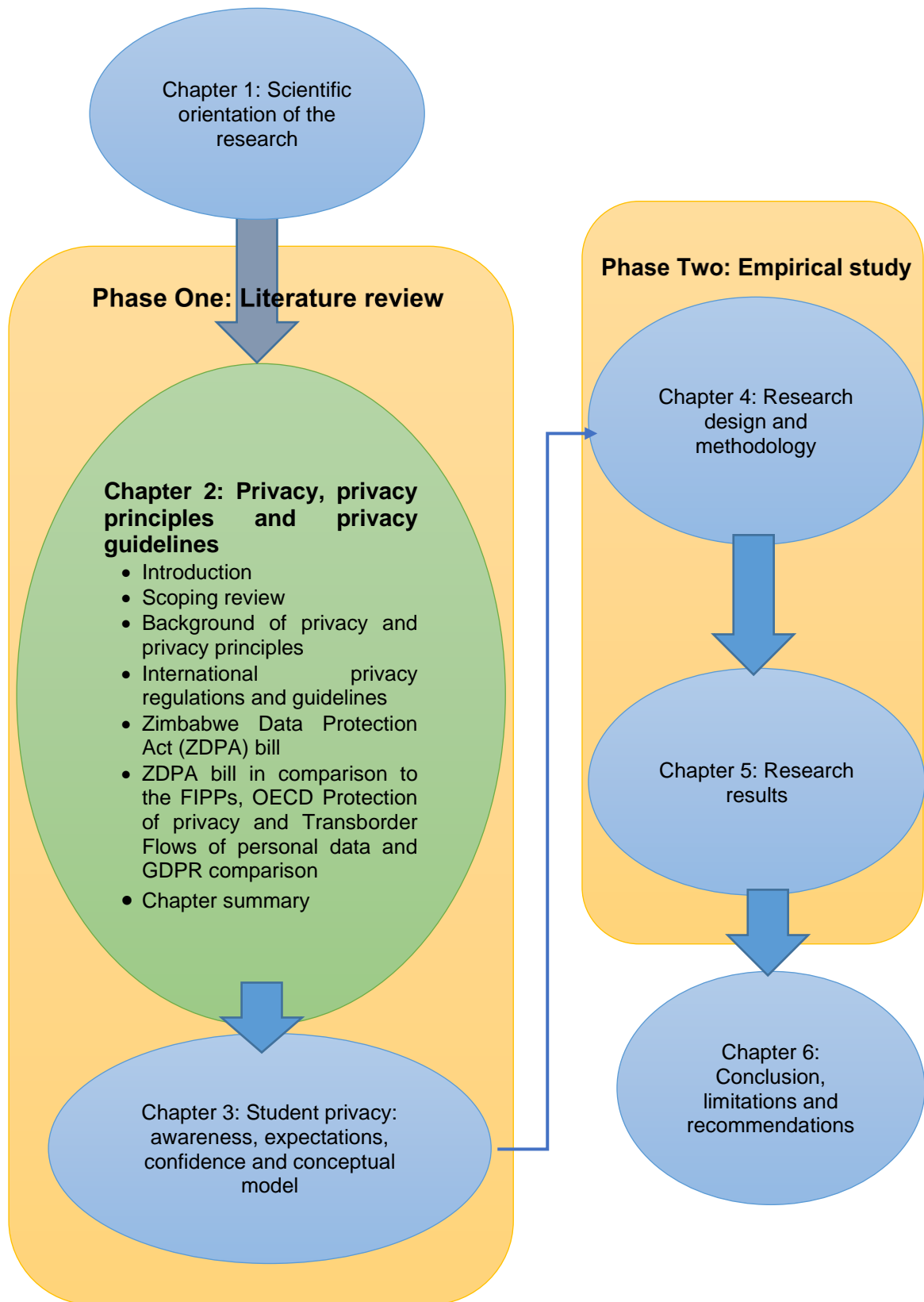


Figure 2.1: Chapter summary (Source: Developed for this research)

2.3 SCOPING REVIEW

This research adopted the scoping review, which is termed “literature mapping” by some scholars (Davis, Drey & Gould, 2009; Dijkers, 2015; Pham, Rajic, Greg, Sargeant, Papadopoulos & McEwen, 2014). There are many definitions for scoping review, though they all seem to emphasise the aspect of a broader perspective to the topic under research (Arksey & Malley, 2005; Davis et al., 2009; Dijkers, 2015; Kokolakis, 2017b; Tricco et al., 2016). A scoping review involves synthesising and analysing a wider range of both research and non-research material in a bid to provide a greater conceptually clarified field of evidence or topic (Davis et al., 2009; Davis, Drey & Gould, 2009). It is a synopsis of a huge field of research (Colquhoun et al., 2014). From a different perspective, scoping review is “a form of knowledge synthesis that addresses an exploratory research question aimed at mapping key concepts, types of evidence, and gaps in research related to a defined area or field by systematically searching, selecting, and synthesising existing knowledge” (Colquhoun et al., 2014 p.1292-4). Mays, Roberts and Popay (2001 p.194) define scoping review as a method “aim to map rapidly the key concepts underpinning a research area and the main sources and types of evidence available, and can be undertaken as standalone projects in their own right, especially where an area is complex or has not been reviewed comprehensively before”.

A scoping review permits a more generalised question and inquiry of similar literature (Peterson, Pearce, Ferguson & Langford, 2017). More advantages provided by a scoping review include having a much smaller depth but with a larger conceptual range, making it flexible and able to cater for a variety but relevant literature that uses assorted methodologies (Davis et al., 2009; Dijkers, 2015; Peterson et al., 2016). The main objectives for conducting a scoping review are to summarise and disseminate the research findings, identification of gaps in the research area, making some recommendations, especially for research to be conducted in the future, as well as for mapping the literature body with the relevance to location, time, origin and sources (Arksey & O'Malley, 2005; Colquhoun et al., 2014).

2.3.1 Stages in the scoping review

Using the Arksey and O'Malley (2005) model, the following are the stages of the scoping review:

- i. **Identifying the research question** – Researchers use the Population, Concept and Context (PCC) mnemonic i.e., population (who), concept (what) and context (with what quantifiers) (Colquhoun et al., 2014). This is where the domain to be explored is specified (Dijkers, 2015).
It starts with wide descriptions for the sample population, the outcomes, to guarantee breadth of search coverage, and then using the scope and volume of references generated for setting parameters.

The scoping review in this study was done for the following reasons:

- to define privacy terminology like privacy, personal information, personal information processing, privacy concerns, privacy breaches, security policies and privacy compliance.
 - to have an overview of existing work and show how privacy is applicable to universities.
- ii. **Find the appropriate studies** – This is done through the databases (electronic), reference lists, websites of organisations and conference proceedings. (Dijkers, 2015). Identifying relevant studies as exhaustively as possible, selecting primary studies (both published and unpublished) and as well as reviews relevant for answering the main research question. researcher adopted an approach that involved probing for research evidence through different sources in order to achieve this.

Databases that were used include ACM, ScienceDirect, IEEE Xplore, Scopus, Google Scholar, Sage Research and Web of Science. Some online websites were used to enhance literature not found in books, journals, and conference proceedings. This was done to make the selection comparable. All these information sources were added into the Mendeley desktop application for easier navigation and administration of sources. The years of publication included ranged from **2000 to 2020**.

- iii. **Select studies which are applicable to the question(s)** - The criteria for inclusion used in the scoping study is correlated with the type of study, the type of intervention, the care recipient group, and career group. It is vital for decision making though it is time consuming (Colquhoun et al., 2014). Unlike systematic reviews, the inclusion and exclusion criteria are established post hoc, after familiarization with literature has been acquired (Arksey and O'Malley, 2005).

In this study, the scoping review was conducted to assist in defining privacy related terms. It also gave an overview of existing work and showed how privacy is applicable to universities. The following key words were the main focus: "privacy", "privacy perceptions", "privacy concerns", "personal information", "privacy breaches", "privacy compliance", "privacy and awareness", "privacy and expectations", "privacy and confidence", "information privacy perception", "privacy models", "privacy and social contract" among several other functional terms of the study. A process of searching and reviewing was done. Relevant articles were downloaded from the online databases and uploaded to the Mendeley desktop application for easier usage. Articles matching the search criteria were read with the appropriate ones selected. For the exclusion criteria, studies external the publication dates of preference, studies external to the student privacy expectations, privacy awareness levels and privacy confidence levels were excluded. In addition, all studies not describing the privacy of personal information were excluded.

- iv. **Charting the data** – This is the material on and from other relevant research studies (Dijkers, 2015). Key items as an output from the primary research reports were reviewed. A summary of each study was done in an excel sheet. Also summarised were the collecting standard information on each study on aspects like the author(s), the year of publication, the study location, the duration and the type of intervention, sample space (population), the purpose of the study, the methodology used, output measures and the crucial results.
- v. **Collate, summarise and report the results** - This is a stage involves the collating, summarising as well as reporting of the output/results. The exposure of the gap in this study is centered on the literature review, which depicted how different scholars managed to do their own research as well as the weaknesses in those studies. The significance must not be on the "weight of evidence",

neither must it be on the evaluation of the evidence quality; rather, it should be on the analytic model for the guidance of the account of narration from the existing literature. After charting, an in-depth analysis of the features of each study, the interventions, sample population, all the participants, the research methods and instruments used, deliverables and gaps were done. A total of 1 189 publications from the academic databases were retrieved and 637 publications were recovered from the Google (the search engine). Duplicate publications totaling 645 were removed from the search. After the exhaustive exclusion criteria based on many aspects, including the screening done using titles and abstracts for relevance, a total of 105 publications met the conditions necessary to be included in this research. Figure 2.2 below illustrates the stages according to the search that was conducted.

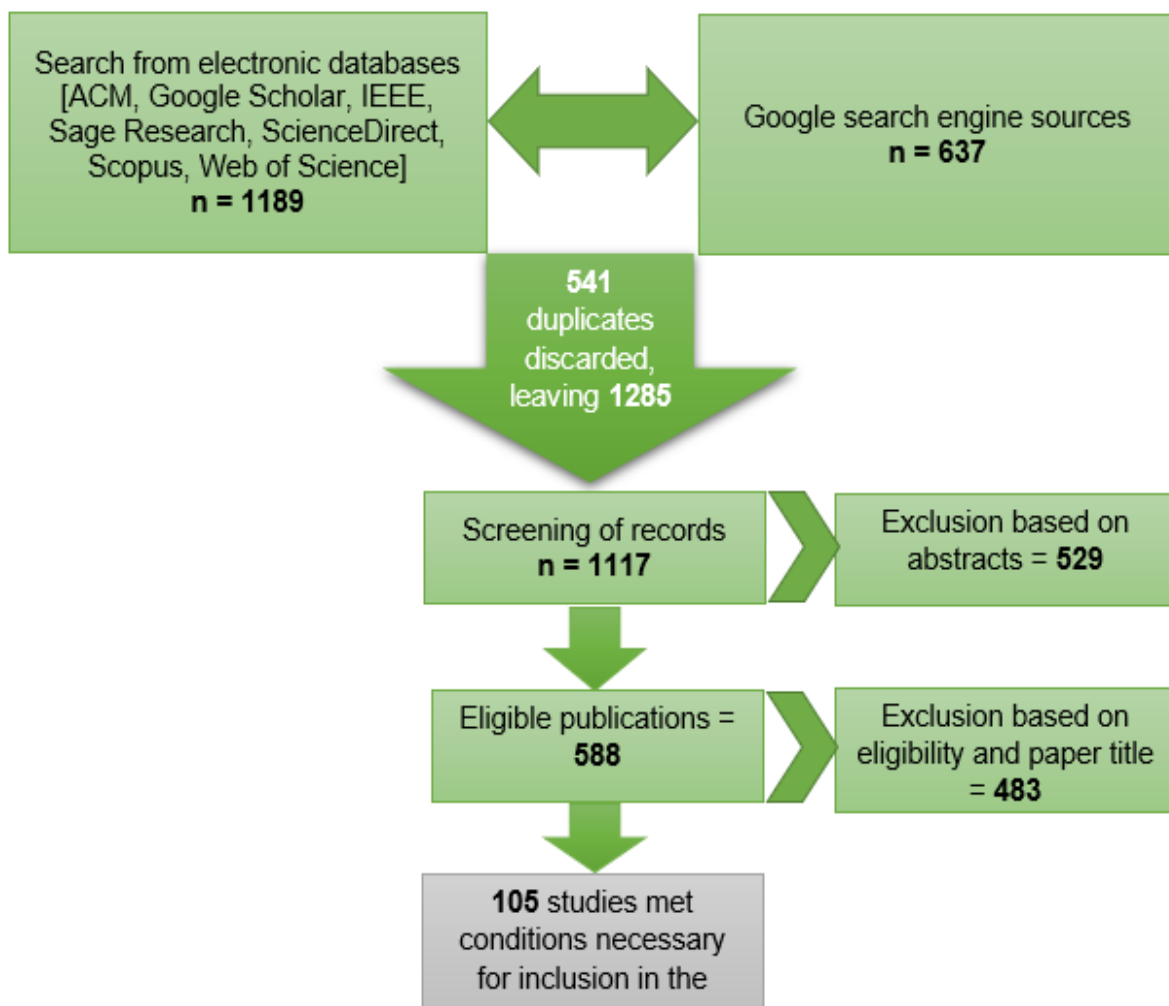


Figure 2.2: Search phases on student privacy awareness, expectations and confidence

vi. Consultation exercise - The last stage is optional, and it relates to a consultation exercise with experts. This phase was excluded from the scope of this scoping review.

2.3.2 Overview of existing research

This section gives an overview of existing research on privacy. Related privacy models are discussed and examples of universities that have compliance privacy models are given. Also done in this section is a discussion about privacy instruments and privacy models and the reasons for not adopting them. A brief discussion of student perceptions (awareness, expectations and confidence) on privacy is also done.

2.3.2.1 Related privacy models

In privacy models, the focus is on how privacy works (Mai, 2016). Research has been conducted extensively on privacy related matters. To make conclusions on such privacy related studies, instruments and models have been developed. A few examples can be cited.

A study (Malhotra, Kim & Agarwal, 2004) for analysing online consumer (student) concerns on privacy and their reactions to different privacy threats on the internet developed an instrument and a validated model. The main drawback of their instrument and model is that it was only peculiar to the online context, making it difficult to be customisable for an academic environment, covering the student perceptions. Hence, it could not be adopted for this study. Kyobe (2010b) developed a framework (similar to a model) which could be used in a university environment for compliance with legislation on information security. Awareness was considered one of the problems in compliance and the study recommended that existing controls be used in alignment with the regulatory requirements. Unfortunately, his framework proffered guidance in information security compliance.

Another privacy model for mobile users was developed for the measurement of privacy concerns (Xu, Gupta, Rosson & Carroll, 2012). It included the perceptions of users but it was limited to the mobile context. Samani, Ghenniwa and Wahaishi (2015) also developed a privacy model for the analysis of privacy concepts and concerns but the scope of the model was only limited to the Internet of Things (IoT) technology. Thus,

it only focused on the personal information privacy when using IoT applications. An attempt to analyse privacy models was also made by Victor, Lopez and Abawajy (2016) although, again, their model was limited to big data privacy in this digital world.

A 29-item instrument developed by Martin, Gupta, Wingreen and Mills (2015) for the privacy of personal information placed more emphasis on disclosure, storage, awareness, use and collection related issues. They also developed a conceptual model that can aid in achieving the personal information privacy. The objective of their instrument and model was to reflect on the internet users' concerns pertaining to information privacy. The instrument by Martin et al. (2015) could not be adopted for this research because it does not examine student perceptions from the awareness, expectations and confidence perspectives, as it was only meant for a small sample. More so, the conceptual model does not give the specifics of how the student perceptions are addressed and the implication of the aspects addressed in the research to trust and confidence

One popular model amongst privacy concerns scholars, the Internet Users Information Privacy Concerns (IUIPC), was used by Harborth and Pape (2019). Its main focus was on the measurement and analysis of privacy concerns of online users and therefore, the instrument and model are not be ideal for the measurement of student perceptions on privacy.

In fact, many researchers focusing on privacy have developed privacy instruments and to some extent, privacy models. Unfortunately, they only suited certain defined scopes and contexts and this research could not adopt neither the already developed instruments nor the models. More so, these models were not based on FIPPS or privacy conditions of the law, which was a limitation towards their adoption in this study. This research made use of both local (ZDPA) and international privacy principles and regulations in its perceptions measurement (FIPPs, the OECD privacy regulations and the GDPR), hence the need for developing new privacy instrument and privacy model.

2.3.2.2 Privacy models in academia

The 105 studies alluded to above were used to search for available literature on what was being done by other universities on privacy models. It was found that some universities had privacy models customised with the current privacy best practice regulations. For example, the University of Plymouth has a privacy model that is grounded on the customisable General Data Protection Regulation (GDPR) and focuses on what type of information does the university have, who has authority over the information, where to locate the information and how long is the information going to be kept (University of Plymouth, 2019). The model, as indicated by the University of Plymouth (2019), aims to achieve compliance with regulatory obligations, including the GDPR, privacy protection of individuals and reducing security breaches.

Monash University from Australia customised their privacy model with the GDPR in mind because they were cognisant of the impact of the GDPR on some of their European partners, since the GDPR can be activated even by association and Monash university has global reach, including with European Union universities (Monash University, 2020). This implies that there is need for them to meet the compliant clauses and requirements (Daly, 2018). The university had separate statements on how privacy will be upheld based on the data protection and privacy collection based on general student data, admission data, alumni information, employee information, research information and even visitors and inquiry data. The objectives of the model included the implementation of privacy measures that enable compliance where applicable and getting a template of drafting a privacy model that complies with such international standards consistent with the GDPR (Monash University, 2020).

The University of Canterbury also has a privacy model that complies with the New Zealand Information Privacy Principles, which underpin how information will be used, and these include purpose collection, source of personal information, manner of collection, access, storage and security, correction of information, checking accuracy of information before use, limits on use, limits on disclosure and unique identifiers (University of Canterbury, 2019). In addition, the Flinders University used a model that allowed them to uphold privacy principles through a privacy policy, personal information protection procedures and provision of a quick guide for the management of privacy as asserted by the Flinders University (2016). The privacy policy model

serves the purpose of showing commitment by the university on how they value the privacy and protection of students' personal information.

In comparison to this research's context, these models do not integrate student awareness of students on privacy awareness and the expectations of student on privacy which, in the researcher's view, are prerequisites for instilling confidence based on the social contract theory. Their main focus was on awareness, which is one concept from a total of three that are examined in this study. The privacy models emphasised their national privacy policy frameworks and the GDPR. They do not take cognisance of the FIPPs principles and OECD privacy guidelines. In addition, most of the models and frameworks thrust their determination on privacy implementation by the universities, indicating the various steps to be observed to without essentially observing other components like the awareness, the expectations and the student confidence in the university.

2.3.2.3 Privacy awareness influence in compliance

In a research for the model that favours compliance with policies and regulations in a university setting, Kyobe (2010) highlights that awareness and training are some of the privacy and security practices needed for compliance with regulatory requirements. From his study, an awareness practice favours compliance as it increases students' knowledge on privacy related matters. According to Kyobe (2010), laws and regulations can only be useful if there is knowledge and therefore awareness from the students, resulting in compliance. Although this is very important, there is also need to look at what the student will be expecting on privacy and analyse the student's confidence as it will yield privacy compliance (Taddei & Contena, 2013). Chen and Ismail (2013) conclude in their study that although students are aware of the importance of protecting their personal information, they do not clearly grasp the consequences of the university illegally using the personal information. Being aware of their privacy expectations would be crucial for the students, building confidence in the university, resulting in privacy compliance. Therefore, privacy awareness can be instrumental in aiding and guiding a university in privacy compliance as suggested by Kyobe (2010a).

2.3.2.4 Student privacy awareness, expectations and confidence

Student expectations and attitude were analysed (Kurkovsky & Syta, 2011) in relation to using electronic communication and its effect on trust and privacy. Students showed awareness of privacy policies and regulations, but had the expectation that the electronic communication must always remain private. Similarly, in an effort to gather student expectations in an e-learning environment, students were asked to submit information they would trust and have confidence in (Dwyer & Marsh, 2016). The results showed that the students had high levels of awareness, with varying confidence and preference levels in engaging the e-learning systems. Furthermore, a study by Dwyer and Marsh (2016) posits that for proper engagement between the university and the students, students are supposed to be actively involved in how they make decisions on their personal information privacy. These studies show awareness and levels of confidence of students on privacy related issues but lack the aspect of gathering more information on the student expectations. Therefore, there is need for a follow up study on awareness, expectations and students' confidence, especially with new regulations like the ZDPA being regarded as the cornerstone in upholding privacy principles within university environments in Zimbabwe.

Universities are expected to increase privacy awareness and permit students to exercise their consent right when personal information is to be handled, and lack of awareness is a threat to the students' privacy (Isabwe & Reichert, 2013). According to Botha et al. (2015), this awareness must not be a once off event, it must be done continuously so that individuals and organisations are educated on what is expected of them in privacy. It is also important to realise that expectations will continuously change in the increasingly digital age (Arnold & Sclater, 2017) and as such, students will keep changing goal posts in terms of their expectations.

Studies have been done to assess several concepts within the university environment (Adelola et al., 2014; Chen & Ismail, 2013; Coleman & Purcell, 2015; Dwyer & Marsh, 2016; Kokolakis, 2017; Kurkovsky & Syta, 2011; Kyobe, 2010b; Stange, 2011; Taddei & Contena, 2013), but none has been carried out on the students' awareness, students' expectations and the attributes that constitute to an increase of student confidence in the university. This raises the necessity of a diagnostic tool to aid universities in being thoughtful of privacy concerns by the students and their

expectations personal information protection, privacy and assist in giving effect to adherence with the privacy constitutional right. The next section discusses privacy background and privacy principles.

2.4 BACKGROUND OF PRIVACY AND PRIVACY PRINCIPLES

Privacy is believed to vary from one culture to the other (Djatkiko, 2014; Martin, 2015). Although there exists many definitions of privacy (Choi, Lee & Sohn, 2017; Katell et al., 2016; Kurkovsky & Syta, 2011a; Miltgen, 2009; Mohamud et al., 2016), it seems grasping its limits and scope is elusive to many theorists (Pelteret & Ophoff, 2016). There are various concepts that are discussed in this chapter pertaining to privacy, but the inceptive point should be a clear understanding of defining the term “privacy” and related concepts.

2.4.1 Privacy definitions

Privacy is "the ability of an individual to control the terms under which their personal information is acquired and used" (Ackerman & Mainwaring, 2005 p.2). From a different perspective, Almatarneh (2011) defines privacy as a multi-dimensional concept that gives the right to avoid personal information disclosure to others and that very right to be left alone. Miltgen (2009) weighs in and views privacy as the confined mentality within individuals that it is constantly limited to the capability of individuals to limit access to one's personal information, and the influence of self-disclosure particularly on the internet. Although Miltgen's definition is concentrated on internet privacy, it resonates with Schofield and Joinson's (2008) definition in that they all give the right to disclosure to an individual. Besides suggesting that privacy is the right to be left alone, Smit, Lyons, McAllister and Slonim (2009) also reiterate that the definition has since evolved because of advancements in technology, as it now includes the conviction that individuals are supposed to have control over whom and when they might decide to disclose their personal information. Smit et al. (2009) seem to have integrated definitions by Ackerman and Mainwaring (2005), Almatarneh (2011), Miltgen (2009) and Schofield and Joinson (2008).

Chen and Ismail (2013 p.434) define privacy as "the right to be free from secret surveillance and to determine whether, when, how and to whom, one's personal or

organisational information is to be revealed". Besides disclosure, Chen and Ismail (2013) seem to be emphasizing the control aspect in defining privacy. Talib et al. (2014) also defines privacy as the right of people to control their own personal information and to decide whether to keep or disclose it. This definition also puts much emphasis on the control to one's personal information. Mohamud et al. (2016) define privacy as being linked to the ability of a person to share information with others, all the safeguards that are needed on the information and the freedom to decide whether to keep information to oneself without being forced to share. So it can be further said that personal information privacy is the ability of any person to have control of information about oneself (Choi et al., 2017). These definitions are centred on the control of personal information though some are adding the aspect of deciding whether to keep or share the personal information. Some definitions add to their scope to cover more aspects like keeping, sharing and all the necessary safeguards to protect personal information.

Privacy seems to be the most challenged concept with many information intermediary companies like Facebook, Microsoft and Google at the vanguard of defining their user privacy conditions, especially on how the collection of data is done, how the processing of the data is done and practises of information dissemination (Sargsyan, 2016). In a broader sense, privacy can be viewed from multiple dimensions. An argument from some school of thought posits that privacy is no longer regarded as a social norm since most people are used to sharing their personal information and experiences especially when online, as argued by the Facebook founder, Mark Zuckerberg (Jordaan & Van Heerden, 2016). On the contrary, Jordaan and van Heerden (2016) contend that some individuals are quitting Facebook citing concerns about their privacy. This means that privacy issues are complex and will need to be understood from a broader perspective.

A summary of definitions by different researchers on privacy is shown in Figure 2.3 below.

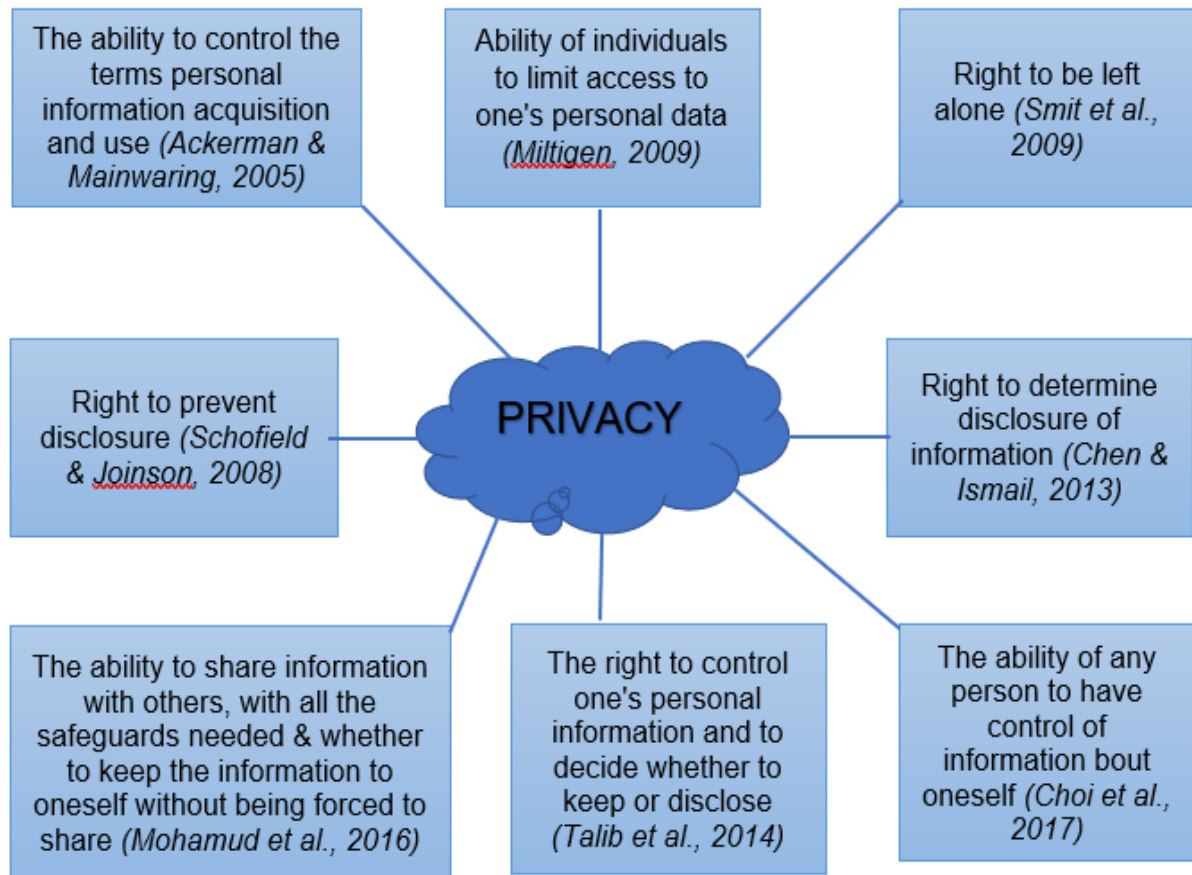


Figure 2.3: Different privacy definitions

From Figure 2.3 above, it can be noted that the most common aspects in understanding and defining privacy are the ability to be left alone, having control over personal information with respect to acquisition, disclosure and sharing of the personal information and security safeguards on personal information.

Within the context of this study, the researcher integrated various aspects in defining privacy since most of them focused only on one or the other domain. For example, one definition could be limited to control, the other on disclosure, or being left alone. The researcher defines privacy as the ability of an individual to be left alone and have control of one's personal information ranging from how the personal information is acquired and shared and/or disclosed, with the expectation that the entity that processes information will apply the necessary security safeguards that are needed to accomplish integrity, availability and confidentiality of such personal information.

Therefore, there is need to understand personal information.

2.4.2 Personal information

The OECD (2013, p.13) defines personal data/ information as “any data or information concerning an identifiable or identified individual”. Privacy concepts and concerns on personal information have moved from simply focusing on the physical body, as the advances in information technology have evolved towards its use and abuse by individuals and companies (Chen & Ismail, 2013). According to El-sheikh (2013), the aspect of personal information protection is a crucial human right aspect that demands organisations and institutions not to be given authority of deciding policies in this regard, as it is deemed a serious matter which must not be compromised in any way.

Santanen (2018) stresses that privacy is a prudent social issue that is affecting everyone and lack of it limits people on how they disclose themselves especially during social interactions. This formulates the concept of personal information under discussion. Privacy of personal information is a fundamental expectation by anyone who uses technology and it has to be respected, anything else will constitute a psychological contract breach (Mamonov and Benbunan-Fich, 2015). Personal information which can be gathered, processed, stored and used include information such as names, age, sex, email, ID number, address, phone number, location details, financial details and health details (Sargsyan, 2016).

According to the ZDPA (Zimbabwe Data Protection Act Bill, 2013 p.7), personal information is;

...information relating to a data subject, and includes: (a) the person's name, address or telephone number; (b) the person's race, national or ethnic origin, colour, religious or political beliefs or associations; (c) the person's age, sex, sexual orientation, marital status or family status; (d) an identifying number, symbol or other particulars assigned to that person; (e) fingerprints, blood type or inheritable characteristics; (f) information about a person's health care history, including a physical or mental disability; (g) information about educational, financial, criminal or employment history; (h) opinions expressed about an identifiable person; (i) the individual's personal views or opinions, except if they are about someone else; and (j) personal correspondence pertaining to home and family life.

This working definition by the ZDPA summarises personal information in terms of characteristics of a person, his/her behaviour, opinion/views and the person's attributes and his/her personal possession. Personal information is needed in organisations and institutions so that it can be processed for various uses as deliberated in the following section.

2.4.3 Personal information processing

Protection of information contributes towards its privacy (Miltgen (2009). It is also of paramount importance that when information is gathered, it is processed and used only for the purposes it has been collected for, otherwise it becomes a breach of privacy (De Hert & Papakonstantinou, 2012). In their working definition, the Data Protection Bill of Zimbabwe (Zimbabwe Data Protection Act Bill, 2013 p.7) defines personal information processing as referring to;

...any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as obtaining, recording or holding the data or carrying out any operation or set of operations on data, including (a) organization, adaptation or alteration of the data; (b) retrieval, consultation or use of the data; or (c) alignment, combination, blocking, erasure or destruction of the data.

The above definition puts emphasis on all the actions and processes that are undertaken on personal information. In addition, Kim, Park, Park and Ahn (2019) state that personal information processing must also include operations to personal information such as collection, organisation, storage, recording, alteration or adaptation, consultation, usage, dissemination, transmission, disclosure or otherwise availing it, restriction, its integration or destruction.

As pointed out by Lawler and Molluzzo (2011), some students in universities are not privy to how their sensitive personal information is gathered, used and how it is shared. This also creates an avenue for personal information misuse. Use of personal information for individuals has many advantages but it is also equally prudent that the information is protected adequately, which calls for legislations to be put in place to

regulate its usage (El-sheikh, 2013). In the European Union, the GDPR has made it a prerequisite that information can only be transferred from Europe to any country as long as it does have adequate laws on data protection, in accordance to the European Commission (Sargsyan, 2016). Personal information privacy and its processing are a continuous information concern to multiple stakeholders like individuals, scholars, business people, government regulators and more so, privacy activists (Ozdemir, Benamati & Smith, 2016; Yang & Wang, 2014).

Personal information is being collected, stored and processed by universities. Every time a student requires a service at a university, personal information about the student is submitted (Yang & Wang, 2014). The table shown below depicts examples of personal information of students that universities process.

Table 2.1: Examples of personal information that universities process

Study	Personal Information	Example
Rezgui & Marks (2008)	Student electronic records and student identification	Social security numbers and biological material, alumni and Scan IDs for registration
Kyobe (2010)	Student performance for exam purposes	Student enrolment, student marks
Kurkovsky & Syta (2011)	Private student information	Academic records, financial records and health related records
Lawler, Molluzzo & Doshi (2012)	Personal information in e-learning environments	Email addresses
Azemović (2012)	Student performance in e-learning environment	Student courses, grades, exam marks
Yang & Wang (2014)	Student registration	Personal photos, mobile numbers, physical address
Hossain & Zhang (2015)	Student age during enrolment	Student age
OAIC (2015)	Personal information collection during enrolment and registration	Admission, enrolment, academic progress, studies, participation and attendance, tuition fees and penalties, academic agreements, discipline, assessments etc.

Bansal, Zahedi & Gefen (2016)	Sensitive privacy information	Student's health records, disability, religious information etc.
Nwaeze, Zavarasky & Ruhl (2017)	Student personal information during registration and enrolment	Student name, student ID, date of birth, phone number, email address, social security number
Feri et al. (2016)	Disclosure of personal information	Name of subject and the result

From the above table, it can be seen that the university uses personal information for student enrolment and registration and examples are names, age, gender, student numbers, student IDs, physical addresses, social security numbers, email addresses, phone numbers and photos. Once the student is enrolled, the university will also need to capture the student's health records, academic records, financial records, attendance, academic agreements, disciplinary issues, assignments and assessments in academic progress, examination marks, and alumni records. The ZDPA bill will therefore apply to universities as these fields of student personal information are collected by the universities. As highlighted in the ZDPA bill (Zimbabwe Data Protection Act Bill, 2013), the bill will apply to both private and public entities – universities included, as long as they collect, use, process, transmit and store information of any identifiable persons (including students). The processing of personal information brings about many privacy concerns.

2.4.4 Privacy concerns

Evidence points to the fact that people are increasingly making personal information readily available publicly, leading to the upsurge of privacy related concerns (Choi et al., 2017; Kruikemeier et al., 2020; Mamonov & Benbunan-fich, 2018; Nadasen, Pilkington & Da Veiga, 2016). Privacy concerns are a continuous troublesome dimension in information technology research and they are an international area of concern (Kokolakis, 2017; Mamonov & Benbunan-Fich, 2018; Ozdemir, Benamati & Smith, 2016; Sodiya & Adegbuyi, 2016). They can be viewed as beliefs about the possibility of undesirable penalties of the gathering, collection and use of personal information (Kruikemeier et al., 2020). The concerns by the customers on privacy are largely based on their lack of control regarding their personal data as well as being sceptical on how the data collector will handle their data during processing (Okazaki et al., 2020). They are common as long as there is existence either in digital form or

otherwise of personally identifiable information (Sodiya & Adegbuyi, 2016). Surveys carried out indicate that privacy concerns in the digital age are skewing upwards due to the complexity of controlling new technological trends (Kokolakis, 2017; Kruike-meier et al., 2020; Okazaki et al., 2020). These privacy concerns have also been increased by the fact that websites can now collect information unobtrusively, which also affects trust issues (Bansal et al., 2016; Bellman, Johnson, Kobrin & Lohse, 2004; Haddad & Aïmeur, 2018; Martin, 2018). As posited by Aghasian, Garg, Gao, Yu and Montgomery (2017), ignorantly sharing personal information especially when online poses privacy risks.

Privacy concerns become easy to handle when there is an appropriate strategy for aggrieved persons to lobby a complaint about concerns as propounded by Adelola, Dawson and Batmaz (2014). To help address most of the privacy concerns that are originating from the increase in use of personal information and the risk it poses to the generality of the whole globe, the OECD assists in combating them (OECD, 2013a). There is also the GDPR, which aims to harmonise all data protection laws within the EU member states and try to offer better compliance using regulatory models (Preuveneers, Joosen & Ilie-Zudor, 2016). The Fair Information Practices Principles also aims to lower and correct some of the growing privacy concerns in the use and processing of personal information (Guffin, 2017).

Students need to have confidence in the university that they will observe and uphold their personal information privacy (Akpojivi & Bevan-Dye, 2014). Students gain confidence in the university if it processes their personal information observing the privacy guidelines and privacy legislations, as stated in the privacy model by OAIC (2015). Unfortunately, privacy concerns can hinder trust and confidence within an institution (Hasbullah, Abdul, Wan & Isa, 2013; Kokolakis, 2017; Miltgen, 2009); Gajanayake et al., 2011; Heath, 2013). Globalisation, growth of internet and the dominant upsurge in social media usage have also immensely contributed towards the growth of privacy concerns (Martin, Gupta, Wingreen & Mills, 2015). One major problem for raising privacy concerns is the profiling of personal information by university administrators, as this is an intrusion into sensitive personal information that might lead to the discovery of “non-obvious private information” (King & Forder, 2016). As a mitigating technique, one way of coming up with solutions to privacy concerns is to give students overall control of how they are to use their personal information

(Sargsyan, 2016), which will ultimately increase trust and hence confidence (Huang & Bashir, 2016).

As deduced from interviews by Stange (2011), students are most concerned about their personal information confidentiality and there is need therefore for student engagement in privacy related issues, including the quality of the information that the university will be handling. Studies (Fink, 2012; Gajanayake et al., 2011; Yang & Wang, 2014) have discovered that if students are having privacy concerns, they tend to disengage participation and prevent sharing some vital information, which might be detrimental to the university needs and demands for information use. Privacy concerns are also determined by the level and degree of control over one's personal information, which also ultimately has influence over trust and confidence (Taddei & Contena, 2013).

Privacy concerns are relevant to this study because they impact on and affect student confidence levels (Akpojivi & Bevan-Dye, 2014; Huang & Bashir, 2016; Katell et al., 2016; Kurkovsky & Syta, 2011; Stange, 2011), as students might disengage participation in providing information that might be crucial for university use (Anjum et al., 2018; Gajanayake et al., 2011; Stange, 2011). Privacy concerns are also a result of privacy breaches as discussed in the next section.

2.4.5 Privacy breaches

One can define privacy breaches as unauthorised disclosure of personal information (Islam, Watson, Iannella & Geva, 2017). It has been deduced from empirical research (Lawler & Molluzzo, 2011; Lumpur, 2010) that people tend to share personal information without seeking permission or consent from friends, and this constitutes privacy breaches. The GDPR obligates any organisation/ institution/ company to take the necessary safeguards and to inform its data subjects instantly if there is a breach to its data/ information (European Union, 2016a).

Because of the use of various techno-driven instances that have the capability of collecting and leaking personal information, this has led to the upsurge of incidences of privacy breaches (Kokolakis, 2017; Mamonov & Benbunan-fich, 2018; Okazaki et al., 2020). Surveys indicate that privacy breaches in the digital age are skewing

upwards (Kokolakis, 2017; OECD, 2013). This is mainly accredited to the use of many sophisticated tools, techniques and equipment in the digital age (Iachello & Hong, 2007). Privacy breaches need better safeguarding ways and the need to design incident response strategies in order to protect privacy (OECD, 2013b). These privacy breaches are also mainly regarded as a responsibility of the data safeguarding entities (Iachello & Hong, 2007). Data breaches are a result of unwanted behaviour that can be analysed from many perspectives, including employees not following the right procedures, thieves stealing devices especially portable ones or unprotected systems being accessed by hackers (OECD, 2013b).

According to Rezgui and Marks (2008), the University of Texas had information breaches of 200 000 student records which were accessed illegally and such records included student social security numbers, biographical information and alumni information. In addition, according to an online blog for the analysis of university data breaches in the United Kingdom (Irwin, 2020), posits that data breaches in university environments are becoming more frequent as supported by empirical evidence of 54% of universities reporting data breaches. Within the Zimbabwean context, it has been reported that the Harare Institute of Technology (HIT) has been attacked twice within two years and sensitive personal information including names, passwords and registration numbers was stolen (Mudzingwa, 2018). The National University of Science and Technology (NUST) was also compromised, where hackers demanded a ransom in the form of bitcoins so that the university system would be restored (Pindula News, 2017). These are cases of privacy breaches on student personal information.

Research on academic privacy breaches concluded that personal information breaches constitute at least 21% of all breaches reported, representing the highest number of any breaches in comparison to any other business domain (Ayyagari & Tyks, 2012). The breaches include personal information disclosure through hacking, unauthorised personal information disclosure, student social security numbers being displayed, examination results being displayed, viewing admissions and enrolment lists, universities not disclosing vulnerabilities and accounts records among other breaches (Privacy Rights Clearinghouse, 2019). As research has shown, the breaches could have been mitigated if there was more awareness to curb such incidences (Krzych & Ratajczyk, 2013). There appears to be a relationship amongst the total

number of students and the data breaches (Mello, 2018). In other words, the more students the university has, the more likelihood there is of data breaches. Therefore, raising awareness about student personal information privacy breaches is prudent in a university setting (Ayyagari & Tyks, 2012).

The data controller has a duty to report any form of privacy breach to the regulating body (Fink, 2012). A data controller refers to "any natural person and legal person excluding a public body which alone or jointly with others determines the purpose and means of processing of personal data" (Zimbabwe Data Protection Act Bill, 2013 p.6). Any form of breach would cause panic and privacy concerns to the students and they might not know the severity of the breach on their personal information (Ackerman & Mainwaring, 2005; Kyobe, 2010b). Such an experience (privacy breaches or violations) will have a negative impact on the confidence in the university of the students in observing their personal information privacy (Bansal et al., 2016; Huang & Bashir, 2016; Kruikemeier et al., 2020). Privacy compliance by employees within an organisation can result in the reduction of privacy breaches (Coleman & Purcell, 2015; Greene & Arcy, 2009).

Institutions must know that one key precursor for data breaches and violations is lack of awareness (Botha et al., 2015) and having higher awareness levels will reduce or lower the rate of privacy breaches reports (Tan, Wen Yong Chua & Chang, 2014). Universities will be exposed to technological growth/trends in data collection, sharing of information and data mining techniques and as such, there is need to also consider the costs associated with data breaches (Bansal et al., 2016). Therefore, in case of a breach, the data controller has to immediately report such a violation within the shortest possible time (OECD, 2013b; Preuveneers et al., 2016a; Zimbabwe Data Protection Act draft bill, 2013), with the GDPR stating that reporting has to be done within 72 hours (Cornock, 2018). In cases of privacy breaches and violations, there is need for warnings as early as possible. Therefore, the organisation should comply to avoid the backlash of the consequences of privacy breaches, which some organisations are not aware of (Botha et al., 2015).

Privacy breaches are relevant to this study because they reflect on the need for notifications and awareness by institutions to help curb them. The organisations are likely to have less privacy breaches if their employees are aware of privacy during the

processing of customers' personal information (Botha et al., 2015; Tan et al., 2014). Privacy breaches are believed to give negative perceptions to students on privacy (Anjum et al., 2018). There is need to curb the increase of privacy breaches as witnessed in institutions of higher learning (Coleman & Purcell, 2015). According to Waldman (2020), it is unfortunate that sometimes the users are cognisant of such privacy concerns and breaches, but they behave in an contradictory manner.

2.4.6 Privacy paradox

Privacy paradox is the tendency of customers to behave in a manner that contradicts the privacy concerns stated or that contradicts their privacy attitudes (Bandara et al., 2020; Hallam & Zanella, 2017). It is a tension between the customer's preferences and their actual behaviour (Barth & de Jong, 2017; Martin, 2020; Waldman, 2020). Martin (2020) and Kokolakis (2017) further explain the privacy paradox as a scenario when consumers (students) attach value to privacy during surveys but their actions suggest that they still continue disclosing their personal information. The privacy paradox concept is further constrained by the fact that although user privacy has become a fundamental issue worth addressing, social networking sites are now part of our daily lives and act as social actors (Fatima et al., 2019). This results in completely divergent outcomes of the social world. The privacy paradox is complex because on one hand there is the general pressure for service providers to protect users' personal information and on another hand the service providers need to fulfil their business obligations, in some cases using personalised services (Kaaniche, Laurent & Belguith, 2020).

In other terms, the privacy paradox is a scenario when the level of privacy behaviour is in incongruity with the levels of privacy concern stated (Li, Luo, Zhang & Xu, 2017). This phenomenon can be analysed from both the organisation (university) as well as the user (student) perspective. The students are conflicted between expressing their concerns on how their personal information protected and handled, against their behaviour in voluntarily giving away such personal information especially when online and their failure to protect their personal information (Gerber, Gerber & Volkamer, 2018). The university employees are aware that they need to collect student personal information for processing. At the same time, there is need for limiting the collection only for the specified purposes. Thus, a tension is created, which according to Martin

(2020), is a paradox on privacy. Therefore, it is imperative that the privacy paradox is reduced. One of the ways of mitigating and reducing the paradoxical behaviour is the promotion of privacy protection and awareness (Barth, de Jong, Junger, Hartel & Roppelt, 2019).

The privacy paradox is important in understanding the human behaviour, especially in the university context in this study. There is a paradox in privacy as the university tries to gather as much information from the students as possible for use, against the need for having students' privacy, a situation lamented by Cloarec (2020). As the university will be trying to use students' information for the common good, the temptation and risks of information misuse will create privacy concerns (Cloarec, 2020). The university must not be a victim of the paradoxical behaviour, as they claim to be cognisant of student privacy concerns but go on to disclose their personal information nonetheless.

2.4.7 Privacy compliance

Regulations are put in place to instil compliance and the privacy concerns can only be swiftly alleviated with the help of regulations, as alluded to by Burdon (2011). Actually, regulations are a remedy to failure in compliance as they provide a roadmap on how privacy issues must be handled (Gellman, 2017). That is why many countries, including Zimbabwe, are trying to uphold the privacy of personal information by coming up with regulations for information collection, handling and usage. The privacy compliance task has been tasked to the data controller, the one who will be processing the personal information of people (OECD, 2013a; Zimbabwe Data Protection Act Bill, 2013). According to the OECD privacy regulations (2013), every data controller must provide for suitable safeguards founded on privacy risk evaluation that ensures compliance to privacy principles.

There must be fair warning on those employees who fail to comply, with consequences clearly stated (Kurkovsky & Syta, 2011). Accountability and auditing as FIPPs privacy principles, increase privacy compliance as organisations must be accountable (Federal Trade Commission, 2007; Gellman, 2017). The GDPR was also put in place to proffer the rules for protecting and personal information processing, to safeguard the fundamental human rights as well as freedoms of any natural person on their personal information and ensuring the free movement of personal data within Europe

(Cornock, 2018). Therefore, there is need for compliance with respect to these GDPR requirements. The GDPR applies to Zimbabwe, as European students can be engaged in research and studies within Zimbabwean universities.

Research (Kurkovsky & Syta, 2011) has concluded that when users are having their electronic communication monitored, they are more likely to comply with privacy laws and principles and it is even better if they are made aware of such monitoring policies. As Gellman (2017) argues, compliance plays a very important role in instilling confidence about an organisation, institution or entity in terms of how they will handle personal information. Organisations and institutions are meant to comply with the ZDPA and failure to comply will result in various penalties (Zimbabwe Data Protection Act Bill, 2013). Privacy compliance tends to reduce personal information abuse, leading to the observation of ethical consideration which is critical in this information age (De Hert & Papakonstantinou, 2012; Ortiz, Chih & Tsai, 2018).

Rezgui and Marks (2008) assert that university staff must be aware of the consequences and disciplinary action as a result of non-compliance with the institution's privacy policy. Awareness campaigns can also be used as a tool for compliance with privacy regulations (Rezgui & Marks, 2008). The presence of a privacy policy in a university environment increases compliance with privacy regulations as employees will be knowing (awareness) in advance (Stange, 2011). In fact, institutions can also increase privacy compliance by having an officer to handle and deal with privacy related issues (Kyobe, 2010b). It is also a technique of ensuring privacy compliance and confidence building when privacy related matters are handled by the office of the top management of the university, including that of the Vice Chancellor (OAIC, 2015). Students need to have confidence that the university has privacy policies in place and that the university employees comply with the policies. (Kurkovsky & Syta, 2011).

Non-compliance to a regulation by employees must be met with some disciplinary action, a penalty or some form of punishment (Kyobe, 2010a; Rezgui & Marks, 2008). Organisations seek to uphold privacy principles through the designing of compliance-monitoring programs and procedures (Burmeister, Drews & Schirmer, 2019; Tom, 2018) and these might include training for awareness. It is the duty of the data controller to provide for suitable safeguards, founded on privacy risk evaluation, that

ensure compliance to privacy principles (Danezis, Domingo-Ferrer, Hoepman & Schiffner, 2014; Pouillet, 2018). This assertion is also alluded to by Gellman (2017) who argues that it is the duty of the organisation to come up with measures that ensure compliance to privacy regulations. Every institution must understand the regulatory requirements and come up with their own means of ensuring compliance (Miltgen & Smith, 2015). There is need for approaches to eliminate privacy concerns in favour of student participation and one of the remedies is privacy regulation compliance (Chang, Wong, Libaque-Saenz & Lee, 2018; Chen, Yang, Wang & Niu, 2012; Kokolakis, 2017). The best way of ensuring compliance by an institution is by offering them security and privacy awareness, which will help in the modification of the employees' behaviour (Ortiz et al., 2018).

Privacy compliance is relevant to this study in that the student expects that university employees will comply with privacy requirements (Callanan, Jerman-Blažič & Blažič, 2016; Gellman, 2017). Privacy compliance is also believed to be a major boost for confidence in the university (Callanan et al., 2016; Kafali, Jones, Petruso, Williams & Singh, 2017). International privacy principles and best practices are discussed next, followed by an overview of the ZDPA bill.

2.5 INTERNATIONAL PRIVACY REGULATIONS AND GUIDELINES

There are a number of privacy guidelines that have been accepted internationally to govern how personal information is used and to uphold the spirit of privacy. Within the context of this research, the Fair Information Practice Principles (FIPPs) and the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Cooperation and Development (OECD) are discussed in this section.

2.5.1 The Fair Information Practice Principle (FIPPs)

The Fair Information Practice Principles (FIPPs) are internationally recognised privacy principles that regulate both the private sector and all government entities (Federal Trade Commission, 2007; Gellman, 2017). They are a set of international practices that depict the recognised international practices for privacy in using personal information (Sargsyan, 2016). The FIPPs are an anthology of incorporating agreed and accepted principles into policies of organisations and institutions around the world and are

applicable when trying to evaluate information processing that has an impact on individual privacy (Guffin, 2017). The FIPPs were initially used to control how governments would use individual personal information, but the rules have been extended to the private sector (companies and institution) since technology has been evolving on a daily basis and is impacting heavily on personal information handling (Chang et al., 2018; Schwaig, Kane & Storey, 2006). As summarised by Guffin (2017), the FIPPs are beneficial to both individuals and organisations as they assist in ensuring how personal information should be used.

The FIPPs have gone through evolutions and iterations since its inception in the 1970s (Gellman, 2017), but its sole purpose is to uphold the personal information privacy (US Department of Homeland Security, 2008). The FIPPs comprise of eight principles, namely notice/openness, choice/individual participation, purpose specification, use limitation, access, security and safeguards, data quality/ integrity and accountability/audit (Cate, 2006; Chang, Wong, Libaque-Saenz & Lee, 2018; Guffin, 2017; OAIC, 2015; Teufel, 2008; US Department, 2008). These are depicted in Figure 2.4 below.

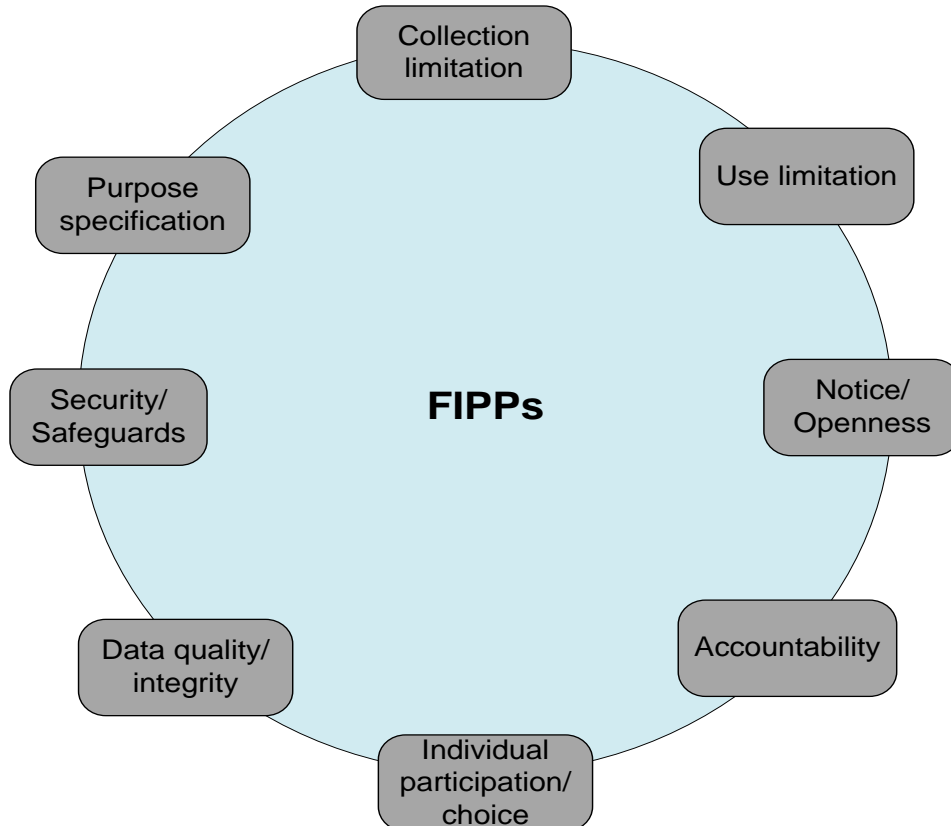


Figure 2.4: Fundamental FIPPs

A discussion of the FIPPs overview is done below.

- **Accountability** - this principle holds organisations liable for implementing the FIPPs and the conditions in a respective data privacy law. Reporting is also part of being accountable (Chang et al., 2018). It also stretches to offering training to employees on how they should use personal information and also auditing how the personal information is used and stored (Cate, 2006). Awareness campaigns by universities on personal information privacy related issues, the presence of security and privacy policies, putting in place the necessary security safeguards are some of the ways in which universities are accountable to privacy related issues.
- **Notice/ Transparency** - requires institutions and organisations to post notices, showing the manner in which, they will use personal information - how it is collected, protected, used, shared and disposed (Gellman, 2017; Sargsyan, 2016). Notice enforces disclosure of an organisation's information policies before the collection of any personal information (Chang et al., 2018). Developing a privacy statement/policy within an organisation is one way of achieving transparency of how personal information is processed (Teufel, 2008). This is done to achieve transparency with customers and employees and in the university context, with students.
- **Individual participation/ Choice** - provision granted to customers/people of selecting which personal information can be collected about them and how it can be used (Chang et al., 2018). It simply gives individuals an ultimate choice to participate on how their personal information will be used, normally called consent (US Department of Homeland Security, 2008). In a university context this could relate to sharing with third parties of their personal information, and students need to have the choice of sharing their personal details like names, cell phone numbers and email addresses.
- **Data quality/ Integrity** - The information should be relevant, precise, appropriate and, above all, complete in a bid to achieve the integrity of information (Teufel, 2008). The reason for information integrity is to reduce chances of using unfitting information and conclude a decision based on that

information (Gellman, 2017). As suggested by Guffin (2017), there has to be a way that individuals can also amend and correct their personal information so that their information maintains accuracy and completeness as attributes of secured information. Students might change their physical addresses, cell phone numbers, email addresses and they must have access to such information as and when they require to amend the information.

- **Security** - this touches on the controls that are in place for keeping the personal information secure and accurate to uphold information confidentiality, integrity and availability (Chang et al., 2018). It requires organisations to guard and defend the value and security of personal information (Guffin, 2017). This is one reason for which universities put in place security policies (Chua et al., 2017) to guide the implementation of security controls to protect student personal information.
- **Use limitation** - Use limitation entails using information for the specified purpose, as stipulated in the notice (Homeland Security, 2008; Teufel, 2008). When such information is to be shared by the university, there has to be consent or it must be for any other purpose that is in harmony with the initial purpose for collection (Guffin, 2017).
- **Purpose specification** – It states that personal information must be used only for the specified purposes in their policies (Cate, 2006). Personal data stored should be pertinent to the motive for their use as alluded to by Cate (2006). The university is compelled to provide a notice on the specific motive or purpose for collecting personal information and prescribe how it will be used, stored, processed, maintained, disclosed or disseminated (Guffin, 2017). Gellman (2017) highlights that the purpose must be specified before data collection time.
- **Collection limitation** - The principle states that information to be collected must be necessary and relevant to the accomplishment of a specified purpose and it means not to collect more personal information than what is required (Teufel, 2008). The type and quantity of information collected must be limited to that which is essential for the fulfilment of a specified task (Gellman, 2017). The collected information should only be maintained for a period spanning the

necessity of the information to accomplish a specified task (Guffin, 2017). Information must be collected by lawful and fair means and this must be done indiscriminately (Gellman, 2017).

The FIPPs are voluntary principles that encourage interoperability globally (Kokolakis, 2017). Though it is agreeable that FIPPs are not laws, they formulate the backbone of privacy laws and bestow the guidance on how personal information will be collected, used, stored, disclosed and protected (Teufel, 2008). They are relevant to this study because the FIPPs guidelines can easily be aligned with the ZDPA. They are also privacy fundamental practices that most countries ground their data protection regulations on (Tikkinen-Piri, Rohunen & Markkula, 2018), including Zimbabwe. The FIPPs are also relevant in this study because if the proposed Student Personal Information Privacy Perception (SPIPP) conceptual model is to be mapped to FIPPs, it becomes easier to adapt the model for other jurisdictions. It is also important to ensure that the SPIPP model is in line with international privacy principles, which means that its adoption will be in line with international standards. The FIPPs were instrumental in the formulation of other international privacy guidelines like the privacy principles that were used by the Organisation for Economic Cooperation and Development – OECD (Schwaig et al., 2006) and of particular importance to this study is their Protection of Privacy and Transborder Flows of Personal Data model of the OECD, which are discussed in the next section.

2.5.2 The Organisation for Economic Cooperation and Development (OECD) Protection of Privacy and Transborder Flows of Personal Data

The OECD Protection of Privacy and Transborder Flows of Personal Data document evolved from the founding principles of the FIPPs (Schwaig et al., 2006). The OECD is a distinctive forum where different governments address challenges facing the world (e.g. economic, environmental, technological and social) by working together (OECD, 2013a). The OECD's Protection of Privacy and Transborder Flows of Personal Data document is based on the notion that personal data protection within and across the borders is an important entity for gaining trust in e-government, e-business and any other online activities where information collection will be involved (OECD, 2007). According to the OECD Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013a), member nations must develop and adopt laws that protect privacy,

certify that there are no forms of intolerance against data subjects and adopt some complementary measures that are not limited to skills development, education and awareness as well as come up with technical measures that will help in the protection of privacy.

The OECD is on the lead in motivating efforts to assist institutions, organisations and governments to respond to challenges in governance, information economy and demographic population (OECD, 2013a). The OECD privacy document also states that it is the data controller's duty to account and maintain the integrity, confidentiality and security of personal data/ information of individuals (OECD, 2013a). The OECD member states met regularly to deliberate on issues affecting privacy within its member states and mapped some guidelines for nations to assist each other on privacy matters that might need brainstorming (OECD, 2013a).

The eight OECD privacy principles are collection limitation, purpose specification, data quality, use limitation, individual participation, security safeguards, openness and accountability (Cate, 2006; OECD, 2013b, 2013a). The following section gives an extract of the eight principles according to the OECD Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013a p. 14) document:

- “The **Collection limitation principle** stipulates that there has to be some personal data limitations on how it is collected. In addition, it should be done with full consent of the data subject”.
- “The **Purpose specification principle** also alludes to the fact that the purpose for collecting the personal data must be specified not later than the time of data collection”.
- “The **Data quality principle** dwells around the how personal data is aligned to the purpose, how it is supposed to be used for. Such data should be up-to-date, should be complete and accurate”.

- “The **Use limitation principle** states that personal information must not be used, made available or disclosed other than that it was collected for as specified when the information was collected”.
- “**Individual participation principle** discusses the rights of an individual which are not limited to challenging any data relating to him (this might yield data to be erased, data amendment, data rectification among others), receive some communication within a reasonable time frame on data concerning to him and the form of data should be readily intelligible to him”.
- The “**Security Safeguards principle** states that personal information must be protected against risks that include destruction, modification, use, disclosure, unauthorised access or any loss, deploy security safeguards which are reasonable”.
- “The **Openness principle** dictates that for the spirit of openness, there should be means of establishing the nature and existence of personal data, its identity, data controllers' residence as well as the main purpose of the data”.
- “**Accountability principle** indicates that the data controller should be responsible for complying with all the measures”.

The OECD Protection of Privacy and Transborder Flows of Personal Data document is crucial and relevant to the development of the SPIPP conceptual model. The researcher believes that the implementation of the eight OECD principles in a model abets in contributing to the quality of life for many individuals, institutions, governments departments, corporates and even nations at large with regards to privacy. Amongst all the international privacy regulations, the *OECD Protection of Privacy and Transborder Flows of Personal Data* has the most commonly used privacy guidelines (Tikkinen-Piri et al., 2018). The guidelines are reflected in existing as well as emerging data and privacy protection laws and, above all, they serve as the foundation/base for the creation of leading privacy programs practice and principles for many countries (Johnston and Wilson, 2012).

The conditions in the Zimbabwean Data Protection Act bill (discussed in Section 2.6) are similar to the OECD Protection of Privacy and Transborder Flows of Personal Data document principles and hence the relevance of this to the SPIPP in the development of the Zimbabwe privacy model for universities. OECD privacy principles are relevant in this study because if the SPIPP proposed is to be mapped with the OECD *Protection of Privacy and Transborder Flows of Personal Data*, it becomes easier to adapt the model for other jurisdictions. The OECD Protection of Privacy and Transborder Flows of Personal Data is an internationally recognised guideline for privacy, which means that its adoption is in line with international standards. The recently adopted GDPR is also important in the adoption of a privacy model for this study and is discussed in the next section.

2.5.3 The General Data Protection Regulation (GDPR)

The General Data Protection Act (GDPR) as a European regulation, was designed to focus on the privacy of personal data (European Union, 2016a; Larrucea, Asaf & Santamaria, 2020). The regulation compels companies to increase their transparency when they are handling and using consumers' (students') personal information, as noted by Bandara et al. (2020). The GDPR's scope also extends beyond the EU nations. According to the GDPR, all non-EU and international companies (and institutions) must comply with the GDPR if EU citizens' data are processed by them (European Union, 2016a; Tikkinen-Piri et al., 2018). This means that the GDPR is not bound by any territorial applicability/ territorial scope (Pelteret & Ophoff, 2016). Such a clause prompts the relevance of the GDPR in this study because although the GDPR is an EU regulation, its relevance is broad and it covers many countries and hence many institutions if EU citizen data is processed by them.

2.6.1 Aims of the GDPR

The main goal of the effective GDPR is regulating the collection and processing of personal data (Kaneen & Petrakis, 2020). This increases accountability and on how personal data is used (Cornock, 2018). The GDPR directs how companies as well as governments should collect and also process personal information for individuals, and provides a legal model in terms of companies' rights and obligations (Custers, Dechesne, Sears, Tani & van der Hof, 2017). However, preparedness for the GDPR

is not yet at the expected levels although companies are coming to terms with the provisions of GDPR and are increasingly complying. In case of failure of compliance (infringements), huge fines were put in place where a "total of 20million euros or an equivalence of 4% with respect to the total annual worldwide turnover of the previous financial year" is charged (Krempel and Beyerer, 2018). Cornock (2018) and Tankard (2016) are of the opinion that one of the positive things from the current GDPR as compared to predecessor privacy regulations is that it motivates organisations and companies to avoid data breaches as much as possible by securing their systems. Data breaches must be informed without unjustified delay and, if possible, within 72 hours after awareness of the breach, unless if there is reasonable justification (Allen & Overy LLP., 2017).

2.6.2 Relevance of GDPR in this study

As discussed, the GDPR makes its applicability very distinct as it focuses on personal data processing by processors and controllers within the EU member states, and EU citizen data that is processed in other countries (Larrucea et al., 2020; Tikkinen-Piri et al., 2018). If the SPIPP model is mapped with the GDPR, it can be applied in other jurisdictions in future. More so, Zimbabwe is yet to publish any privacy related guideline(s) and material, hence there is need to leverage on what other developed nations like those in the EU have done and customise it to suit the Zimbabwe scenario. This means that for the ZDPA bill to be effective, it also has to incorporate principles from many international privacy regulations including the GDPR, for easier integration. By aligning the GDPR to the regulations within the ZDPA, Zimbabwe will be in line with international standards in terms of upholding privacy.

The world is now one global village with rules and regulations in need of alignment for ease of integration by students who might intend to study in Zimbabwean universities. This implies that there is need for synchronisation even of how personal information is to be processed, aligning the GDPR for the EU nations and ZDPA bill in the proposed model. As noted by Cornock (2018), the GDPR is a pinnacle of ensuring industrial best practice which was intended to harmonise the data privacy laws in the whole of Europe, to protect as well as empower all EU citizens' data privacy as well as restructure the procedure companies and organisations across the data privacy domain.

The SPIPP model must conform to international privacy guidelines and best practice, so that it can be adopted to other jurisdictions. The GDPR is included because it is the most recent widely notable privacy development in Europe which has the potential to affect any nation globally directly or indirectly. Its flexibility to be customised is another factor, notwithstanding the fact that every nation that processes EU citizens' personal information will be obliged to abide by the demands of the GDPR to avoid privacy breaches. Cornock (2018) and Tikkinen-Piri et al. (2018) also attest that the GDPR aims to enhance how personal information is protected and integrated digitally amongst all European nations, since the previous directive was failing to meet the privacy requirements of the digitalised environment.

The next section discusses the ZDPA bill.

2.6 ZIMBABWE DATA PROTECTION ACT (ZDPA)

The government of Zimbabwe has designed many bills for various disciplines and such bills include those aligned to ICT usage (Chetty, 2013; Gambanga, 2016). One good example of an ICT bill within the last decade is the ZDPA bill (Zimbabwe Data Protection Act Bill, 2013). A closer look into the ZDPA bill summary analysis by Chetty (2013), indicates that there are privacy principles that match other international laws, which is a positive within the Zimbabwean context. These include its focus on personal information processing (which includes all personal data about any individual). In addition, the bill explicitly states that "the processing of personal information/data is prohibited unless the data subject has given consent in writing for such processing or as required by the law and that the consent can be withdrawn by the data subject at any time without any explanation and free of charge" (Zimbabwe Data Protection Act Bill, 2013, p. 18). It is meant to be a legislation that administers how public and private entities (including universities) processes personal information while safeguarding against the unlawful personal data collection and use (Chetty, 2013). It is very important to apprehend the fact that Zimbabwe is yet to promulgate the ZDPA and derives its foundation from international set of principles as its guidelines (Chetty, 2013), although motions are being moved to get the presidential assent as soon as possible (Gambanga, 2016) .

2.6.1 The Data Protection Authority of Zimbabwe

As stipulated in the Zimbabwe Data Protection Act Bill (2013), the Data Protection Authority of Zimbabwe will be a corporate independent establishment mandated to sue as well as being sued in its corporate name as the data enforcer. Some of its functions, according to the Zimbabwe Data Protection Act Bill (2013), in Section V, will include:

- Regulating the manner of processing personal information using various established conditions,
- Promoting and enforcing personal information processing environment which is fair,
- Submitting to the courts any breach that is not aligned to the fundamental principles of privacy protection model in accordance to the act,
- Receiving complaints from the aggrieved and instigate investigations, and
- Advising the relevant minister accordingly on information privacy rights.

2.6.2 Principles of the Data Protection Act bill

According to the Zimbabwe Data Protection Act Bill (2013), the principles of data protection can be divided into the quality of data and lawfulness of processing. These are explained as follows:

- **Quality of Data** - Personal information processing must be relevant, adequate and not immoderate to the purpose. This personal information must always be kept very accurate and always up-to-date. It has to be accessible, independent of the technology used to access it, i.e., technology evolution must not impact and considered an obstacle for the future processing or access of the personal information
- **Lawfulness of Processing** - The processing of the personal information must be mandatory, done fairly and legally, with the processing properly specified and explicit. Sensitive data might also be processed though it is very limited within the bill and when such processing happens, consent with the data subject is a prerequisite.

2.6.3 Roles of the data controller

The roles of the data controller are many as accorded by the Zimbabwe Data Protection Act Bill (2013):

- As stipulated by the Zimbabwe Data Protection Act Bill (2013), the maintenance of data integrity, its confidentiality and its privacy are all duties vested within the powers of the data controller in accordance with Article 24 in Section V.
- As stipulated by Articles 31, 32 and 33 in Section VI of the Zimbabwe Data Protection Act Bill (2013), processing of sensitive information is subject to consent, and the data subject might withdraw such consent anytime without any explanation.
- As stipulated by Article 23 Section V of the Zimbabwe Data Protection Act Bill (2013), the controller has to ensure that personal data processing is done necessarily, lawfully and fairly. This will take cognisance of the fact that it is collected for the specified and legitimate purpose, with all the reasonable regulatory and legal data protection provisions well in place.
- As stipulated by Articles 21 and 22 in Section V of the Zimbabwe Data Protection Act Bill (2013), when the controller intends to gather data from the data subject, they must specify the controller's name and address (or their representatives), aim of processing, state of compliance with request is compulsory or not, other information which is dependent on the specified processing nature as stipulated by the authority.
- As stipulated by Articles 25, 26 and 27 in Section V of the Zimbabwe Data Protection Act Bill (2013), the controller must take all the necessary steps to protect and safeguard personal information, using the appropriate standards for information security. If there is a breach, the data controller has to notify the Data Protection Authority of Zimbabwe without any delay.

2.6.4 Rights of data subjects

According to the ZDPA bill as highlighted in the Zimbabwe Data Protection Act Bill (2013), in Articles 31-38 of Section VI:

- The data subject has the access right to any personal information anytime, of the information pertaining to them being held by the controller.
- The data subjects also have the access right to personal information to modify, reduce limitations or rectify. This is not only applicable to when the processing is crucial in carrying out obligations and specified controller rights in the employment law field, or maybe the processing is done within the social security laws, or processing for data which the data subject has already made public, scientific research processing or better still, processing for the formation of defence of legal claims.

The next section provides for the mapping of the ZDPA bill with the FIPPs, the OECD Protection of Privacy and Transborder Flows of Personal Data and the GDPR.

2.7 Comparison of the ZDPA bill with the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data and the GDPR

The bill (ZDPA) will impact on how public entities, like universities, will process and use student personal information. There is need for privacy alignment to comply with the law if these universities are to evade paying large sums of money as fines. To better understand the bill and its relevance to other privacy regulations and principles, there is need to align it to the FIPPs, OECD and GDPR privacy guidelines discussed above. This will aid in assessing how the ZDPA compares with international standards as stipulated by the FIPPs, OECD privacy principles and the GDPR. Table 2.2 gives a summary for mapping the sections of the ZDPA to the FIPPs, the OECD and the GDRP sections.

Table 2.2: Summary of the ZDPA bill sections in alignment with FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data and GDPR sections

ZDPA Bill Sections	FIPPs	OECD	GDPR
Quality of data – section III	√	√	√
Sensitive information – section IV	√	√	√
Disclosure when collecting personal information – section V	√	√	√
Authority to process – section V	√	√	√
Security – section V	√	√	√
Security breach notification, obligation of notification and content of notification – section V	√	√	√
Internal controls and safeguards – section V	×	√	√
Openness of the processing – section V	√	√	√
Accountability – section V	√	√	√
Rights of the data subject – section VI	×	√	√
Penalties – section VII	×	×	√
Transborder flow - section X	×	√	√
Whistleblowing - section XII	×	×	√

From the table above, it can be seen that the ZDPA bill has covered many sections that are also included in the provisions of the FIPPs, OECD privacy principles and the GDPR. The comparison was done first on the headings of the privacy principles and regulations and then on the content of the subsequent sections. In the ZDPA bill, the main headings that are of importance to this study include quality of data, rules on the personal data processing, duties of data controller and rights of data subjects. The only difference is that the ZDPA allows for whistleblowing, which is a unique component as compared to other jurisdictions and principles except the GDPR. FIPPs and OECD do not include penalties and whistleblowing. The whistleblowing clause was established to increase chances of gathering information from the general public and, as such, there are procedures that are followed when whistleblowing, as explicitly explained in Section XII: Whistleblowing Zimbabwe Data Protection Act Bill (2013). FIPPs also does not address transborder flow, internal controls and safeguards and data subjects' rights and, in contrast, this is discussed by the OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPA bill.

2.7.1 FIPPs as the baseline for privacy model formulation

Using the FIPPs as the baseline in this study, the components from the OECD Protection of Privacy and Transborder Flows of Personal Data, the GDPR and the ZDPA bill were joined. The choice to use the FIPPs as the baseline was anchored on the fact that they are assumed to offer the underlying and founding privacy guiding principles in the self-regulation of personal information in this digital world (Cate, 2006; Gellman, 2017; Merwe & Staden, 2015). The OECD Protection of Privacy and Transborder Flows of Personal Data of 2013 was a review of the founding FIPPs, sustaining the fact that most privacy principles are grounded on the FIPPs (Gellman, 2017).

In the alignment of the ZDPA bill with the FIPPs as the baseline, the OECD Protection of Privacy and Transborder Flows of Personal Data and the GDPR, it can be noted that the ZDPA bill has paragraph headings like Accountability, Openness of the processing, Authorisation, Quality of data (data quality) and Security, which are similar to those of the FIPPs and OECD. To have a complete alignment with the FIPPs, an additional consideration was made on the content of the bill and paragraphs 21 and 22 discuss collection of information from the data subject (*collection limitation*), paragraph 17(1) discusses purpose for collecting information (*purpose specification*) and paragraph 32(1(a)) discusses limitations to the access and use of personal data (*use limitation*) (Chetty, 2013; Zimbabwe Data Protection Act Bill, 2013). Table 2.2 below shows the eight FIPPs principles as the baseline and how it maps to the OECD Protection of Privacy and Transborder Flows of Personal Data document, the GDPR and the ZDPA.

Table 2.3: Summary of privacy components grounded on FIPPs guidelines

FIPPS principles	OECD	GDPR	ZDPA
Notice/ Openness on information sharing (Homeland Security, 2008 on FIPPs; OECD Paragraph 15c; GDPR 103, 122, 132 & Article 57(b) & (d); ZDPA paragraph 13(1)(b)).	√	√	√
Individual participation/ choice (Homeland Security, 2008 on FIPPs; OECD Paragraph 13; GDPR Paragraph 18(1); ZDPA paragraph 30).	√	√	√
Use limitation (Homeland Security, 2008 on FIPPs; OECD Paragraph 10, ZDPA paragraph 32(2(a))).	√	√	√
Purpose specification (Homeland Security, 2008 on FIPPs; OECD Paragraph 9; GDPR Paragraphs 45, 156 & 162; ZDPA paragraph 17, 21 & 22).	√	√	√
Collection limitation (Homeland Security, 2008 on FIPPs; OECD Paragraph 7; GDPR Chapter III Article 15; ZDPA paragraph 32).	√	√	√
Information quality (Homeland Security, 2008 on FIPPs; OECD Paragraph 8; Article 47 (2)(d); ZDPA paragraph 15).	√	√	√
Security controls and safeguards (Homeland Security, 2008 on FIPPs; OECD Paragraph 11 & 17; GDPR Paragraphs 49, 83,94; ZDPA paragraph 24).	√	√	√
Accountability (Homeland Security, 2008 on FIPPs; OECD Paragraph 14 & 15(a); GDPR Paragraph 85; ZDPA paragraph 30).	√	√	√

From the table above, the OECD privacy principles, the GDPR and the ZDPA all have the basic eight principles as set in the FIPPs privacy principles. This underlines the fact that the ZDPA is aligned and in line with the fundamental international privacy principles and guidelines.

2.8 CHAPTER SUMMARY

In this chapter, the researcher carried out a scoping review to synthesise, analyse and discuss key privacy concepts and components, define privacy related terms and affirm the gaps in research. An overview of international privacy guidelines, namely, FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data was done. Also done was an overview of the GDPR. To finalise the chapter, the Zimbabwean Data Protection Act bill (ZDPA) was discussed, concluding with a comparison between the ZDPA bill, FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data and the GDPR. The next chapter focuses on discussion of student privacy awareness, expectation of privacy and students' confidence on the university, as well as the various privacy components, formulating the privacy perceptions that will lead to the development of the SPIPP model.

CHAPTER THREE: INFORMATION PRIVACY PERCEPTION CONCEPTUAL MODEL

3.1 INTRODUCTION

This chapter addresses the concept of information privacy perceptions based on the three main concepts, namely awareness of privacy rights, student expectations on the privacy of their personal information and focusing on student confidence in the university to meet privacy expectations and to comply with privacy regulatory requirements. It also executed a theoretical analysis of the relevance of the various policies, models and privacy principles like the FIPPs, OECD, GDPR and the ZDPA bill which formulates components needed for the attainment of the three main concepts, and this ultimately led to the privacy conceptual model development. This chapter attempts to achieve the theoretical aims in section 1.5.2, namely i) to conceptualise privacy awareness of students from a theoretical perception, ii) to conceptualise privacy expectations of students from a theoretical perception, iii) to conceptualise student confidence in academic institutions from a theoretical perception, and iv) to develop a conceptual model of privacy awareness, expectations and confidence of students from a theoretical perspective.

3.2 CHAPTER OVERVIEW

The chapter is segmented into five main parts. These are:

- First Part: Section 3.3 - The concept of information privacy perceptions is discussed and then the researcher proposes a definition of privacy perceptions. The social contract theory will also be discussed.
- Second Part: Section 3.4 – Privacy within the university-student context, discussion of privacy concepts.
- Third Part: Section 3.5 – Discusses the six privacy components that constitute the conceptual (SPIPP) model.
- Fourth Part: Section 3.6 – Consolidation of privacy components by adding privacy policy, privacy education and consent, together with the other six components.

- Fifth Part: Section 3.7 - The development of the SPIPP model – defining a conceptual model and discussion of the three main concepts and conceptual model components adopted from the discussion.
- Sixth Part: Section 3.8 – Theory on information privacy perceptions instrument.
- Seventh Part: Section 3.9 – Summarising chapter three.

A summarised snippet of this chapter’s discussions is shown in Figure 3.1.

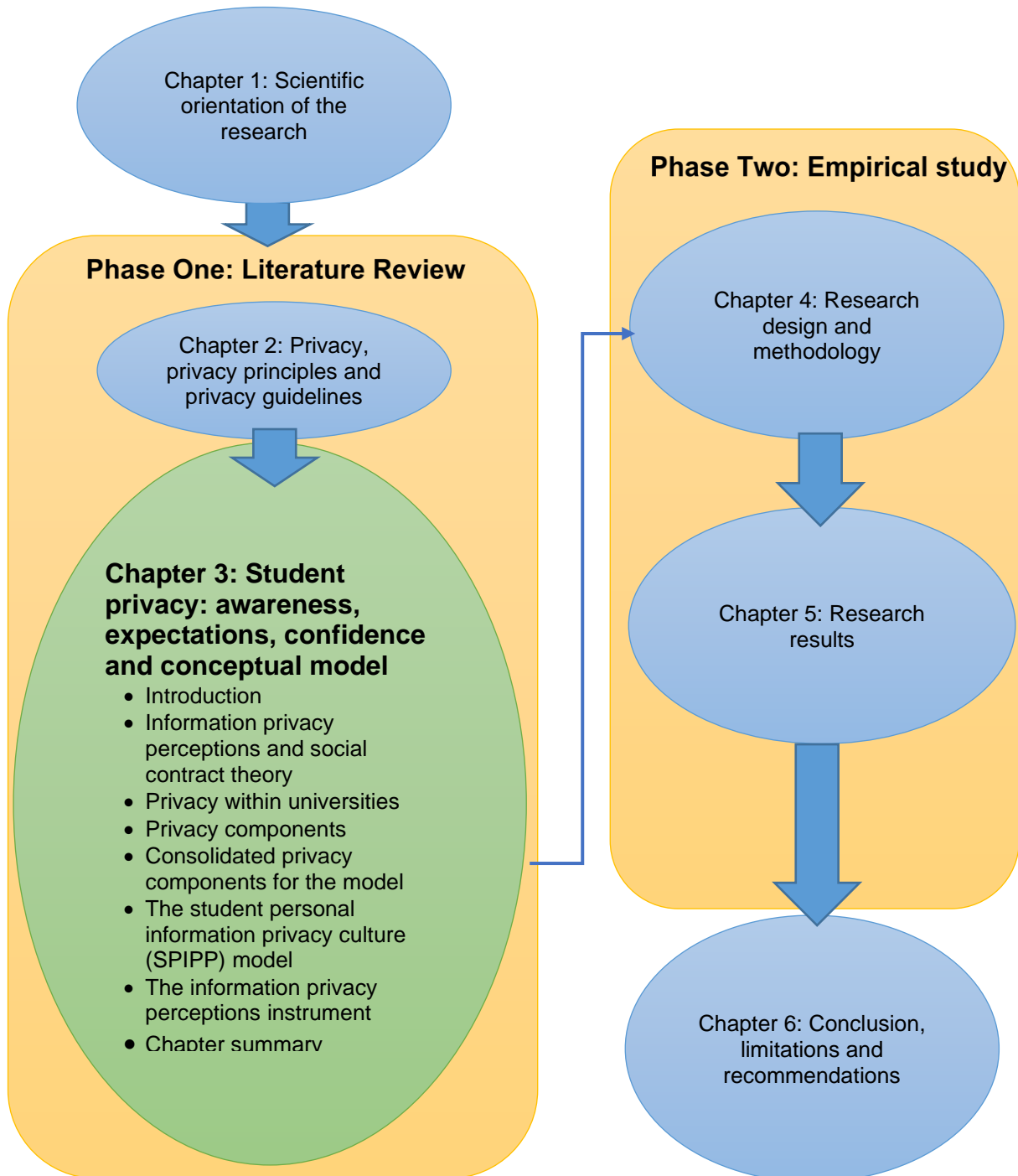


Figure 3.1: Chapter summary flow chart (Source: Developed for this research)

3.3 INFORMATION PRIVACY PERCEPTIONS

This section presents an overview of the information privacy perceptions and gives a discussion on the social contract theory.

3.3.1 Overview of information privacy perceptions

The university must comprehend the privacy perceptions of students in order to better protect the students' personally identifiable information collected by the university. As observed by the researcher, the university collects and uses students' personal information for various uses in areas like the admissions department, registrar's office, finance department, accommodation, health related information etc. More focus must be invested in the perceptions of individuals (students) on the sharing and the readiness to provide their sensitive personal information (Choi et al., 2017). These perceptions on privacy are expected to change as students are exposed to life experiences (Da Veiga, 2008) and their perceptions are dependent on awareness, their expectations and their confidence levels within the context of this research.

Increasing awareness of the students can be done in many ways. The use of a privacy policy is an imperative method of escalating the awareness perceptions of users in privacy control and planting positive perceptions related to privacy risks (Hooda and Yadav, 2017). In fact, the presence of a privacy policy was discovered to induce a favourable individual perception on privacy (Capistrano and Chen, 2015). In other words, privacy policies increase awareness of the privacy of customers' sensitive personal information. The use of such policies emphasises that focus must be invested in the perceptions of individuals (students) on the sharing and the willingness to provide their sensitive personal information (Choi et al., 2017). The mere presence of a privacy policy can enhance their willingness to share.

Wu, Vitak and Zimmer (2019) argue that many scholars have tried to identify various privacy behaviours and perceptions of individuals but there exists a gap on using the findings for policy suggestions and formulations. Warren, Sulaiman and Jaafar (2014) indicate that if trust is developed, there is reliance on the systems present and this will result in positive perceptions and willingness to participate even in personal information sharing. Individuals perceptions on privacy protection through regulatory

means is deemed salient in ascertaining their trust in organisations/ institutions in relation to information privacy ((McKnight et al., 2002; Miltgen & Smith, 2015). Availability of control options within a privacy system can also increase users' trust, which will permit them to disclose their personal information and hence positive perceptions (Ge, Peng & Chen, 2014).

Having low security levels can negatively impact on the perceptions of the students on the privacy of their personal information and this can diminish the trust levels because privacy has an effect on students' perceptions and trust (Arapaci, Kilicer & Bardakci, 2015). Kyobe (2010) bemoans the lack of awareness in security (which is believed to overlap with privacy) (US Department of Homeland Security & Homeland Security, 2017) within universities might result in their privacy being compromised. In a survey to find the awareness and perceptions of students on the protection of their personal data (Chen & Ismail, 2013), students declared that it was the duty of the institution to abide by the privacy rules, not theirs, and this was a main contributor to challenges in personal data protection.

Privacy concerns have been a complex dimension in the digital age of information technology research (Kruikemeier et al., 2020; Mamonov & Benbunan-fich, 2018; Ozdemir et al., 2016; Sodiya & Adegbuyi, 2016). Personal information privacy is an international area of concern (Hallam & Zanella, 2017; Miltgen & Smith, 2015) and as such, students in Zimbabwe are also affected. This will eventually affect Zimbabwean students' expectations on privacy and it could impact negatively on student confidence levels that the university will be able to securely process their personal information since Zimbabwe does not exist in isolation from the global space. It becomes difficult to guarantee data protection when there is no way of guaranteeing how students' personal information will be processed.

As suggested by Stange (2011), there is need for a better comprehension of students' perceptions on the privacy of their personal information so that recommendations can be made on how to engage and improve privacy of their personal information. Implementing the recommendations will increase the students' confidence in the university's handling of their sensitive personal information. Da Veiga (2018b) points out that the privacy confidence concept is represented by the perceptions of an individual on whether the organisation is processing their personal information in

alignment with the privacy regulatory requirements. The purpose was to ascertain the level of privacy compliance, which has the potential of giving them trust in the institution. Therefore, if the privacy expectations of the students are not being met, it means that the university will have to alter the awareness criteria they use to impart privacy knowledge to students.

In this research's context, information privacy perceptions are suggested to cover the three basic concepts, namely the privacy expectations, the privacy awareness and the student's confidence levels in the universities' capability in upholding information privacy. These privacy perceptions are crucial, especially in guiding how individuals within an organisation are supposed to behave (Da Veiga & Martins, 2015). The most important aspect in grasping these perceptions within an organisation is privacy awareness, which gives people an apprehension and cognisance of the organisation's information privacy (Sung & Kang, 2017). It also helps in preventing privacy breaches, as alluded to by Sung and Kang (2017). This position information privacy perceptions of students as a very important factor in privacy compliance and hence the need to appreciate them within universities. The three concepts are discussed in Section 3.4 below with the aim of discussing their relevance to the information privacy perceptions under study.

3.3.2 The social contract theory on privacy

The social contract theory is defined as the mutually beneficial agreements that a society can naturally develop and agree on the use and protection of personal information (Kruikemeier et al., 2020; Martin, 2018). It is more of a tacit agreement that is entered by members of a certain society, according to Casman (2011). Kruikemeier, Boerman and Bol (2020) perceived it as an imaginary contract that a group of people feel when they share their personal information. The social contract theory posits that privacy is governed by shared norms and values within a particular society (Bandara et al., 2020). These privacy norms can be adjudicated using the social contract theory, resulting in the assumption that many users would not want their personal information to be compromised (Martin, 2015). Using the social contract theory to privacy, there is need to comprehend the privacy norms on why, what and whom the information within a community is shared (Martin, 2018). Martin (2018) argues that a community or a relationship can have stated and unstated informal

privacy agreements (social contracts) that the groups or individuals can either respect (adhere to) or violate.

Even with the presence of privacy concerns, users who view privacy as a social contract can continue transacting based on procedural, moral norms, and hypothetical contracts. Therefore, despite the privacy concerns, users can still have positive perceptions based on the social contract theory according to Kruikemeier, Boerman and Bol (2020). Although the user is concerned about information disclosure, they can still proceed with the personal information sharing with the organisation based on the social contract theory (Bandara, Fernando & Akter, 2020). Only when there is less reliance on the social contract will the user adopt a particular behaviour, trying to safeguard their personal information privacy (Kruikemeier et al., 2020).

Using the social contract theory, an analysis of student awareness perceptions can be done and, whether institutions are meeting the privacy expectations of the students. As pointed out by Martin (2015), meeting student expectations through the social contract theory propagates trust and confidence, resulting in positive perceptions. In actual fact, trust and lack of it can be viewed as a result of either the organisation meeting or violating the user's contextual privacy expectations (Martin, 2018). Interestingly, Martin (2018) indicates that users tend to feel safe in continuing transacting even if there are perceived lower risks to the rules of contact based on the social contract theory. The student's assumption is that the university will gather and use the personal information in accordance with the procedural and moral norms. In context, the university must note that once the students are given a reason to be concerned about how the university is handling their personal information, they can easily develop negative perceptions towards the social contract theory (Martin, 2015).

3.4 PRIVACY WITHIN UNIVERSITY – STUDENT CONTEXT (THE THREE CONCEPTS)

The privacy of personal information is a notion that requires to be observed and grasped in a university setting. Students have their peculiar privacy expectations as well as privacy awareness levels, which lead to the accumulation of confidence in the university by the student, especially when the university meets the expectations on privacy (Alnatheer, Chan & Nelson, 2012). The three concepts, namely the privacy

awareness, the privacy expectations and the confidence of students in the university, are portrayed in Figure 3.2 below as the initial building blocks within the conceptual model. The three concepts are deliberated from the perspective of student.



Figure 3.2: Conceptual model for privacy concepts

The awareness, expectations and confidence concepts on privacy with regards to the university are discussed in the following sections.

3.4.1 Student privacy awareness

This section covers the awareness of students on their rights on privacy, awareness of university privacy policies as well as students' awareness of university awareness programs. Privacy awareness is the first concept under this study that has influence on students' perceptions on their personal information privacy. Awareness is realised when individuals seem informed about the organisation's privacy principles, especially on how personal information is used (Fortes & Rita, 2016). Therefore, the university has to do all it can to increase students' awareness of privacy issues.

The awareness level of students will increase if students are informed periodically about the risks to their privacy and if they are educated about how best they can control their personal information (Malandrino et al., 2013). This is so because they will be cognisant and appreciative of the value of privacy to their personal information. Research by Hooda and Yadav (2017) indicates that the millennials are in need of awareness campaigns on privacy. These millennials represent a large number of the university students. The students will need to be aware of all the possible vulnerabilities *a priori* when they are to use any online platform at university level (Yang & Wang, 2014). From literature, Lawler and Molluzzo's research resonate with Isabwe and Reichert (2013), who recommend that universities must promote privacy awareness, in the process allowing students to have control over giving consent or

even not, especially when handling personal information. This will result in the development of positive perceptions.

Results of different study (Yang & Wang, 2014) show that students from both China and Japan are aware of their private protection legally but they have limited knowledge on the privacy laws. Their study was broad in the fact that it covered two great Asian nations (Japan and China) assessing student awareness in privacy; unfortunately, it was only limited to privacy in eLearning. The awareness campaigns and other various training programmes will aid in mitigating and reducing various privacy related issues (Tikkinen-Piri et al., 2018). This will yield positive perceptions on privacy. To help the students value their own privacy as well as reduce their depth of exposure when online at universities, they expect these awareness campaigns more often (Chen & Ismail, 2013).

Awareness gives a discernment about a situation just as notice, which is amongst the FIPPs' fundamental principles for information privacy (Vail, Earp & Antón, 2008). One way of increasing awareness is by using privacy notices by the university (Vail et al., 2008). In view of this, it follows that users including students, also need to know the importance of awareness of privacy rights and privacy policies by university, particularly when they are using electronic means (Kyobe, 2010a). Privacy policy compliance by the university, as posited by Botha et al. (2015) and Kyobe (2010a), goes arm in arm with awareness since the lack of awareness signifies that a user will not going to be privy to the finer specifics for compliance, resulting in student non-compliance on privacy issues. Fink (2012) also states that privacy awareness can be useful for the creation of an atmosphere in which all students are well-informed about privacy associated issues, which can assist in their partaking in all university related tasks. Privacy policies are valuable for increasing awareness (Chua et al., 2017). Student awareness of privacy matters can be improved by encouraging students to read the privacy policies.

When awareness is prioritised, students can exercise their rights and consent to the handling of their personal and sensitive data as afforded to them within the privacy policies (Isabwe & Reichert, 2013). This happens because the students will be cognisant and aware of their privacy rights. The Zimbabwe privacy act implores that it is the obligation of the organisation as the data controller to distribute knowledge and

to increase awareness to the customers (Zimbabwe Data Protection Act Bill, 2013). As an effective privacy practice, an organisation (university) must periodically carry out information on privacy training sessions to ensure that its employees and all relevant stakeholders are equipped with privacy related information (OAIC, 2015). When awareness is a primary concern for an institution, privacy risks tend to be under control (Nasir, Arshah & Ab Hamid, 2017; Pensa & Di Blasi, 2017). In some instances, there is need to make sure that the awareness programs are tailored in such a way that they also incorporate various demographic levels as well as different cultural aspects (Mohammed & Tejay, 2017). This is done to try and reach out to all age groups on awareness issues.

A research conducted by Lawler and Molluzzo (2011) evaluated the extent of student awareness of all privacy dimensions like age differences and gender differences among other dimensions and advocates the need to familiarise users with the privacy policies within the social network sites. As deduced from the study, 56% of the students did not read privacy policies and 67% of them were not sure if their personal information could be used in any other way. Further research indicates that if people (in this case students) were aware of all the information that they disclosed about themselves ignorantly, they would come up with ways of preventing it and upholding privacy of their personal information (Malandrino et al., 2013). This is complimented by research results of Chen and Ismail (2013), which showed that students lacked in-depth knowledge of privacy but were aware of personal information privacy, i.e. awareness does not translate to understanding. They argue further that 50% of students simply agree to the terms and conditions for the sake of continuity, without reading the contents. Chen and Ismail's (2013) survey on student awareness and perceptions of the personal information protection and privacy discovered that in as much as the students might be aware of the protection of their personal data, they still don't know the consequences of using personal data illegally because of their limited knowledge on awareness. Increasing awareness can open the gateway for compliance by the university.

Awareness is considered a prerequisite for compliance (Fink, 2012; Isabwe & Reichert, 2013; Kyobe, 2010a). Lack of awareness in one's privacy obligation will eventually result in privacy compliance failure by the student (Botha et al., 2015). Since compliance is crucial, both the university and student must comply with the privacy

act. Awareness of risks associated with information sharing *a priori* will also help in reducing privacy concerns as the students will be able to put in place proper protection mechanisms for their sensitive data (Aghasian et al., 2017; Isabwe & Reichert, 2013). Nwaeze, Zavarsky and Ruhl (2017) research also suggests that compliance with privacy of personal information as well as low privacy concerns result from proper awareness initiatives within organisations. However, for compliance to be a fully understood and appreciated concept, the data controller (the university) has to play a pivotal role (OECD, 2013a). Training students on information privacy awareness can improve student knowledge on privacy, which reduces chances of them becoming victims, especially on privacy related issues (Manworren, Letwat & Daily, 2017).

Research results (Botha et al., 2015) indicate that sometimes users are not too concerned about the effects of certain legislatures and policies because they lack awareness. There is the general troubling questions as to why we still have data privacy issues even when policies and guidelines have been on the increase to cater for awareness (Sodiya & Adegbuyi, 2016). This is also corroborated by Govender (2015) who posits the key question i.e. *why do we still have many privacy concerns and issues when organisations and institutions are compelled to align with various data privacy policies?* It should be noted that even with the increase in the growth of privacy awareness and any other privacy laws and policies, sometimes it does not have any reciprocal effect in reducing the amount of data collected and processed about the user (Sargsyan, 2016). This is so because, according to Degroot and Vik (2017), privacy issues are complicated and organisations now thrive on the availability of information to survive.

Therefore, it is imperative that the organisation prioritises increasing privacy awareness of its employees so as to convince the employees to alter their behavioural tendencies towards compliance (Ortiz et al., 2018). Researchers (Isabwe & Reichert, 2013; Lawler & Molluzzo, 2011) made recommendations that universities must promote this privacy awareness, which will consequently allow students to have control over their personal information through consent. This will result in positive privacy perceptions on awareness.

3.4.2 Student privacy expectations

The second privacy concept under discussion in this study is privacy expectations. This section covers the students' expectations on their privacy rights and expectations on how the university must handle their personal information. The perceptions of customers can differ based on their expectations with the organisation when handling and using their personal information (Martin, 2015). In addition, Da Veiga and Ophoff (2020) indicate that the expectations that organisations will meet such privacy expectations vary due to various factors like their demographic profiles or culture. In the process of meeting the customer privacy expectations when processing their personal information, the organisations also need to comply with the data protection legislations (Da Veiga, 2018a). Student privacy expectations are likely to vary due to factors like age, courses under study and backgrounds. Although the study by Schumacher and Ifenthaler (2018) was limited to e-learning, it indicated that if user expectations are met, users will have more control on their personal information, leading to more disclosure. It is also imperative to recognise the fact that most of the privacy expectations can be grounded on social contract, within a certain community or society (Martin, 2015). There are certain expectations that are a result of societal norms and values, and students will simply rely on the social contract approach in such privacy instances.

When students go to a university, they have a certain level of expectations on privacy when they share their information with the university (Mamonov & Benbunan-fich, 2018). Talib et al. (2014) argue that sometimes these expectations are misplaced. Therefore, it is the duty of the university to meet the privacy expectations of the students. Although Hossain and Zhang's (2015) was limited to online social networks, it reported that if user expectations are met, users will have more control on their personal information and more disclosure. This is also corroborated by Schumacher and Ifenthaler (2018), whose study was, however limited to e-learning analytics. As a result, there is need by the university to meet the student privacy expectations, especially in controlling how they disclose their personal information.

FIPPs acknowledge that individuals can expect to have privacy of their personal information (Cate, 2006). These individuals have different privacy expectations in real life based on their experiences, their goals and the social contract theory (Martin,

2015) and there is need to come up with ways of monitoring and controlling these expectations (Ackerman & Mainwaring, 2005). The university must also thrive to achieve students' expectation of fairness (Vail et al., 2008). Because of the stiff competition that exists amongst the universities, universities now need to appreciate the fact that the student expectations and perceptions matters in gaining a competitive advantage as they seem to search for universities that align with their information needs including privacy (Almadhoun, Dominic & Woon, 2011).

In addition, institutions need to intersect with privacy expectations of the students in a bid to avoid various forms of lawsuits (Smit et al., 2009) in case of breaches. The law must be seen to be enforcing individuals' expectation of the right to privacy of personal information (Capistrano & Chen, 2015). The student will be expecting the university to uphold privacy, which will ultimately give them trust (Callanan, Jerman-Blažič & Blažič, 2016; Gellman, 2017). Furthermore, the organisation (institution) also has a certain level of expectations on how the personal information should be managed and used according to the laid laws (Burdon, Lane & Von Nessen, 2012). For the students to express their own personal expectations on how their personal information will be used, awareness (discussed in section 3.4.1) must be the cornerstone to allow the student to appreciate privacy of their personal information (Krzych & Ratajczyk, 2013). This was also submitted in a study by Schumacher and Ifenthaler (2018) that showed that meeting the expectations of students on privacy increases their promptness in disclosing the required personal information details.

It is generally difficult to assist a subject (student) without a clear understanding of their expectations, hence the need for a clear understanding of their expectations within an organisation (institution) (Krzych & Ratajczyk, 2013). This implies that an understanding of student expectations can greatly aid understanding why people (students) violate privacy rules (Degroot & Vik, 2017). Negative perceptions of privacy expectations may negatively impact on an individual's sense of dignity, affecting the sense of control of the individual and eventually lowering their emotional well-being and self-esteem (Mamonov & Benbunan-Fich, 2015). This is valid especially if their expectations on privacy are violated, resulting in privacy breaches; therefore, there is need to protect their interests so that the way their personal information is handled will be kept under control (Acquisti, Friedman & Telang, 2006; Feri et al., 2016).

Good privacy policies must be cultivated and be used to translate the organisation's expectations into smart, specific and attainable objectives, which the student can easily meet and adhere to (Capistrano & Chen, 2015). Clearly stated rules and policies within universities are an expectation of students on how their confidential personal information should be treated, and it negates accidental missteps in handling personal information (Degroot & Vik, 2017). Even when the university is to process personal information, expectations are placed on privacy that the collection will be minimal and more so, relevant reasonable expectations on how personal information is obtained from the individual (Braun, Fung, Iqbal & Shah, 2018; Mo, 2014).

Martin (2015) argues that socially acceptable behaviour within a society can shape privacy perceptions of users. It follows that people (students) have certain privacy norms like authorisations, prohibitions and commitments that they expect within a university (Kafali et al., 2017), and these are some of the benchmarks for privacy trust in universities and a violation of such norms results in privacy violations. In as much as the customer (student) has certain expectations in terms of how the processing of their personal information is done, it is largely the data controller's duty (university) to comply with privacy legislation to increase student trust and hence confidence that the university is meeting their privacy expectations and doing it within the legal model (Chang, Wong, Libaque-Saenz & Lee, 2018; Da Veiga, 2018b; McKnight, Carter, & Clay, 2009).

3.4.3 Student confidence in the university

This section covers the confidence of the student in the university observing the student privacy rights and to some extent, how the university must handle their personal information to instil confidence in the student. This is the third concept of privacy perceptions in this study.

Confidence is a result of trust (Huang & Bashir, 2016). This trust is one of the crucial factors in the development of a new relationship, and trying to foster information sharing is trust (Hina & Oxley, 2014). Therefore, if universities could avail themselves in a transparent manner, students would feel empowered and it would enable a sense of trust and would consequently boost student confidence and be easy to collaborate in giving out more information (Dwyer & Marsh, 2016). One of the ways of creating

trust is the presence of privacy notices within organisations (discussed in section 3.4.1), which will ultimately result in the emergence of confidence (Chua et al., 2017; Stange, 2011). An individual's comprehension of how their personal information is used after being collected is crucial for building trust (Lancelot & Smith, 2019).

Chua et al. (2017) and Fortes and Rita (2016) submit that privacy concerns poses a negative consequence on trust, which will result in negative perceptions of students' confidence levels. Adding to the privacy concerns is the presence of privacy breaches that are believed to impact negatively on trust and confidence, resulting in users being reluctant to expose themselves (Anjum et al., 2018). This might affect students, resulting in their reluctance to share their personal information which is processed by the university. Because of the continual privacy concerns of how privacy breaches will harm consumer (student) confidence levels in organisations when they handle their personal information, stakeholders concerned must adopt new solutions (Bush, 2016). The university ought to come up with ways of increasing the confidence of students on their personal information privacy.

Users can develop positive confidence perceptions that the organisation will not misuse their personal information (Huang & Bashir, 2016). This is a result of people having trust in an organisation handling their personal information safely, resulting in having more reliability of the social contract and increasing their likelihood of sharing their personal data (Kruikemeier et al., 2020). In the same study (Kruikemeier et al., 2020), it was concluded that consumers (students) have low confidence perceptions in that organisations are protecting their personal information, which negatively impacts on the social contract. In a bid to ascertain the confidence perceptions of customers on whether the organisations are handling and processing their personal information in check with regulatory requirements, Da Veiga (2018b) discovered that consumers (students) had low confidence levels in organisations. This results in the breach of the social contract and even trust (Da Veiga, 2018b), which is fundamental for instilling confidence and willingness to engage (Dwyer & Marsh, 2016). Huang and Bashir (2016) argues that trust is a dominant factor in privacy. Indications are that consumers (students) are very concerned with how their personal information is being used by organisations and this affects their trust in the organisations (Da Veiga & Ophoff, 2020). It is important to analyse the confidence levels of consumers (students) to ascertain their perceptions levels because it will cascade down and result in privacy

compliance (Da Veiga, 2018a). Confident students were found to be prepared to part with their personal information (Stange, 2011).

If a university pledges privacy, it affords a sense of faith and trust, thereby instilling confidence, resulting in positive information privacy perception that can be witnessed within the entire institution (Alnatheer, Chan & Nelson, 2012; Chua et al., 2017). The commitment from the data controller to protect privacy of personal information using the privacy policy reduces the emergence of negative perceptions as a result of privacy related issues (Hasbullah et al., 2013; OECD, 2013a; Tan et al., 2014). A confidence instilling and an effective data protection mechanism must have well documented formalities of filing concerns or complains (Adelola et al., 2014), which consequently yield confidence and trust (Sodiya & Adegbuyi, 2016).

Trust that is correlated to confidence (OECD, 2013b) is defined by Vail et al. (2008, p.443) as “the belief that the trustee will act cooperatively to fulfil the trustor’s expectations without exploiting its vulnerabilities”. The OECD (2013b) defines trust as an element of gaining confidence in someone or something and as a fundamental attribute that binds relationships between stakeholders in an institution as its loss will have serious negative consequences on the institution (OECD, 2013b). Through inference, it can be said that confidence originates from trust (Shen, Bernier, Sequeira, Strauss and Pannor, 2019). Most privacy concerns emanate from lack of trust between two contesting parties; for instance, the university and the student (Hasbullah et al., 2013). Lack of trust in stakeholders is attributed to failure in understanding (Hina & Oxley, 2014).

There is also need for the organisation (university) to understand the behaviour of people (students), as this will help in finding ways of addressing their interests in a bid to increase confidence (Akpojivi & Bevan-Dye, 2014). The emergence of positive perceptions on privacy by individuals creates a privacy culture within an organisation that respects and upholds privacy and creates an environment that inspires trust and confidence in the university by the students (OAIC, 2015). In some instances, trust fails to align with the privacy environment (Hossain & Zhang, 2015). This is so because users normally trust a privacy model that will assist them in notifying them of potential privacy related issues and, as a result, they gain trust and confidence (Callanan et al., 2016). Trust is a situation when students have absolute belief that the learning

environment is credible and reliable, and this is an acute element in seeking confidence (Dwyer & Marsh, 2016). To some extent, presence of restrictive measures by universities when handling personal information increases trust and confidence of students (Kafali et al., 2017).

Giving customers (students) extra control on their personal information can be a major boost in terms of confidence (Dwyer & Marsh, 2016; Rao, Chen & Dhillon, 2014). One way of giving users control over their personal information is through privacy training. Cognisance of information privacy through training has the advantage of reducing risks and, in the process, raising confidence (Personal Data Protection Competency Model for School Students, 2016). In the Information Security Compliance Policy model designed by Nasir et al. (2017), training was considered one dimension that has the potential to yield security policy compliance and, consequently, privacy confidence in an institution. This will result in positive privacy confidence perceptions. There university must realise the need to make acquaint students of with privacy policies , as this can increase students' compliance to the privacy policies (Da Veiga, 2018b; Kurkovsky & Syta, 2011). Students need to feel optimism and having the ultimate control over their personal information, which will cultivate confidence in the institution (Chang et al., 2018; Rao et al., 2014).

Disclosure of personal information is premised on students' confidence in the university (Mamonov & Benbunan-Fich, 2015). As Da Veiga (2018b) suggested, confidence is product of an organisation (institution) that observes and respects privacy policies and rules when handling the personal information of a customer (student). In as much as students might have a positive mind set on analytics being done by universities using their personal data, they are also sceptical about privacy issues. In fact, when there is too much monitoring, students tend to be demotivated by such an act and lose confidence about the institution in the process (Schumacher & Ifenthaler, 2018).

The university has to appreciate the students' privacy *expectations* so that they can well protect the personal information of the students that they collect, which can ultimately increase the student confidence in the university when they are processing their personal information (Iachello & Hong, 2007). It is beneficial to the organisation (institution) to come up with ways of achieving positive privacy perceptions of people

(students) by making privacy policies easier and understandable and conducting privacy training workshops to increase awareness (Chua et al., 2017). Failure to instill positive perceptions on privacy will result in the emergence of problems in the privacy of personal information (Afroz, Islam, Santell, Chapin & Greenstadt, 2013; Chen and Ismail, 2013). In addressing the three concepts, there is also need to comprehend the privacy components that help in formulating the SPIPP conceptual model.

3.5 PRIVACY COMPONENTS

A revisit to the components in Table 2.3 indicates that these were measured from either the student or the university perspective. For the context of this section, discussions are done from the student's perspective. This means that the accountability and security controls and safeguards are not included in the final model for regulating privacy within a university. The remaining 6 (six) components include notice/openness to information usage, information quality, use limitation, purpose specification, collection limitation and individual participation/ choice as discussed below. These constitute the key components of the proposed SPIPP conceptual model.

3.5.1 Notice/ Openness

Notice and openness are inscribed in the Homeland Security (2008) document on FIPPs, the OECD Protection of Privacy and Transborder Flows of Personal Data Paragraph 12 & 15c, the GDPR 39, 58, 78, 103, 122, 132 & Article 57(b) & (d) as well as the ZDPA bill Paragraph 13(1)(b) & 29. Notice is amongst the most important principles of privacy rights from the FIPPs, and it increases awareness of privacy. While notices are assumed to increase awareness on privacy related issues, they also affords the data subject (student) with trust and hence confidence, which is important for the relationship amongst the parties concerned (Stange, 2011). There has to be a provision to cover notice both to the data controller and to the aggrieved individual in case of any data breach, and the requirement for the notification is that it should be very flexible to allow for the inhibition and avoidance of further damage (OECD, 2013b). Notices force institutions to be transparent and open as possible on how they will use personal information of data subjects (Gellman, 2017; Sargsyan, 2016).

Appropriate notice is required before the collection of personal information, used, processed, stored, disseminated or disclosed (Guffin, 2017). *Therefore, students need to be aware of the presence of privacy policies* (Chen & Ismail, 2013; Guffin, 2017; Sargsyan, 2016). When there is privacy breach, a notice has to be provided within the earliest possible time; the GDPR states that it has to be within 72 hours (Chang et al., 2018; Cornock, 2018). *Short, flexible and non-ambiguous is what students expect on the notices* (Preuveneers et al., 2016). In a bid to enable and promote awareness in institutions, a privacy policy can be used.

A student requires accessibility to all their private, sensitive and personal information (Azemović, 2012). If the university is open on how it will use student personal information, students will have confidence in the university because it is an indication of the institution's desire towards compliance with privacy (Isabwe & Reichert, 2013). As alluded to by Dwyer and Marsh (2016), institutions must be open with students on what they will use their personal information for so that they gain trust, which is needed in instilling confidence that the university really observes and respects their privacy. Openness also encourages student participation, in case there is need to gather more information from the students (Katell et al., 2016). *Everything about personal information must be so transparent on all the practices and policies, even how the personal information is going to be kept and used by the organisation, and this is done through publishing of privacy policies* (Guffin, 2017; Katurura & Cilliers, 2016; OECD, 2013a; Sargsyan, 2016; Zimbabwe Data Protection Bill, 2013). Confidence can also be increased when students realise the presence of controls and safeguards within an institution.

In summary, the importance of notices in this research relates to the following:

- Students know about privacy related issues through privacy notices (Guffin, 2017; Stange, 2011).
- Notices make organisations (institutions) as open and transparent as possible on how they will use data subjects' personal information and these are supposed to be publicised by the institution (Gellman, 2017; Sargsyan, 2016).

3.5.2 Information quality

FIPPs (Homeland Security, 2008), the OECD Protection of Privacy and Transborder Flows of Personal Data document Paragraph 8 and Article 47 (2)(d) as well as the ZDPA Bill Paragraph 15 clearly articulate information quality as crucial in upholding personal information privacy. As outlined by the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data and the ZDPA bill, information quality is an important attribute that has to be observed by the organisation (university) for information integrity (Cate, 2006; Guffin, 2017; OECD, 2013b, 2013a). In addition, Gellman (2017) and the US Department of Homeland Security (2008) indicate that *personal information must be complete, timely/up-to-date and accurate and must be appropriate for the purpose for use.*

Information quality is satisfied with the presence of information security and in his research, Banerjee (2015) defines information security as embroiled in three main dimensions formulating the CIA, namely confidentiality, integrity and availability. *It is the duty and entitlement of the agencies and universities to sustain information security for information quality* and for them to collect, create, process, store, use, manipulate, disclose or disseminate personal information with its desired attributes like relevance, accuracy, completeness and timeliness as reasonable as possible, in ensuring fairness to individuals and students (Guffin (2017). This will increase student confidence in the university, since they will trust that information will have integrity.

Most privacy policies, guidelines and bills discussed in this research view the information quality component as an important entity to this study because:

- Information must be complete, up to date and accurate and appropriate for the collection purpose (Homeland Security, 2008).
- It is the prerogative and duty of the university to make sure that they uphold information security for information quality (Guffin, 2017).

3.5.3 Purpose specification

The principle of purpose specification in FIPPs within the Homeland Security (2008) document, the OECD Protection of Privacy and Transborder Flows of Personal Data

Paragraph 9, the GDPR Paragraphs 45, 156 & 162 and the ZDPA bill Paragraph 17, 21 & 22. The OECD, GDPR, FIPPs and ZDPA bill all highlight the importance of specifying the purpose for collecting personal information (Chetty, 2013; Guffin, 2017; Homeland Security, 2008; OECD, 2013b, 2013a). As highlighted by Chetty (2013) in the ZDPA bill, *personal information should be processed for an explicit, specified and legitimate purpose which must be indicated on or before the collection time*. Therefore, use specification can be used hand in hand with the consent clause as it clearly states what information will be needed and for what it will be used (Merwe & Staden, 2015). *The principle compels the data collector to specify the purpose of personal information collection not later than the collection point* (Bonner & Chiasson, 2005; Cavoukian, 2009; OECD, 2013b).

According to Katurura and Cilliers (2016), once it is collected, the information must not be used or directed for any additional purpose which was not beforehand specified, except for other unavoidable reasons like fraud, avoidance of harm or for legal purposes. Students will expect the model to fully observe this clause. It also aids in raising their confidence levels and a reduction in privacy breaches and various privacy violations (OECD, 2013b).

In summary, the purpose specification component is crucial and:

- The university must specify the purpose and be explicit when collecting personal information (Chetty, 2013; OECD, 2013a).
- The university should specify the purpose for student personal information collection before or during the point of collection (Bonner & Chiasson, 2005; Cavoukian, 2009; OECD, 2013b).

3.5.4 Use limitation

The FIPPs stipulates that there has to be restrictions on the internal usages of information pertaining to an individual in a record keeping organisation (Gellman, 2017). According to the OECD (2013 p.14), *"personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law"*. Therefore, there is need for more focus

on the two concepts, i.e., consent by the student as the data subject and the authority of the law which can override everything. The student will expect a limit to the amount of information collected by the university and acquire the right to use the information through the student's consent (Cate, 2006; Teufel, 2008). This implies that the university has to use the student's personal information for the purpose specified in the notice (Guffin, 2017). There will not be any collection or any use of personal information without the mandatory consent (Cate, 2006). This means that the purpose must be clearly spelt out and explicit (Chandramouli, Grance, Kuhn & Landau, 2006). If there are other legal reasons for the student's personal information to be used, the student will comply (Preuveneers et al., 2016).

The importance of use limitation in this study as stipulated by the OECD (2013) rests on the following:

Personal information must not be disclosed, made accessible or used for purposes not specified in accordance with [the Use Limitation Principle] except:

- with consent from the data subject, or
- using the authority of the law.

3.5.5 Collection limitation

The Homeland Security (2008) document on FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data Paragraph 7, the GDPR Chapter III Article 15 and the ZDPA bill Paragraph 32 all state the principle of collection limitation as a fundamental requirement for achieving information privacy. When *personal information is being collected, it must be fair, lawful and limited for the only specified purposes* (Cavoukian, 2009). There must be limits and restrictions on how personal data is collected and such data must be obtainable through fair and lawful means and, where suitable and necessary for the specific purposes, with the data subject's consent and knowledge of the data subject (Cavoukian, 2009; Chetty, 2013; Gambanga, 2016; OECD, 2013a). The collection must be done by all lawful means and with consent of the data subject (Guffin, 2017). Collection of a large amount of personal information can be a cause of concern among students as it raises privacy concerns (Rasmussen & Dara, 2014). Data collection minimisation entails limiting the

amount of collected data as well as how this data will be retained by any company (Li, 2019). According to Li (2019), all data storage presents a conducive environment for data "thieves" whether inside or outside the company/organisation and as a result, they amplify the potential threats to the consumer (student).

In addition, Li (2019) highlights that large data retained by a company (institution) might be used in ways that contradict the consumer (student) expectations. Students expect the university to collect as little information as they can (Ivanova & Grosseck, 2015). According to Preuveneers et al. (2016), one way of ensuring information privacy is to limit as much as possible, the information collected by organisations and institutions for use, in the process reducing the number of privacy concerns. Limiting personal information collection gives an advantage of user participation in giving their personal information (Kokolakis, 2017). *There are limits regarding the type of collected information by an organisation (university) about individuals (students) and it should therefore be restricted to what is considered necessary for the specified collection purpose* (Cavoukian, 2009; Gellman, 2017). It must not extend to non-relevant issues like religion, political affiliation and ethnic origin among other issues.

The collection minimisation is significant, and:

- The university must collect information fairly, lawfully and only for the stated purposes (Cavoukian, 2009).
- The university must the limit collection of personal information that is not essential for academic purposes (Cavoukian, 2009; Gellman, 2017).

3.5.6 Individual participation / choice

FIPPs (Homeland Security, 2008), the GDPR Articles 12 - 15; OECD Protection of Privacy and Transborder Flows of Personal Data Paragraph 132 and Part VI Paragraph 31 - 32 of the ZDPA bill highlight individual access and participation to personal information. The right to access and individual participation must be active unless if it violates the rights of other individuals (Bellman, Johnson, Kobrin & Lohse, 2004; Homeland Security, 2008). Individuals (students) are given the right of choice; they can chose whether or not they want to participate in providing personal information (Chandramouli, Grance, Kuhn & Landau, 2006). In the OECD Protection

of Privacy and Transborder Flows of Personal Data principle, number 7 is the Individual Participation principle (Hughes, 2015; Iachello & Hong, 2007) and according to the OECD (2013a p.15), “an individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended”.

Every individual who has his personal information collected has the right to amend the information collected anytime (Gellman, 2017). This means that institutions must include students when they intend to use the students’ personal information by seeking consent and they must also cater for techniques of redressing and correcting should there be need. The data controller (university) must be able to provide responses to requests by the data subject (student) even on the personal information collected as confirmation (OECD, 2013a). Knowing who has access to one’s personal information as well as how they store it is very important within a university environment (Katurura & Cilliers, 2016).

A principle like individual participation was designed to smooth the path for instilling knowledge and participation on the individual (Cate, 2006). When a student challenges the university and wins the case on issues relating to his/her personal information, the information must be deleted, amended or altered to the student’s satisfaction (Iachello & Hong, 2007). A data controller can provide information about data subjects periodically to keep them informed (OECD, 2013a). Chetty (2013) posits that student personal information must always be accessible despite the fact that technology is dynamic and keeps changing, that is, technology must never be an obstacle that denies access or even the personal information processing. The right to participate granted to individuals (students) increases transparency and the language used to communicate with the data subjects has to be very clear and plain to increase understandability (Tikkinen-Piri et al., 2018).

According to the FIPPs, OECD, GDPR and the Zimbabwean Data Protection Act bill, the individual participation principle is relevant and important to this study. Therefore:

- Organisations (university) must provide a confirmation to the student as the data subject on the collected personal information (OECD, 2013a).
- The data subject (student) must follow the clearly set procedures when they make a request for confirmation on the collected personal information, as specified in the principle of Individual participation (OECD, 2013a).

The above 6 (six) components are part of the proposed SPIPP model (Section 3.7: The Student Personal Information Privacy Perceptions model). There are other proposed additional components that are fundamental in comprehending students' perceptions. These are discussed below.

3.5.7 Additional components

As suggested by Cate (2006), the most fundamental FIPPs principle is the notice and it is normally assumed by the use of the **privacy policy**. As an awareness document, a privacy policy discloses how organisations must collect, manage, disclose or use personal information related to an individual (Chua et al., 2017). Studies have revealed that privacy concerns are addressed in the privacy policies (Chua et al., 2017). A university will require a privacy policy if it to infuse awareness to the students. As indicated earlier, the university under study does not have any. Students also requires education related to privacy issues as a crucial component in having responsible students (Mohamud et al., 2016; Zorica, Biskupic, Ivanjko & Spiranec, 2011).

A study (Farooq, Kakakhel, Virtanen & Isoaho, 2016) also indicated that **privacy education** is one key measure of reducing information security concerns within an organisation/ institution. This means that any privacy model to be designed within a university environment must have privacy education as one important component. It can also be noted that with all the discussed components (notice/openness to information usage, purpose specification, information quality, collection limitation, use limitation and individual participation/choice), the student is involved through consent.

Central to the OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR documents and the ZDPA bill is **consent**, as it makes sure that the individuals' data are processed during collection only in a manner that is specified when the consent is granted (De Hert & Papakonstantinou, 2012). This is the right that is afforded to students to participate and be made aware of practices and disclosures in the life cycle of their personal information (Akalu, 2018).

Therefore, in addition to the six components highlighted in Table 2.3 in Chapter 2, the following are proposed to assess awareness, expectations and confidence of students within a university as argued in the above paragraph. These are part of the consolidated SPIPP model:

- privacy policy,
- privacy education and
- consent.

Below is a discussion of the additional components included in the SPIPP conceptual model.

3.5.7.1 Privacy policy

The scope of the privacy policy discussion is both the student and university perspective. *Privacy concerns can be allayed by having a clear and concise privacy policy* (Vail et al., 2008). Privacy of personal information can only be ensured and be realised if there are privacy policies in place to bind individuals, organisations, institutions and government (Kurkovsky & Syta, 2011). A privacy policy addresses many potential privacy breaches as it acts as a guideline for preserving personal information (Chua, Herbland, Wong & Chang, 2017; Kafali, Jones et al., 2017) in a bid to inform the people (students) about privacy related issues. Nasir, Arshah and Ab Hamid (2017) also posit that to reduce information security problems and privacy breaches and risks, a privacy policy has to be used within an organisation or institution. A privacy policy can be thought of as a notice that discloses how an organisation collects, manages, uses as well as discloses of a customers' personal information that relates to customers who are identifiable from that information an organisation possesses (Chua et al., 2017). Chua et al. (2017) also states that a privacy policy is a document that outlines how organisations handle any client/employee/customer

(student) data and information that they gather in their operations. Both definitions suggest that a privacy policy dictates how an individual's (student's) personal information should be processed.

The OECD advocates measures like having privacy policies as a solution to address compliance by the controller on the individuals (OECD, 2013a). Nwaeze et al. (2017) and the OCED (2013b) also suggest that changing of privacy polices more frequently causes users (students) to be confused and will lead to students being wary of the institution's privacy practices unless if it is for a broader use of personal information. When institutions display privacy notices, it helps in addressing students' concerns of privacy issues, in the process increasing student trust and willingness to give personal information when the need arises (Callanan et al., 2016; Nwaeze et al., 2018; Ullah, 2017). Students prefer privacy policies which are short and to the point so that they are not demotivated in reading them (Miltgen, 2009). This will at least motivate students to read them through. For example, Lawler and Molluzzo (2011) empirically deduced that 56% of people do not read their privacy policies, which will require the need to shorten them.

Some security breaches are due to the organisation lacking internal controls (like privacy policies) on how personal information is to be used (Ackerman & Mainwaring, 2005) and failure to put in place rules to govern personal information access (Gellman, 2017). Students only want information that they perceive to be very relevant and vital in a privacy policy as opposed to going through the whole document (Rasmussen & Dara, 2014).

A study by Govani and Pashley (2005) shows that 80% of students rarely read privacy policies. The university has to come up with user-friendly mechanisms of ensuring that students do read their privacy policies to increase their awareness of privacy related issues. Furthermore, Strange (2011) argues that some students do not have confidence in their institutions because the privacy policies lack vital clauses to ensure confidentiality of their personal information. A privacy policy document therefore has to be initiated by the university itself and make it part of the university policy, as rightfully pointed out by Strange (2011). *A privacy policy statement should be short, precise, clear, to the point and easy to understand and navigate by the students and,*

above all, it is the duty of the university to show how information is being handled and processed (Rao et al., 2014).

According to the FIPPs, OECD, GDPR and the Zimbabwean Data Protection Act bill:

- The university should have a privacy policy (Kurkovsky & Syta, 2011; Vail et al., 2008).
- The privacy policy should be easily understandable (Govani and Pashley; 2005; Rao et al., 2014).

The privacy policy is therefore relevant and important in this study.

3.5.7.2 Privacy education

Privacy education is not detailed in FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR or the ZDPA bill as part of principles, but it is included in the development of the SPIPP model because for awareness to be realised, there is need for thorough privacy education (Isabwe & Reichert, 2013; Yang & Wang, 2014). The OECD advocates measures like privacy education as a solution to address compliance by the controller on the individuals (OECD, 2013a). Education increases awareness according to Rezgui and Marks (2008). Therefore, privacy education is effective in terms of making key and informed decisions and it should be understandable to increase student awareness (Fink, 2012).

Privacy education is imperative as it enlightens the student why personal information is collected, how it will be used, the personal information sensitivity and what the student will get after sharing with the university their personal information (Young & Quan-Haase, 2008). As suggested by Fink (2012), privacy education can remedy students' lack of knowledge on privacy issues. Massive student education is needed, as students are sometimes ignorant (lack awareness) about understanding the motive behind privacy of personal information (Chen & Ismail, 2013; Isabwe & Reichert, 2013). There is need for an increase in public privacy education (students in this case) on how they should safeguard their personal information and how they should report a security breach (European Union, 2016b) according to the regulation 2016/679 of the European parliament and the Council of the European Union.

According to Gellman (2017), for the OECD model to be operative, privacy education is imperative in dropping privacy breaches. To increase privacy education, emphasis should be on privacy issues during teaching orientations as well as using student emails to distribute privacy related bulletins once or twice a semester (Fink, 2012). Privacy education in the form of workshops allows a live presentation by experts to the students and any issue that needs to be clarified will be attended to for students to fully grasp the privacy issues (Gellman, 2017). Coleman and Purcell (2015) *advocate for the university to have a bigger role in educating the student on the importance of privacy especially on the privacy of their financial details, protection of their personal mobile devices, identity theft on social media platforms, and monitoring of unauthorised access to their emails* As suggested by Botha et al. (2015) and Sargsyan (2016), *these privacy education sessions must be done frequently (continuously) as people (students) will need to be reminded continuously* and be informed well in time since the policies keep evolving as technology also evolves. For the university students and staff to fully appreciate privacy, there is need for some education and workshops to assist them in privacy awareness (Nwaeze, Zavarsky & Ruhl, 2017).

Privacy education is an important component to this study. Therefore:

- The university should have existing privacy education for students on the safe keeping of students' financial details, the protection of their personal devices, identity theft issues online, and monitoring of unauthorised access to their emails among security measures (Coleman & Purcell, 2015; Fink, 2012).
- Students will have to be reminded continuously through privacy education, of privacy related issues (Botha et al., 2015; Sargsyan, 2016).

3.5.7.3 Consent

Consent is discussed from both the student and university perspectives and it is not a principle but is rather imbedded in the FIPPs, the OECD Protection of Privacy and Transborder Flows of Personal Data, the GDPR and the ZDPA bill as a fundamental right required before sharing information (Homeland Security, 2008; OECD, 2013a; Tikkinen-Piri et al., 2018; Zimbabwe Data Protection Act draft bill, 2013). Consent is

the right of an individual to be communicated with and to or not give authorization when information relating to them is needed to be used (Federal Trade Commission, 2007; Swartz & Da Veiga, 2016). According to the OECD Privacy Model (2013) and the Zimbabwe Data Protection Act Bill (2013), consent of the data subject is an essential human right aspect in information sharing as the data subject is given the right to choose participation in personal information usage. Consent also entails granting users the right to have control of how personal information relating to them will be used except where inappropriate (Sargsyan, 2016). As outlined in the GDPR, the data subject must freely give consent, and should the data subject so wish to alter or even withdraw his/her own personal information, they must do so without any form of harassment or intimidation (European Union, 2016b; Personal Data Protection Competency Model for School Students, 2016).

According to the DLA Piper (2017), there are two types of consent regimes, namely the opt-in and the opt-out. Opt-in is when the data subject is giving the data collector the right to collect and use of information, whereas opt-out is the revoking of such a right to collect and use such information (Jordaan & Van Heerden, 2016). *Individuals are granted the choice and right of consent by opting-in for the personal information sharing* (Chua et al., 2017; Jordaan & Van Heerden, 2016). *If one does not want to continue sharing personal information or to receive certain communications, they have the right of opting-out* (Krishnan & Vorobyov, 2015; Swartz & Da Veiga, 2016).

Though policies and principles compel consent when student personal information is collected, there are exceptions for cases like when the information is needed for the prevention or detection of fraud/law enforcement, when the student is mentally incapacitated or seriously ill, for charity related issues, for medical, legal or security issues (Gellman, 2017). Taddei and Contena (2013) stress that students have to avail their personal information willingly without any form of pressure. In addition, students will be expecting the university to be clear when they want to collect data about them, and do this with their approval as this could improve their confidence in the university because they will feel involved (Taddei & Contena, 2013). As highlighted in research (Hasbullah et al., 2013; Miltgen, 2009; OAIC, 2015; Sargsyan, 2016; Gajanayake et al., 2011; Heath, 2013), consent is a basic need as students will be knowing what is expected of them.

In summary, the student consent component is important to this study, and:

- Students have the choice and right of consenting to opting-in for their personal information sharing (Chua et al., 2017; Jordaan & Van Heerden, 2016).
- If they no longer want to continue personal information sharing or receiving certain communications, the student can opt-out (Krishnan & Vorobyov, 2015; Swartz & Da Veiga, 2016).

3.6 CONSOLIDATED PRIVACY COMPONENTS FOR THE MODEL

The privacy components as derived from Table 2.3 are shown in Table 3.1 below and discussed in this chapter, and these are notice/openness to information usage, information quality, use limitation, purpose specification, collection limitation and also individual participation. The three additional components, namely privacy policy, privacy education and consent are also included.

The table headings show various components (principles) and where they can be derived from, be it from the FIPPs, OECD, GDPR or the Zimbabwe Data Protection bill. The headings also have the measurement perspective column, indicating whether the component is being assumed from the student or the university perspectives.

Table 3.1: Consolidated privacy components

COMPONENTS	FIPPs	OECD	GDPR	ZIM bill	MEASUREMENT PERSPECTIVE	
					Student	University
Notice/ Openness on information sharing (Homeland Security, 2008 on FIPPs; OECD Paragraph 15c; GDPR 103, 122, 132 & Article 57(b) & (d); ZDPA paragraph 13(1)(b)).	√	√	√	√	√	√
Information quality (Homeland Security, 2008 on FIPPs; OECD	√	√	√	√	√	√

Paragraph 8; Article 47 (2)(d); ZDPA paragraph 15).						
Purpose specification (Homeland Security, 2008 on FIPPs; OECD Paragraph 9; GDPR Paragraphs 45, 156 & 162; ZDPA paragraph 17, 21 & 22).	√	√	√	√	√	√
Use limitation (Homeland Security, 2008 on FIPPs; OECD Paragraph 10, Z ZDPA paragraph 32(2(a))).	√	√	√	√	√	√
Collection limitation (Homeland Security, 2008 on FIPPs; OECD Paragraph 7; GDPR Chapter III Article 15; ZDPA paragraph 32).	√	√	√	√	√	√
Individual participation/ choice (Homeland Security, 2008 on FIPPs; OECD Paragraph 13; GDPR Paragraph 18(1); ZDPA paragraph 30).	√	√	√	√	√	√
Security controls and safeguards (Homeland Security, 2008 on FIPPs; OECD Paragraph 11 & 17; GDPR Paragraphs 49, 83,94; ZDPA paragraph 24).	√	√	√	√	×	√
Accountability (Homeland Security, 2008 on FIPPs; OECD Paragraph 14 & 15(a); GDPR Paragraph 85; ZDPA paragraph 30).	√	√	√	√	×	√
Privacy policy (Homeland Security, 2008 on FIPPs)	×	√	√	×	√	√
Privacy education ((Homeland Security, 2008 on FIPPs; OECD	×	×	√	√	√	√

Part 19(g); GDPR Paragraphs 132)						
Consent ((Homeland Security, 2008 on FIPPs; OECD Paragraph 7 & 10; GDPR Articles 6, 7 & 8; ZDPA paragraph 18, 19, 20, 31(b)).	√	√	√	√	√	√

3.6.1 Inclusion criterion into the SPIPP conceptual model

A criterion was defined to identify which of the components in Table 3.1 above to include in the SPIPP conceptual model. As such, the following were considered:

- For adoption into the SPIPP conceptual model, a component must have 2 ticks (√) I measurement perspective, from both the student perspective and the university perspective.
- A component with one tick in the perspective column could not be included in the proposed SPIPP conceptual model.

As highlighted in section 2.7.1, security and accountability components are executable by the university. Students cannot do anything to put in place security systems or being accountable for their information processing by their university and the compliance with privacy regulations since these are a prerogative and a task of the university. From the above criterion, it can be concluded that security control and safeguards as well as accountability are excluded from the SPIPP model.

3.6.2 Measurement perspective

The **measurement perspective** column in Table 3.1 above indicates that the measurement is specified either from the student's perspective or the university perspective. It is imperative to note that both the university and student can be compelled by the above components. For instance, on one hand, the university must give notice to the student and be open on the information they collect (notice/openness); the university must ensure quality of the information they collect (quality of information); the university must specify the purpose for collecting personal

information (purpose specification); the university must limit information use only to the specified use (use limitation); the university must not ask for more/irrelevant information from the student (collection limitation); the university must give a student a choice to participate and share information (individual participation); the university must give guidelines on the privacy of information and its usage within the university (privacy policy); the university must increase student awareness through educating them (privacy education) and it must get consent through a tick box or signature from the student (consent).

On the other hand, the student can also be guided by the same components. To clarify, this column can guide how the students handle their personal information like expecting to read and understand a notice/ openness to increase their awareness before the collection of personal information (Cate, 2006; Chang et al., 2018; European Union, 2016a; Guffin, 2017; OECD, 2013b; Stange, 2011). The students prefer an open policy when they want to have access to their information and they will have confidence in the university if the university is showing transparency (Azemović, 2012; Dwyer & Marsh, 2016; Isabwe & Reichert, 2013; Katell et al., 2016; Katurura & Cilliers, 2016; OECD, 2013a). Although it must be availed and guaranteed by the university, information quality as perceived by the student is also a crucial component as students value information which is up-to-date, current, relevant, accurate and complete. In addition, students will expect some security measures for them to validate it as integral information and they must provide the university with accurate and up-to-date information (Banerjee, 2015a; Cate, 2006; European Union, 2016b; Guffin, 2017; OECD, 2013b).

There is also purpose specification which allows for the student to clearly note the purposes for collecting personal information and the student having confidence and trust with the university that it will not use it for any other purpose without the consent of the student (Chetty, 2013; Homeland Security, 2008; Katurura & Cilliers, 2016; OECD, 2013b). Under use limitation, the university might be required by the student to only use student personal information which is directly relevant for the accomplishment of the university authorised objective (European Union, 2016b; Guffin, 2017; OECD, 2013b). Information collection limitation is also another important component, as it assists the student to take note if the university is collecting their personal information lawfully, fairly and limited (and relevant) to the specified purposes

(Cate, 2006; Cavoukian, 2009; Ivanova et al., 2015; OECD, 2013a; Preuveneers et al., 2016a; Rasmussen & Dara, 2014).

For individual participation/choice, students must be aware and expect to be given the right to select whether to partake or not, whether they want to provide personal information or not and whether they want to have access to the personal information to amend, delete it or not (Iachello & Hong, 2007; Katurura & Cilliers, 2016; OECD, 2013a).

In conclusion, although the university has many duties and responsibilities that include preparing a notice for the students, being open on the information it collects from students (openness), collecting quality information and ensuring that information is validated, specifying the purpose for collecting personal information, making sure that it is not asking more information from the student than is needed and the university giving the student a choice like choice for sharing information or direct marketing, the student must be aware, must expect and consequently have confidence in the university for the same components (Alnatheer, Chan & Nelson, 2012). Therefore, the components are measured from both the student and university perspectives as the two entities are inseparable, that is, there is no university without the student and vice-versa. The privacy components are discussed in the following section.

The above nine privacy components are represented in Figure 3.3 below.

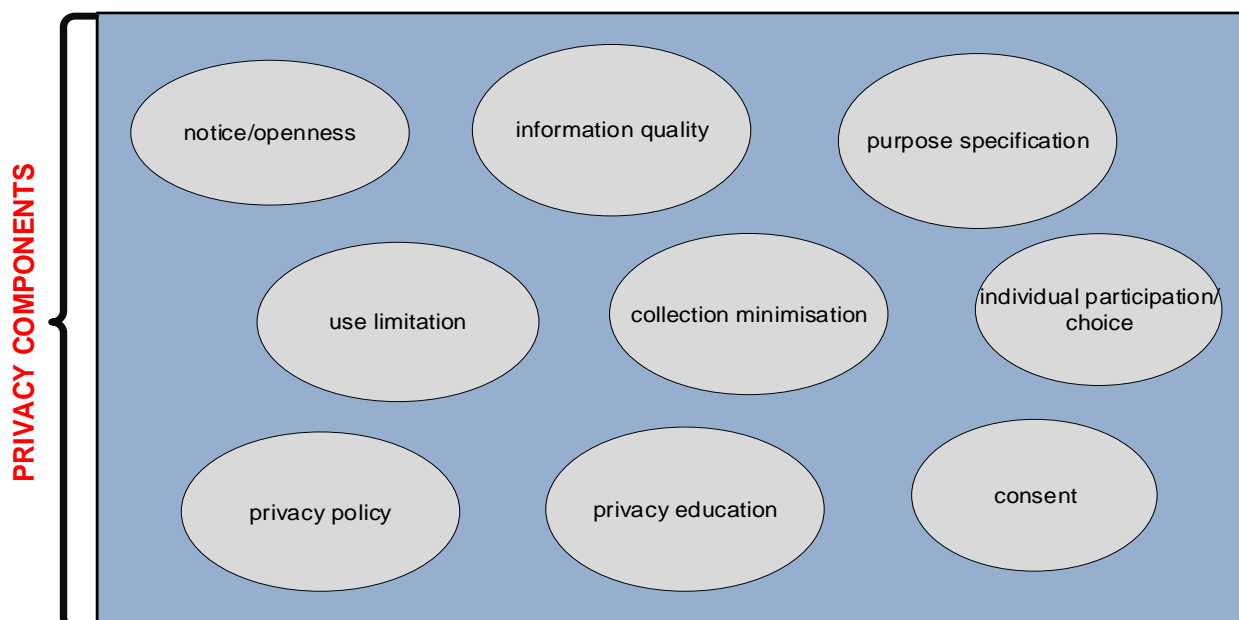


Figure 3.3: Privacy components of the SPIPP

The nine components (notice/openness to information usage, information quality, use limitation, purpose specification, collection limitation, individual participation/access, privacy education, privacy policy and student consent), combined with the three concepts (awareness, expectations and confidence), constitute the components of the SPIPP conceptual model that is applicable to Zimbabwean universities. This is discussed in the next section.

3.7 THE STUDENT PERSONAL INFORMATION PRIVACY PERCEPTION (SPIPP) MODEL

A conceptual model is an overview of concepts that give a comprehensive appreciation of a phenomenon (Jabareen, 2009). It can also be used in research to outline all probable alternatives of actions or representation of preferences in the approach to the school of thought or idea (Mehta, 2013). It consists of a set of theories that provide a firm basis for ones' thinking in regards to how one grasps and plans to research, carry out a title, definitions and concepts from the theories that are appropriate to the title (Grant & Osanloo, 2014). In summary, they act as maps in giving guidelines and direction by identifying the world view of a research topic based on concepts (Green, 2014).

The research focused on the important concepts and components that relate to the conceptual model as well as the relationships that exist between these concepts and components. The literature review provided the researcher with the basis for defining the concepts and components in this research, as well as envisaging the kind of relationships that exist amongst the concepts and components (Grant & Osanloo, 2014). To conceptualise all this, the researcher used the FIPPs privacy guidelines as the baseline, the OECD Protection of Privacy and Transborder Flows of Personal Data document, the recently promulgated GDPR privacy regulation as well as the ZDPA bill. Figure 3.4 below shows the conceptual model for privacy perceptions (the expectations, the awareness and the confidence) towards the university, with the assumed components.

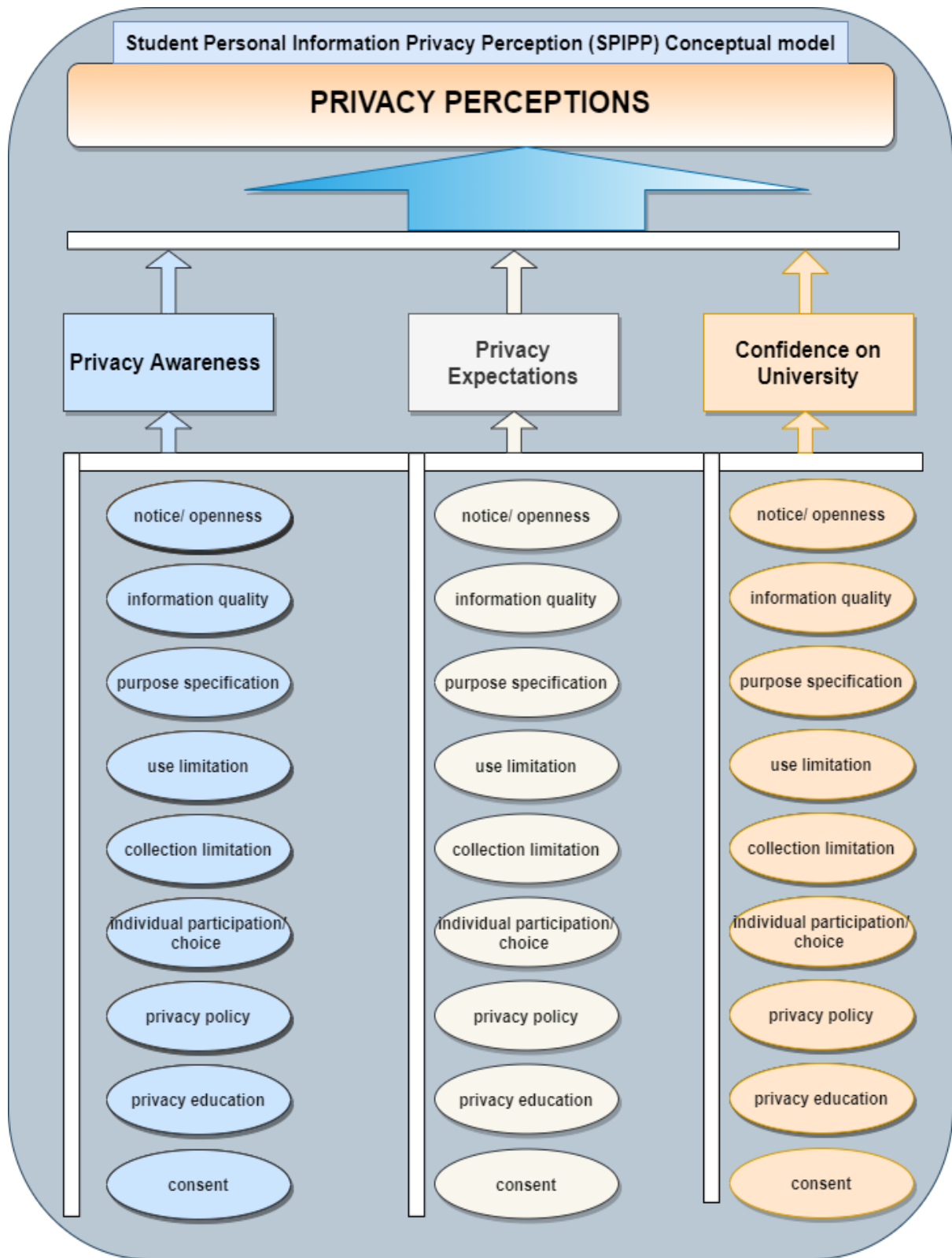


Figure 3.4: The SPIPP conceptual model for a university

In the SPIPP conceptual model above, there are two distinctive sections which are the section for privacy components and the section for privacy concepts. When combined, the two sections are perceived by the researcher to articulate the information privacy

perceptions within the university environment and which the university has to uphold for the privacy of student personal information to be a reality.

- i. **Privacy concepts:** the university should thrive to meet and fulfil these privacy concepts (awareness, expectations and confidence) so that the privacy of the student's personal information is properly articulated within a university environment. The privacy concepts are used for measuring the perceptions about the components. This implies that all the nine components must have a test for the awareness, the expectations and for the confidence.
- ii. **Privacy components:** in the model, nine privacy components will be adopted as highlighted in Figure 3.4 above. The scope of the model is grounded on the personal information from both the university and student perspective on privacy and these were derivatives from the FIPPs, the OECD Protection of Privacy and Transborder Flows of Personal Data document, the GDPR and the ZDPA bill. The components are notice/openness, purpose specification, information quality, use limitation, collection minimisation, individual participation, privacy education, privacy policy and consent. These are considered fundamental in this study since the university plays a very important role in adhering to them as they try to uphold the student's personal information privacy. Each of the nine components should be considered from the perspective of awareness, expectations and confidence. When combined, the components help in comprehending the information privacy perceptions in terms of the awareness, the expectations and the confidence in the university. Meeting student expectations through the social contract theory develops trust and hence confidence, which will result in positive privacy perceptions (Martin, 2015).

3.8 THE INFORMATION PRIVACY PERCEPTION INSTRUMENT

The nine components (notice/ openness, purpose specification, information quality, use limitation, collection limitation, individual participation, privacy education, privacy policy and consent) were all measured based on the three underlying concepts, namely the awareness, the expectations and the confidence. The statements

(questions) were based on theory as discussed in section 3.5. This resulted in the design of an information privacy perception instrument as indicated in Table 3.2 below.

Table 3.2: Summary of information privacy perceptions questions

CONCEPT	AWARENESS	EXPECTATIONS	CONFIDENCE
Notice/ openness			
	I am aware of the university's privacy notices.	I expect to be made aware of privacy through notices.	I have confidence that the university will ensure privacy through privacy notices
	I am aware that institutions can publish a notice for privacy.	I expect to publication of a notice for privacy by the university.	I have confidence that the university will publish notices for privacy
Information quality			
	I am aware that the university should ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection	I expect the university to ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection.	I am confident that the university will ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection.
	I am aware that the university should protect my personal information	I expect the university to protect my personal information.	I am confident that the university will protect my personal information.
Purpose specification			
	I am aware that the university should specify the purpose when collecting my personal information at the point of collection.	I expect the university to specify the purpose when collecting my personal information at the point of collection.	I am confident that the university will specify the purpose when collecting my personal information at the point of collection.
	I am aware that the university should inform me about the purpose of collecting my personal	I expect the university to inform me about the purpose of collecting my personal	I am confident that the university will inform me about the purpose for collecting my personal

	information at the point of collection.	information at the point of collection.	information at the point of collection.
Use limitation			
	I am aware that my personal information should not be disclosed, made available or used except if it is by the authority of the law.	I expect my personal information not to be disclosed, made available or used without my consent by the university.	I am confident that my personal information will not be disclosed, made available or used without my consent by the university.
	I expect my personal information not to be disclosed, made available or used without my consent by the university.	I expect my personal information not to be disclosed, made available or used except if it is by the authority of the law.	I am confident that my personal information will not be disclosed, made available or used except if it is by the authority of the law.
Collection limitation			
	I am aware that the university must collect information fairly, lawfully and for the purposes specified fairly.	I expect the university to collect information fairly, lawfully and for the purposes specified fairly.	I am confident that the university will collect information fairly, lawfully and for the purposes specified fairly.
	I am aware that the university should limit collection of personal information (like religion, political party affiliation, tribe etc.) which is not essential for academic purposes.	I expect a limit to the collection of personal information by the university (like religion, political party affiliation, tribe etc.) which is not essential for academic purposes.	I am confident that the university will limit the collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.
Individual participation			
	I am aware that I can request from the university a confirmation of what personal data the university has collected about myself.	I expect to be able to request from the university a confirmation on what personal data the university has collected about myself.	I am confident I can request from the university a confirmation on what personal data the university has collected about myself.
	I am aware that the university should have a process when requesting	I expect the university to have a process when requesting personal	I am confident that the university follows a process when requesting personal

	personal information about myself.	information about myself.	information about myself.
Privacy policy			
	I am aware that the university should have a privacy policy.	I expect the university to have a privacy policy.	I am confident that the university has a privacy policy.
	I am aware that the privacy policy should be easily understandable.	I expect the privacy policy to be easily understandable.	I am confident that the privacy policy is easily understandable.
Privacy education			
	I am aware that the university should have existing privacy education for students (e.g. on the safe keeping of students' financial details, on the protection of their personal devices, on impersonation issues when on social media platforms, about monitoring of unauthorised access to their emails, on their examination results etc.).	I expect the university to have existing privacy education for students (for example on the safe keeping of their laptops, on the protection of their personal information, when online using social media platforms, on their examination results etc.).	I am confident that the university has existing privacy education for students (for example on the safe keeping of their laptops, on the protection of their personal information, when online using social media platforms, on their examination results etc.).
	I am aware that the university should remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).	I expect the university to remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).	I am confident that the university will remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).
Consent			
	I am aware that I have the right to opt in on the use of my personal information for	I expect to have the right to opt in for the use of my personal information for	I am confident that the university gives me the right to opt in for the use of my personal

	other purposes (like marketing, newsletters, job or product advertisements etc.).	other purposes (like marketing, newsletters, job or product advertisements etc.).	information for other purposes (like marketing, newsletters, job or product advertisements etc.)
	I am aware that I have the right to opt out on the use of my personal information for other purposes if I am no longer interested	I expect to have the right to opt out on the use of my personal information for other purposes if I am no longer interested	I am confident that the university gives me the right to opt out for the use of my personal information for other purposes if I am no longer interested

The information privacy perceptions instrument in Table 3.2 was used in the design of the Information Privacy Perception Survey (IPPS), as shown in appendix E1.

3.9 CHAPTER SUMMARY

The chapter discussed the information perceptions on the three main concepts, namely awareness of privacy, expectations on the privacy of their personal information and confidence in the university to meet privacy expectations and comply with privacy regulatory requirements. Privacy within a university was discussed based on the three concepts, namely student privacy awareness, student privacy expectations and student privacy confidence in the university. The social contract theory was discussed in relation to privacy and its relevance to this study was highlighted. The privacy components that constitute that constitute the SPIPP conceptual model were discussed. A consolidated overview of the additional three components was done and the inclusion criteria for their adoption in the conceptual model was well articulated in summary at the end of each component. This led to the designing of the SPIPP conceptual model and a brief description of the components and the concepts. A summary of the information privacy perceptions instrument, based on theory, was also done. This chapter attempted to fulfil the theoretical aims as articulated in section 1.5.2.

The next chapter, Research Methodology, discusses the research methodology followed in this study. It also highlights the design of the instrument used.

CHAPTER FOUR: RESEARCH METHODOLOGY

4.1 INTRODUCTION

This chapter addresses the empirical objective number 1, namely *to develop a privacy perception instrument measuring privacy awareness, expectations and confidence of students*. The chapter discusses the research methodology. The chapter starts off with a dialogue of the research philosophy, and it moves onto the research approach, research design, research strategy and the time horizon adopted in this research. The population as well as the sampling techniques adopted are also presented in this chapter. The instrument design procedures and instrument purification are also done in this section. The data collection methods are specified and various data statistical analytical methods that include the descriptive, inferential and structural equation modelling are presented. The research hypotheses are also discussed in this section. The conclusion of this chapter focuses on the ethical considerations made in the execution of the research.

4.2 CHAPTER OVERVIEW

The chapter is segmented into ten main parts. These are:

- First Part: Section 4.3 – Defines the research methodology concept.
- Second Part: Section 4.4 – Discusses the research philosophy with its rationale.
- Third Part: Section 4.5 – Discusses the approach adopted and the rationale of the approach.
- Fourth Part Section 4.6 – Discusses the research design research design rationale.
- Fifth Part Section 4.7 – Discusses the research strategy and research strategy rationale.
- Sixth Part: Section 4.8 - Discusses the time horizon and rationale.
- Seventh Part: Section 4.9 – Discusses the population and sampling issues.
- Eighth part: Section 4.10 – Analysis of the data collection criteria, design of the instrument, expert and pilot analysis, reliability and validity.

- Ninth part: Section 4.11 – Discusses the management of data, descriptive and inferential statistics in exploratory and confirmatory factor analysis.
- Tenth part: Section 4.12 – Formulation of the research hypothesis.
- Eleventh part: Section 4.13 Analysis of the research ethical considerations.
- Twelfth Part: Section 4.14 – Summary of chapter three.

A summarised view of the chapter, is shown in Figure 4. below.

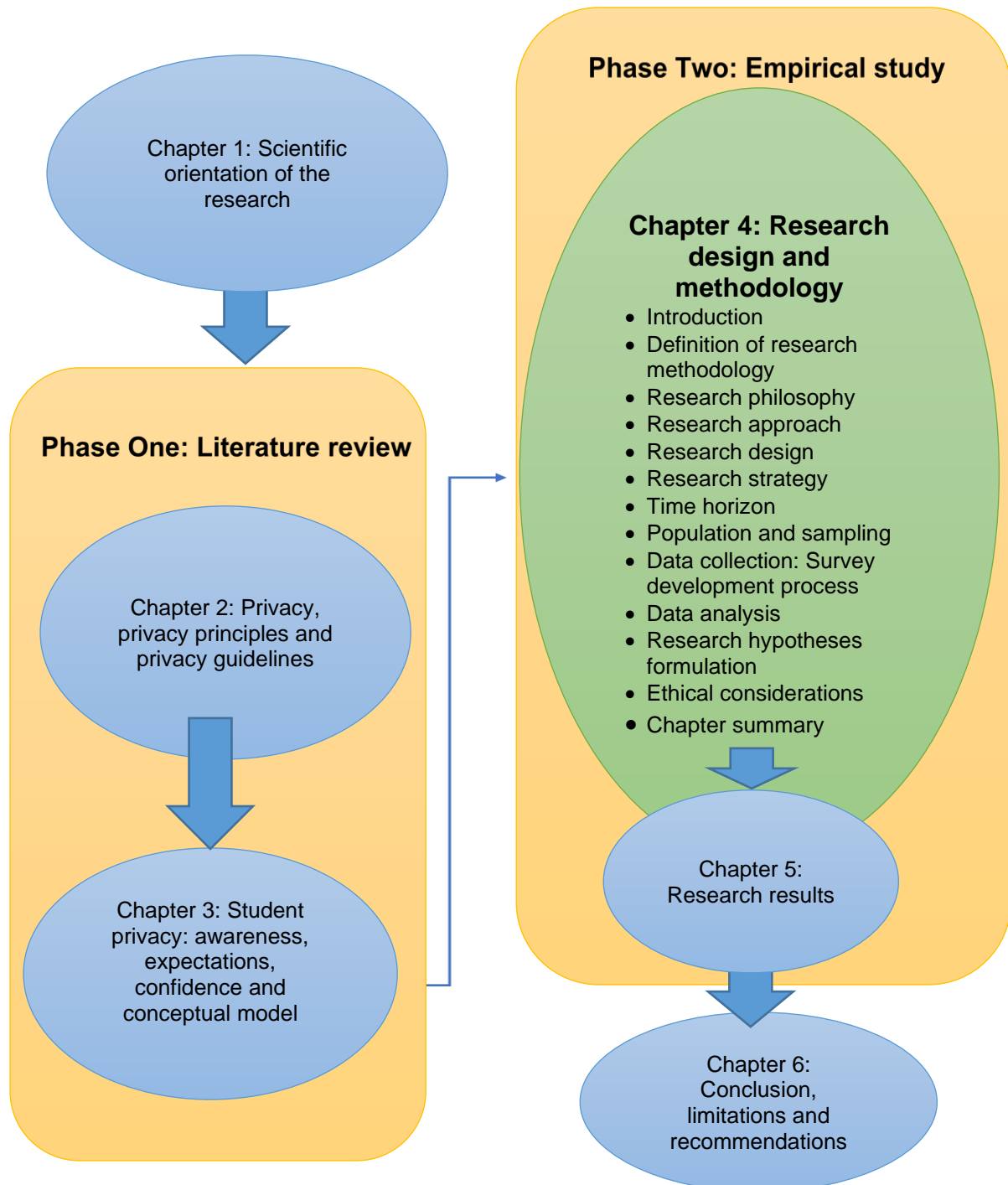


Figure 4.1: Chapter summary flowchart diagram (Source: Author's own compilation)

4.3 DEFINITION OF RESEARCH METHODOLOGY

A research methodology is defined as a scientific way that is used to elucidate a research problem in a systematic way and it involves the research methods as well as the reasons for the chosen study methods (Kothari, 2012). According to Kothari (2012), a research methodology involves the process of collecting data with the aim of making decisions and it consists of a sequence of steps or actions that are essential in carrying out research and the expected sequencing of these stages. Additionally, Saunders, Lewis and Thornhill (2016) opined that a research methodology is a theory of how one undertakes a research. In summary, the research methodology looks at all the processes involved when one is executing research. Research must be undertaken to give responses to questions and it must be undertaken within a model of set philosophies and it uses certain procedures, methods and techniques that will be evaluated for reliability and validity (Kumar, 2011).

The research onion was used to ground this research (Saunders et al., 2016) (See Figure 4.2 below.) The research onion model is used in this research in discussing the research execution in subsequent paragraphs, dealing with the research philosophy, the research approach, the research design, the research strategy, the time horizon and the processes of data collection and analysis.

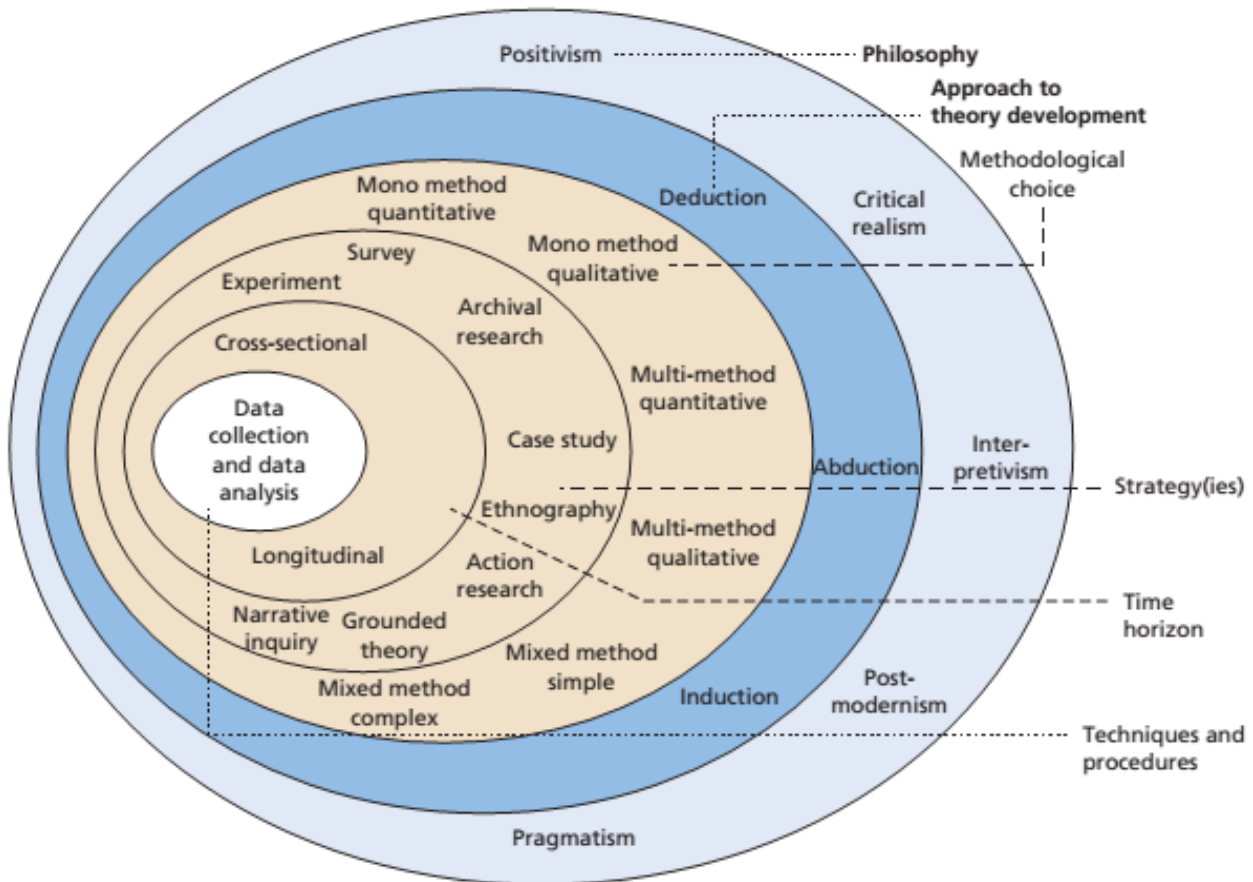


Figure 4.2: The research onion (Saunders et al., 2016)

As shown in the model above, the discussion is done based on various research aspects. The following section discusses the research philosophy.

4.4 RESEARCH PHILOSOPHY

Research philosophy relates to the advancement of knowledge and the description of the knowledge (Saunders et al., 2016). These are the presumptions reflecting on a particular posture that researchers select when they decided to carry out the research (Walliman, 2014). From Figure 4.2 above, it is indicated that the philosophy adopted in this research is positivism. Positivism focuses on empirical data collection, cause and effect-oriented analysis (Neuman, 2014). The social world can be explained in relation to interrelated important philosophical conventions that the diverse paradigms are underpinned on and these are the ontology (nature of reality or what we believe), the epistemology (the art of knowing) and the methodology (the art of discovering the knowledge) (Creswell, 2014; Davidson, 2004; Greener, 2008). Ontology correlates with whether we believe there is one confirmable claim or whether many socially

constructed realities are existence (Chilisa, 2012). Oats (2012) explains that epistemology tries to inquire about the truth and the nature of knowledge. In addition, the methodology looks at various ways and techniques that can be used to find out about the existence of knowledge (Chilisa, 2012; Kivunja & Kuyini, 2017). Using these assumptions, Saunders et al. (2016) assert that research philosophy can be categorised as positivism, interpretivism, pragmatism, post-modernism and critical realism among other philosophies as shown in Figure 4.2 above.

Positivism states that the phenomena which we know through our natural senses like smell, hear, see, taste or touch produce knowledge (Greener, 2008; Riley-Tillman & Reinke, 2011). According to Greener (2008), this helps in carrying out an experiment to approve or even disapprove a hypothesis and the generation of new theory through organising facts together to generate principles, describe them and conclude with the one to be adopted and give the reasons why. Greener (2008) indicates that positivism is typically linked to natural science studies and comprises of empirical testing. The reason is that the ontology of positivism tend to use experimentation and testing to produce knowledge and either approves or disapproves hypotheses (Greener, 2008; Riley-Tillman & Reinke, 2011). Positivism is founded on the notion that science is the solitary premise for true and real knowledge and it therefore assumes that the methods, procedures and techniques that natural sciences uses offer the supreme model for studying the social world (Neuman, 2014; Tracy, 2013). Saunders et al. (2016) posit that in the positivism philosophy, the researcher collects data on particularly any observable truth and then pursue for some regularities and any unpremeditated relationships in the data to produce new principal generalisations. The ontological position of the positivist is realist; its epistemology is said to be objective, and its methodology is said to be empirical, which reveals the position that things like social objects exist as meaningful reality that is external to the social actors that have concern over their existence (Cohen et al., 2011; Kivunja & Kuyini, 2017; Tracy, 2013).

A survey-based approach, which is the research method assumed in this research, is used for primary data collection and it relates to positivism. This means that it becomes logical and easier to adopt this philosophy for this study (Cohen et al., 2011). As argued by Riley-Tillman and Reinke (2011) and Kivunja and Kuyini (2017), many scientific models are viewed by positivists as providing theories, and it will then be

submitted to practical testing, implying that science uses a deductive approach in a bid to extract specific arguments from general accounts of reality.

4.5 RESEARCH APPROACHES

A research can either be deductive, inductive or abductive in terms of its approach (Saunders et al., 2016) as shown in Figure 4.2 above. A deductive approach normally begins by observing the concept or theory, produce a hypothesis from that concept, which must relate to the research focus, and then advance to test that concept (Greener, 2008; Saunders et al., 2016). The focus is to test the theory. In contrast, an inductive approach begins by looking at the research focus and aims to generate theory from the research through exploration by various research methods (Greener, 2008; Saunders et al., 2016). Conversely, the focus is on the generation of the themes. One uses a deductive approach if there is need to adopt a clear theoretical position that will be tested normally through data collection, implying that the research would be theory driven as shown in Figure 4.2 (Oats, 2012; Saunders et al., 2016). In contrast, an inductive approach is a data motivated approach where there is the exploration of the topic and the development of the theoretical explanation (Saunders et al., 2016). The other approach is abduction and it is a technique used to move back and forth between data and theory by combining both induction and deduction approaches.

This study used the *deductive approach* as shown in Figure 4.2 above. The choice of this approach was for the following reasons:

- A deductive approach seeks to extract explicit theories from general accounts of reality (Riley-Tillman & Reinke, 2011). This is the case for this study.
- The deductive approach compliments the positivism paradigm adopted in this research. A positivism paradigm depend on deductive logic, articulation of hypotheses, hypotheses testing, offering mathematical equations and functioning definitions, calculations, predictions and expressions, in a bid to derive conclusions (Kivunja & Kuyini, 2017; Saunders et al., 2016).
- As previously alluded to by Creswell (2014), the deductive approach aims to offer clarifications and to give forecasts grounded on quantifiable outcomes, which is in line with this study.

- According to Chilisa (2012), since the deductive approach is used in the positivism paradigm, it will be objective in the collection of data and, consequentially, it tends to alleviate potential errors and bias, especially on the instruments.

4.6 RESEARCH DESIGN

Research design is regarded as monumental plan in approaching research on a particular research topic (Greener, 2008). According to Creswell (2014), it is a procedure and plan for research that stretches the decisions from broad theory to detailed methods used for collecting and analysing data. The research design (also termed the methodological choice) is the general schedule of how one will go about replying the research questions (Saunders et al., 2016). This is why Cohen et al. (2011) synonymises the research design with the architectural plan when one is constructing a house. The research design will have very clear objectives that are derived from the study questions, with the data collection sources clearly specified, propose how the collection and analysis of data, discuss ethical matters and the constraints most likely to be encountered (Neuman, 2014; Saunders et al., 2016).

Research design can either be qualitative, quantitative or mixed (Creswell & Creswell, 2018; Neuman, 2014). A qualitative research is associated with the inductive approach in the generation of theory, and adopts an interpretivism model that allows for the existence of many subjective perspectives and the creation of knowledge as opposed to the objective model in search of “finding” it in its “reality” (Greener, 2008; Kumar, 2011; Walliman, 2014). According to Guerin and Dohr (2005), qualitative research is mostly used in the exploration of an issue, trying to gain an improved understanding of it, instead of testing or supporting a relationship. Kothari (2012) posits that qualitative research is focused on qualitative phenomena that involve quality or kind and uses research instruments such as interviews, observations and ethnography. Qualitative research is most suitable for behavioural sciences where the purpose is to realise the fundamental human behaviour motives (Greenfield & Greener, 2016; Kothari, 2012). Most qualitative studies use open-ended enquiries to allow the respondents to express their opinions subjectively (Creswell, 2014). Muller (2014) insists that a qualitative design is most appropriate when the purpose of the research

is to gather knowledge of an idea that is unfamiliar and is seeking an understanding using inductive reasoning.

A quantitative research approach is linked to the deductive approach, especially to test theory, often using numbers and consequently, a positivism paradigm and an objectivist perspective of the objects studied (Greener, 2008; Kothari, 2012; Saunders et al., 2016). Quantitative research is one that is founded in measuring the amount (quantity) and is applicable to any phenomenon that can be easily expressed in terms of quantity (Kothari, 2012; Walliman, 2014). It is a systematic empirical investigation of numeric properties and phenomena as well as their relationships (Gerber & Hall, 2017; Greenfield & Greener, 2016). A quantitative approach seems suitable when the study objective is to test the cause-effect and/ or predictive type of hypotheses and it aligns with the deductive logic; the design is appropriate for a phenomenon that has been properly established with regards to theory and concepts (Muller, 2014). Therefore, in a quantitative approach, data must be collected and it uses numerical data (Muller, 2014; Neuman, 2014). Quantitative data can be visually epitomised and analysed using statistical tables and graphs (Curran, 2010).

In the most practical terms, researchers tend to fuse both methods i.e., qualitative and quantitative, in the mixed method design (Greener, 2008; Kothari, 2012; Kumar, 2011; Saunders et al., 2016). A mixed method design seems to strengthen research in that it harnesses the advantages of both research designs and reduces their weaknesses, with the ultimate result being that the two methods will complement each other (Riley-Tillman & Reinke, 2011). According to Riley-Tillman and Reinke (2011), a mixed method design has advantages such as provision of more inclusive evidence for executing a study problem, as compared to either the qualitative or the quantitative. They add that it is more practical in allowing the researcher to be flexible in terms of using the relevant methods, skills and cognition in addressing research problems and more so, a mixed method design permits the answering of questions which could have been so difficult to answer otherwise.

This study adopted the *quantitative research design* as revealed in Figure 4.2 above. The rationale in choosing the quantitative research design for this research was that:

- The research used a survey research strategy and instruments were distributed, resulting in numerical data. Numerical data can only be analysed and validated quantitatively (Greener, 2008; Oats, 2012; Riley-Tillman & Reinke, 2011; Saunders et al., 2016).
- The research aims to measure student awareness, student expectations and student confidence in a university environment. These again, are quantitative parameters hence the adoption of quantitative research design.
- The results are modelled statistically using descriptive statistics, inferential statistics, factor analysis and item analysis, all which are quantitative units of measurement.

4.7 RESEARCH STRATEGY

Greener (2008) suggests that a research strategy can also be regarded as a research method, though it is a debatable subject. Saunders et al. (2016) is of the view that a research strategy is a roadmap or plan of action to achieve an objective. It is a strategy of how the research questions will be answered by the researcher (Cohen et al., 2011). Simplifying, it is a procedural link of the research philosophy to the choice of methods for collecting and analysing data (Neuman, 2014; Saunders et al., 2016). There are numerous research strategies and these include case study, experiment, survey, action research, ethnography, grounded theory and archival research as shown in Figure 4.2 before. Because of its nature and link to the various segments of research like the philosophy, approach and design used, this research adopted the survey research strategy.

A survey is a scientific method for studying people's behaviour that would be difficult to experiment or observe directly (Davidson, 2004; Guerin and Dohr, 2005). The objective of a survey is to provide mathematically gathered information to work as a foundation for the researchers for their outcomes (Greener, 2008). It is also used to provide numerical descriptions of attitude, trends or opinion of a population and it normally uses the population sample to study the population (Creswell, 20014; Walliman, 2014). A survey is used to answer the who, what, where, how much and how many types of questions (Saunders et al., 2016). From the sample results, the researcher analyses and makes some claims about pertaining to the population (Creswell, 2014; Neuman, 2014). One good characteristic of the surveys is that it

allows for the use of instruments from a large population and this is economical, easy to explain and understand and comparisons can easily be done (Saunders et al., 2016). Gerber and Hall (2017) also endorse the survey as a research method that uses instruments to gather more information about people and what they think as well as their behaviour. According to Mathers, Fox and Hunn (2009), Neuman (2014) and Oats (2012), surveys have advantages such as having both internal and external validity and they are efficient and flexible and the samples cover a geographically spaced sample.

According to Mathers et al. (2009), some of the advantages of using a survey in data collection are:

- They have both internal and external validity, especially those based on random sampling that produces a sample resembling a certain population.
- They are efficient.
- They cover samples and participants who are geographically spread.
- On ethical considerations, surveys tend to give a slight advantage because they don't expose participants or influence responses in any way.
- Their flexibility makes them one of the best techniques of data collection because they can be combined with any other technique.

Surveys also have limitations. One of these limitations is the need for large numbers so that they give results with accurate meaning (Guerin & Dohr, 2005). This was mitigated in this research by using a sample size with 270 students. One of the major issues with an online survey is that there is a very low response rate (Jackson, 2009). There were follow-up emails and reminders that were sent on a weekly basis, after the lapse of the initial two weeks, to increase the response rate. This research used online surveys and according to Saunders et al. (2016), such surveys are effective and efficient when all the respondents are IT literate and with internet access. This is the case with the students in this study. Another issue is ascertaining whether one participant will only send one response. In this survey, there was an instruction on the last page to inform respondents to only submit one response. The researcher also used cookies to prevent multiple submissions. Cookies can be handy because if a participant tries to submit again, a message will display that the survey has already been answered. The assumption was that participants would not temper with the

settings to switch the cookies off in their browsers. Due to the massive national electricity load shedding that has been affecting Zimbabwe for the past couple of years, the researcher also used the paper-based survey method whereby the instrument was printed, a presentation made highlighting the reasons for printing hard copies as well as guaranteeing anonymity and confidentiality of their responses. He had to seek consent before giving the hard copies to students. Most students completed the hard copy instruments due to the electricity challenges experienced at the time.

Reasonable actions were taken to clean the data according to student responses. If a question is unclear to the respondent, respondents tend to leave it blank (Jackson, 2009) and this impacts on data analysis. Data cleaning was done on rows of data where the same response was selected right through by the respondent, or where only a few questions were answered and the rest left blank. In addition, in this study, data was scrutinised for obvious duplicate rows. Such rows were deleted and this was recorded in the data cleaning section.

As indicated in Figure 4.2, the *survey* method was considered suitable for this study. This was because:

- The empirical survey aids the researcher to acquire data on the various concepts like the awareness of students on the privacy of their personal information, student expectations on privacy and student confidence levels in the university being able to uphold the personal information privacy.
- Most quantitative research implements the survey design – this also corroborates with Saunders et al. (2016) and Neuman (2014).
- A survey also tends to give a rapid turnaround in data collection (Creswell, 2014), which will boost the reliability of the study since many responses show more information.
- The tool of measurement which is always required for the evaluation of a phenomenon under investigation is the instrument (Chilisa, 2012; Davidson, 2004; Muller, 2014; Tracey et al., 2017).
- The information collected is reliable and objective especially if the instrument is properly designed as one can validate the model statistically using the collected empirical data (Davidson, 2004).

4.8 TIME HORIZON

A survey can either be longitudinal or cross-sectional (Creswell, 2014; Saunders et al., 2016). Longitudinal survey permits for the gathering of data and creates a moving picture about people, events or even social relations over time to have two data sets and then compare (Creswell, 2014; Neuman, 2014; Saunders et al., 2016). Cross-sectional survey, in contrast, allows for the collection of data at one point in time and creates a snapshot about social life (Creswell, 20014; Neuman, 2014). This research followed a *cross-sectional survey* since the survey was sent out at a specific time interval. To allow students sufficient time to respond, a 3 (three) week period was allowed and was extended by 2 (two) more weeks due to the current prevailing electricity and therefore internet challenges. This was considered enough time for students to go through the instrument and give responses accordingly.

4.9 POPULATION AND SAMPLING

A study can use either primary or secondary data (Greener, 2008; Jain, Dubey & Jain, 2016; Kumar, 2011). Primary data is any data which is collected for the first time whereas secondary data is data which exists and has already been collected and analysed by someone (Salkind, 2017). In this research, a sample design was used to collect primary data.

4.9.1 Sample design

Kothari (2012) defines sampling as the process of gathering information about the entire population through analysis of only a segment of it. Greener (2008) describes sampling as an experimental way of analysing a section (sample) that represents the people with their thoughts, activities, relationships, abilities and attitudes among other characteristics. It is a procedure for choosing the number of research units from a well-defined study population (Jain et al., 2016; Walliman, 2014). Identifying how the sample should be chosen is the ultimate objective (Kumar, 2011). Another objective of sampling, as indicated by Gerber and Hall (2017), is to statistically infer information from the population under study so as to gain more information about that population. The designing of a sample requires some decisions to be made, such as identifying the population and sample, the sample size and technique for selecting the sampling.

4.9.2 The sample and population

A sample is a “subset of the people, objects, or events selected from that population” (Lehman, O’Rourke, Hatcher & Stepanski, 2005 p.16). The big issue in research is ascertaining who will be surveyed; therefore, the subset of the population is in most cases selected to represent the whole population (Kumar, 2011). The sample gives a snippet of a population, without necessarily having to study the whole population (Molenberghs, 2010). The population is mostly very large such that it is difficult and not ideal to measure the whole population but rather to focus on the variables of interest from the selected sample (Lehman et al., 2005; Curran, 2010).

Students from the university under study were selected as participants to constitute the sample from a population of all universities in Zimbabwe. Students were included if they were registered at the university. It was not practical to do the research in all universities in Zimbabwe in terms of time, economics and convenience. The research was conducted in one university in Zimbabwe.

4.9.3 The sample size

The sample size focuses on ascertaining how many people will be surveyed (Gerber & Hall, 2017; Kumar, 2011). It is imperative to realise that the larger the sample, the better and reliable the results are (Gerber & Hall, 2017; Jackson, 2009). The required sample size to meet the minimum responses required to validate the instrument statistically can be derived from the number of questions in the instrument and making use of the rule of the thumb highlighted by Gerber and Hall (2017). The researcher multiplied the 5-point scale (discussed in Section 4.10) with the number of items in the instrument and this gave the minimum responses anticipated from the respondents (students). This allowed for the conduct of factor and item analysis and ensuring reliability of the constructs in the instrument.

Using the formula $5(n)$ where n signifies the number of items in the instrument (Gerber & Hall, 2017), it can be computed to 5×54 statements that are in the instrument to get 270. This formula holds if all respondents are to complete all the questions in the instrument. In other words, 270 is the minimum number of students expected for this study, which is the sample size. The instrument (discussed in Section 4.10) was sent

out to a larger sample of +/-350 in order to obtain the minimum number of responses (at least 270 in this case). The researcher recruited the respondents by making a presentation to the participants (students) that highlighted the objective for conducting the research and looking for their participation. Partaking in the study was clearly labelled voluntary and the researcher guaranteed anonymity and confidentiality of the respondents. The recruitment of participants was done using a sampling technique described below.

4.9.4 Sampling technique

The researcher must select the members to institute the sample and ascertain if probability sampling or non-probability sampling will be used (Neuman, 2014; Riley-Tillman & Reinke, 2011; Saunders et al., 2016; Visser, Krosnick & Lavrakas, 2013). In probability sampling, affiliates of the entire population have equivalent prospects of being selected to formulate the sample (Jackson, 2009; Saunders et al., 2016; Visser et al., 2013). In contrast, a non-probability sampling is a technique that has an unknown probability for choosing the respondents (Gerber & Hall, 2017; Jackson, 2009; Saunders et al., 2016; Visser et al., 2013).

Neuman (2014) posits that probability sampling technique is mostly deployed for quantitative research whilst a non-probability technique is mostly used in qualitative research. The most commonly used probability sampling techniques in quantitative research are simple random sampling, stratified sampling, systematic sampling and cluster sampling (Gerber & Hall, 2017; Neuman, 2014; Saunders et al., 2016; Visser et al., 2013). On the contrary, the non-random sampling techniques commonly used in both quantitative and qualitative research methods are quota sampling, purposive sampling, snowball sampling and convenience sampling (Gerber & Hall, 2017; Greenfield & Greener, 2016; Neuman, 2014; Saunders et al., 2016; Visser et al., 2013). A good sampling technique must maximise its degree of representation of the actual population (Salkind, 2017).

For the conduct of the survey in this research, a non-probability sampling procedure was selected, under which the convenience sampling method was considered the most appropriate one (Cohen et al., 2011; Salkind, 2017; Saunders et al., 2016; Tracy, 2013). Convenience sampling, as propounded by Creswell and Creswell (2018) and

Saunders et al. (2016), allows for the selection of cases in a haphazard manner because of their ease of availability and convenience to acquire the sample. It is a way of studying and choosing what is immediately available and continuing until the expected sample size has been acquired (Cohen et al., 2011; Walliman, 2014). According to Cohen et al. (2007), the convenience sampling method is mostly used when students are often perceived to be respondents, which is a case in this research. It is convenient, saves time and is less costly, saving effort of the researcher in trying to find less amenable respondents (Salkind, 2017). Unfortunately, convenience sampling suffers from being prone to bias and influences that are beyond the researcher's control and sometimes the research findings are given less credibility because they might not represent the generality of the population (Cohen et al., 2011; Salkind, 2017; Saunders et al., 2016).

The sample chosen in this research (a private university in Zimbabwe) represents the typical scenario under study, namely Zimbabwean students' perceptions on privacy in terms of their expectations, their awareness levels and their confidence in the university's upholding of privacy when they process student personal information. This increases its credibility. In sampling, bias is defined as the systematic error on the procedures for sampling that result in the distortion of the study results (Elder, 2009; Jackson, 2009). The fact that partaking in the study was voluntary, with no reward of any sort and anonymity being advocated for, tend to reduce bias (Hallam & Zanella, 2017). The stages of data collection can be explained in stages, which are editing, data coding and the creation of an electronic file (Gilliland, 2014).

Students were invited to participate based on their availability. The participants were recruited by the researcher by making a presentation to all students, stressing the purpose of conducting the study and looking for their participation. As indicated earlier, partaking in the study was voluntary and the researcher gave guarantees on anonymity and confidentiality of the respondents.

The researcher selected purposive sampling to choose the experts to partake in this research. As a non-probability technique, purposive sampling is a method that bases the selection of units on the researcher's supreme personal judgment (Greener, 2008; Kothari, 2012; Neuman, 2014). The researcher uses his subjective judgment to select a sample that they believe represents the population, people that are knowledgeable

(in-depth knowledge) by virtue of their profession and a sample that allows him to meet his objectives (Cohen et al., 2011; Greenfield & Greener, 2016; Neuman, 2014; Saunders et al., 2016). In the next section, a description of the survey development process is done.

4.10 DATA COLLECTION: SURVEY DEVELOPMENT PROCESS

After ascertaining the sample, sample size, the next stage was to determine how the data would be collected. Data can be collected in many ways and these include observations, instruments, interviews (personal and telephone), emailing, experiments, documents and schedules among several other ways (Chilisa & Kawulich, 2012; Kothari, 2012; Visser et al., 2013). In this study, information was collected using a quantitative survey called the Information Privacy Perception Survey (IPPS) that the researcher developed. Primary data was collected. The instrument used was discussed in Section 4.6 above. The following sections describe the development of the IPPS instrument used in this research.

4.10.1 Data collection instrument

Any means of gathering data from a study is called a research instrument or research tool (Kumar, 2011). In quantitative research, especially when surveys are used, the questionnaire can be an option used as the research instrument and it exists in both closed ended and open ended formats (Greenfield & Greener, 2016; Guerin & Dohr, 2005; Kazi & Khalid, 2012; Kumar, 2011; Muller, 2014). A instrument is defined as a series of questions written down on a specific topic where the researchers sought the subjects' opinion (Creswell & Creswell, 2018; Guerin & Dohr, 2005; Kumar, 2011). In addition, Riley-Tillman and Reinke (2011) defines an instrument (questionnaire) as a means of collecting data in survey study that encompasses some documented questions that people will respond to promptly on the instrument form itself. Instruments help in gathering more information about people's opinions and perceptions about a particular situation (Neuman, 2014). In this survey, instruments were used for the data collection process.

The answers in an instrument are recorded by the respondents themselves (Creswell & Creswell, 2018). It is very important to prioritise the form and wording of questions

in an instrument as it will impact the quality and type of data derived from the respondents (Creswell & Creswell, 2018). An instrument can be self-administered, when students answer the instrument they have received, or can be an interviewer-administered instrument, which occurs when students are asked questions by the interviewer and students openly respond to the questions (Greenfield & Greener, 2016; Guerin & Dohr, 2005; Kazi & Khalid, 2012). This study used a self-administered instrument, allowing students to respond at their own accord.

Self-administration of instruments is when the tool is distributed as hard copies and through email. As advantages, Kazi and Khalid (2012) suggest that self-administered questions have the ability to reach a wider audience covering a huge sample size, covering a wider geographical spectrum, be able to cover issues/topics which are sensitive and reach out to some most difficult geographical areas. They also increase anonymity (Neuman, 2014). The major drawback of self-administered instruments is the issue of low response rates (Kumar, 2011) and lack of clarity on some issues in the instrument. To improve the response rate in the study, the researcher adopted Kazi and Khalid's (2012) techniques by sending follow-up emails and making sure that the questions were brief. The researcher also printed copies and distributed them to students. To increase clarity, the instrument was provided in the best simplified form, which was taken through pilot and expert analysis. The design of the instrument for this research is described below.

4.10.2 Instrument design and construction

When designing an instrument, questions are designed either as open-ended or closed-ended questions (Jain et al., 2016; Kazi & Khalid, 2012; Kothari, 2012). Possible responses to a scenario are not given in open-ended questions and if an instrument is being used, the participant will have to put the responses in their own words (Kumar, 2011). Open-ended questions are used when it is difficult to grasp all possible answers to the questions and its advantages include the fact that researchers will not be able to suggest answers; it allows students to respond using their own words though the responses can be broad (Guerin & Dohr, 2005; Kazi & Khalid, 2012; Saunders et al., 2016). Analysis of open-ended questions is difficult and some respondents might fail to express themselves, leading to loss of information (Kumar, 2011).

The study used closed-ended questions, which are called forced questions because they give the respondent alternatives to choose from, according to the instructions (Greenfield & Greener, 2016; Guerin & Dohr, 2005; Kazi & Khalid, 2012; Muller, 2014). The negative issues on closed-ended questions must be on their lack of depth, investigator bias where the options given are of the investigator's interest, as well as the tendency of respondents ticking one category without even thinking through them (Kumar, 2011; Saunders et al., 2016). Closed-ended questions help ensure that the information is easily obtained and they are easy to analyse (Kumar, 2011). The way instruments are phrased is of paramount importance to the way participants will respond in the survey.

Kothari (2012) suggests that when instruments are designed, they must be clear and easily understood, simple (convey one thought at a time only) and should conform to the participant's line of thinking. Neuman (2014) also weighs in and highlights some major principles to guide in the design of the instrument which include avoiding any probable confusion on the respondent, designing valid and reliable questions, keeping the perspective of the respondent in mind, clear and meaningful questions. Neuman (2014) concurs with Greener (2008) and Greenfield and Greener (2016) by summarising some of the necessary writing skills to be avoided for an instrument, namely circumventing slang, technical jargon and abbreviations; avoiding confusion, vagueness and ambiguity; avoiding prestige bias and emotional language; circumventing double-barreled questions; avoiding leading questions; avoiding of false promises; avoiding questions about the distant future intentions; circumventing double negatives in the questions and avoiding unbalanced or overlapping response categories. In this research, the researcher avoided the use of abbreviations and slang, and questions were designed without any bias, emotional or leading questions, each question asked only one concept to avoid double-barreled questions, no false promises or future promise intentions were made and all response categories were balanced and consistent throughout. All these features of instrument development were validated by experts and tested through piloting to make sure that they align with the fundamental questionnaire writing skills (Greener, 2008; Greenfield & Greener, 2016; Neuman, 2014).

This study used closed-ended questions so that information gathered becomes quantifiable (Kumar, 2011; Muller, 2014) and analysis can be conducted. Walliman (2014) asserts that in closed-ended questions, the respondent chooses from the given set of answers and they do so quickly. Banerjee (2015) submits that closed-ended questions are easy to understand, which leads to answers that are consistent. Investigator bias was overcome by using all possible responses from a respondent and the questions were brief so that the respondents would not lose focus.

Neuman (2014) argues that designing an instrument has a great impact on the results to be obtained from the study. Therefore, there is need for a final instrument which the respondent can answer honestly, without any bias and that truly represents reality about the subject matter. In the instrument design, the researcher made note of the following design fundamentals as supported by several studies (including Alnathier et al., 2012; Gerber & Hall, 2017; Greenfield & Greener, 2016; Jain et al., 2016; Kothari, 2012; Neuman, 2014; Riley-Tillman & Reinke, 2011):

- Instructions were clear and consistent for respondents to complete;
- Content that promotes bias, especially leading questions, was clearly scrutinised;
- Having a clear, neat and good layout of the questions;
- For students not responding on email, the researcher sent non-response reminders twice every week to increase chances of response;
- Avoidance of sensitive, repetitive and irrelevant questions;
- The order of the questions was made to flow and questions that are related were grouped;
- The use of closed-ended questions as opposed to open-ended questions tends to increase the response rate;

An instrument has the following advantages in a study (Kazi & Khalid, 2012; Kothari, 2012; Neuman, 2014; Saunders et al., 2016):

- It is cheap as compared to many other data collection tools;
- It is free from bias when compared with other techniques because there is no association with the interviewer and respondents are free to answer using their own words;

- There is adequate time to come up with well thought responses;
- Instruments are often made up of large samples and this strengthens the results, making them more reliable and even dependable.

To avoid low response rate, which affects the simplification of the results, some guidelines were followed by the researcher (Greenfield & Greener, 2016; Guerin & Dohr, 2005; Kazi & Khalid, 2012; Kumar, 2011; Riley-Tillman & Reinke, 2011):

- Keep the instrument short and to the point;
- If questions are closed-ended, they are quicker to answer;
- Obtaining captive audience of students like in a classroom to explain the purpose, significance and relevance of the study is quick;
- The use of hard copies, especially for those who had challenges in accessing the internet.

The above techniques in instrument construction and design were adopted in the drafting of the instrument for gathering information for the SPIPP empirical model. As a research procedure, all new instruments are supposed to be subjected to expert review and then to pilot testing in order to validate if they are reliably measuring what they are supposed to measure (Kazi & Khalid, 2012). This was discussed in section 4.10.5.1 under Expert review and 4.10.5.2 under Pilot study section. This is done in research to increase the reliability of the measuring instruments. The instrument design procedures for the research instruments are discussed below.

4.10.3 Instrument refinement process

The process of designing a questionnaire (instrument) goes through various iterations in research. As the process goes through many steps, it is imperative to realise that the developed instrument must be correlated to the aims and research questions of the research (Kumar, 2011). In fact, during instrument design, there is need for a proper linkage between the concepts in aims being investigated and its context in theory (Jain et al., 2016; Kumar, 2011). In the design of the instrument, the researcher used literature theory to design the instrument items. The formulated items or statements were meant to address and answer the research questions highlighted in

section 1.4 and help attain the research aims set in section 1.5. The processes involved in the instrument design are depicted in Figure 4.3 below.

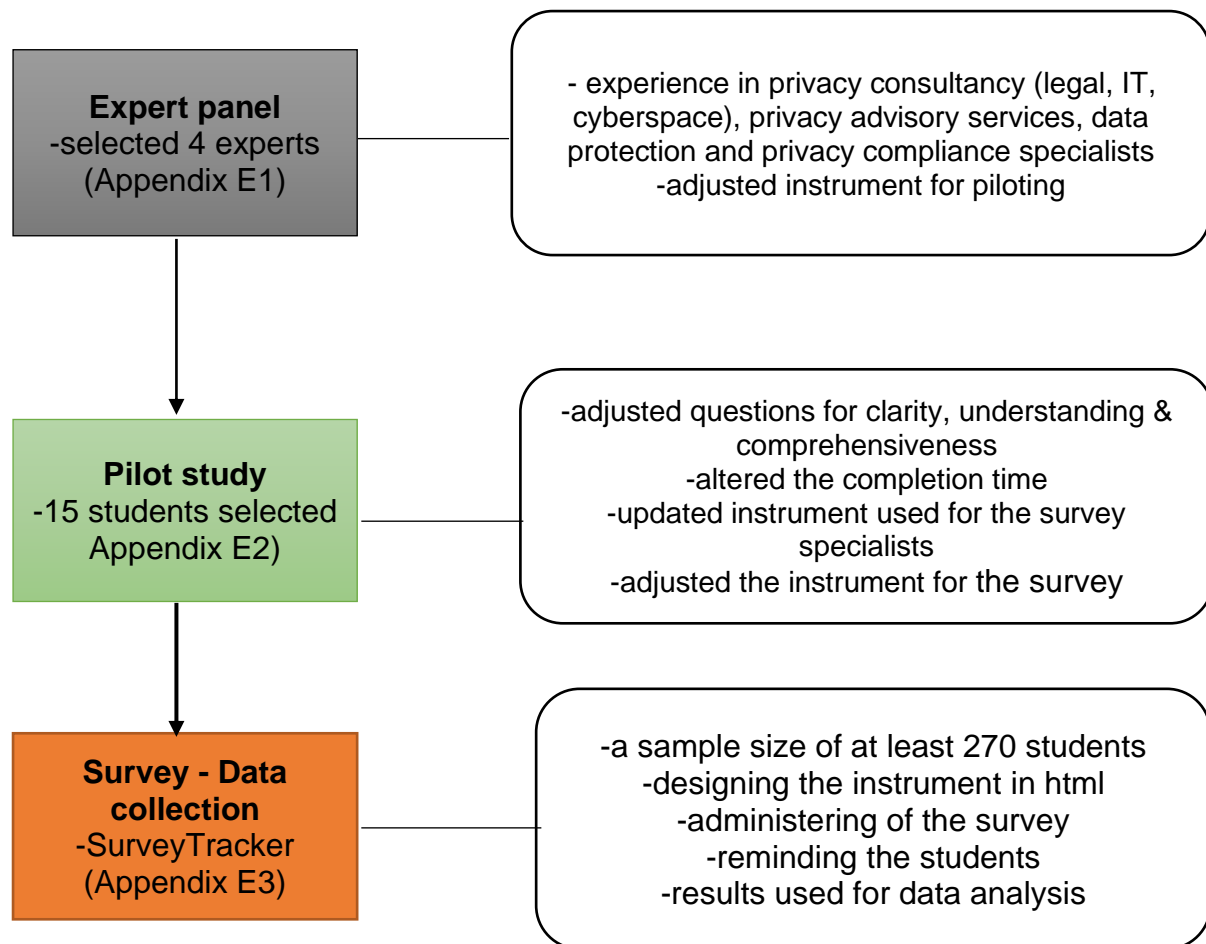


Figure 4.3: Instrument design and sampling

The statements in section 3.8 were taken through the process of expert panel review as conversed in section 4.10.5.1. Expert review is important because it increases the instrument's face validity. Face validity was used on the suitability of the statements on the researcher and the students who responded to them. Face validity was described in section 4.10.8 under Validity. The experts were requested to complete the participation information sheet shown in Appendix C1 and consent to participate in Appendix D1.

The output from the expert review was used as an input for the pilot study. The pilot study involved a total of 15 students. A discussion of pilot review was done in section 4.10.5.2. The focus was on ascertaining that the statements were comprehensive, clear and easily understood. The students were also made to complete the

participation information sheet shown in Appendix C2 and consent to participate in Appendix D2 for the pilot group.

The updated version of the pilot study was then converted into html format, ready for the online survey and this is shown in Appendix E3. This is the version that was disseminated to the participants (students). After conducting the online survey, the results were analysed statistically. This is given attention in Chapter 5, which deals with data analysis and discussion of research findings. Statistical analysis starts with processes like data coding and data cleaning for import to the SPSS package, putting variable labels and value labels among other labels. Also included are descriptive statistics, inferential statistics, exploratory and confirmatory factor analysis, ANOVA, t-tests and correlations analysis.

The next section narrates the various steps taken in the item generation and development of the survey instrument.

4.10.4 Structure of the IPPS survey instrument

This section describes how the instrument for IPPS was designed. A preface as an introduction and the definitions used in the research were encompassed in the front unit. The study instrument was segmented into two sections to aid in realising the objectives of the study stated. These are discussed below.

4.10.4.1 Section 1: Biographical information

A few questions on biographical information were developed in the study to obtain information usable for descriptive purposes. These are:

- Age

This was requested from the participants because it was used to determine whether the various concepts and components had similar interpretations to various participants of age groups. This is done to understand various age group conceptions on a particular field (Greenfield & Greener, 2016). To properly have an analysis on how different generations perceive how collected information was used within universities, their awareness levels, their expectations and their confidence in the

university, the researcher clustered the age into seven ranges, namely the 18 - 25 years, 26 - 30 years, 31 - 35 years, 36 - 40 years, 41 - 45 years, 46 - 50 years and the above 50 years category. These age generations cater for all students at the university; there are students who enrol soon after completing their high school and there are students who enrol for postgraduate studies after attaining the age of 50 years. A student chooses one age group which his/her age falls into.

- Gender

The gender is categorised into three main groups, namely male, female and other. It is very important to know the type of gender and how they perceive privacy as there can exist differences between genders (Chen, Ping & Chen, 2015; Ozdemir et al., 2016). Also important is to avoid discrimination through the inclusion of "Other" to accommodate everyone with their gender preferences. A student chose one option for the gender.

- Nationality

Although the research was conducted in Zimbabwe, it is imperative to also note that the university under study also allows enrolling of students from abroad. Therefore, there was a possibility of having students from abroad learning at the university. This was important, as it assisted in ascertaining what students (respondents) from countries, other than Zimbabwe would perceive privacy of personal information. Six options were given, namely, Zimbabwe, Africa, Europe, America, Australia and Asia. By so doing, all continents were covered.

- Learning mode

When students enrol at the private institution, they are given the right to select the mode of study. These are a) conventional - where students learn on daily basis from Monday to Friday and starting lectures from 08:00 hours to 16:00 hours, b) parallel - where students learn in the evening from 17:00 hours to 20:00 hours and during weekends and c) block - where students learn for specified two-week period, twice a semester. The researcher added "Other" to incorporate any other learning arrangements within the institution. A student chose one learning mode from the available options.

- Year of study

The university caters for students from their first year until they get to fourth year for undergraduate programmes, masters students for two years and doctorate students for a minimum of three years. It also caters for short courses spanning 6 months. A student indicated which year they were in at the stretch of the study.

- Programme

The programmes offered at the university were limited and included Business Management and Information Technology (BBM&IT), Bachelors of Accounting (BAcc), Bachelors of Management in Finance (BBM Finance), Bachelors of Management in Marketing (BBM Marketing), Bachelors of Arts in Development Studies (BA Dev Studies), Bachelors of Arts Dual Honours (BS) specialising in 2 subjects, Bachelors of Theology (BA Theology), Masters of Business Administration in Entrepreneurship (MBA), Doctor of Philosophy (DPhil) and 6 months Certificates in various disciplines. A student indicated at least one programme that they are enrolled in.

4.10.4.2 Section 2: Personal information privacy perception statements

The second section in the IPPS instrument incorporated 54 statements that were used to ascertain student perceptions on the privacy of their personal information from three concepts, namely the awareness, expectations and confidence. The nine components regarded the FIPPs as the reference point and were also fortified in the OECD Protection of Privacy and Transborder Flows of Personal Data document of 2013, the GDPR and the ZDPA bill. A discussion of these components was done in Section 3.5 of chapter 3 and it was concluded that the components for the IPPS instrument are notice/ awareness, purpose specification, information quality, use limitation, collection limitation, individual participation, privacy education, privacy policy and consent and these were used for measuring the three privacy concepts of awareness, expectations and confidence for privacy perceptions. Table 4.1 below depicts the 9 components and the corresponding allocated number of items for each component, as shown in Appendix E1.

Table 4.1: Components and allocated items

IPPS component	Allocated item numbers in the instrument	Total number of items in the instrument
Notice/ openness	Awareness: 1 & 2 Expectations: 3 & 4 Confidence: 5 & 6	6
Information quality	Awareness: 7 & 8 Expectations: 9 & 10 Confidence: 11 & 12	6
Purpose specification	Awareness: 13 & 14 Expectations: 15 & 16 Confidence: 17 & 18	6
Use limitation	Awareness: 19 & 20 Expectations: 21 & 22 Confidence: 23 & 24	6
Collection limitation	Awareness: 25 & 26 Expectations: 27 & 28 Confidence: 29 & 30	6
Individual participation	Awareness: 31 & 32 Expectations: 33 & 34 Confidence: 35 & 36	6
Privacy policy	Awareness: 37 & 38 Expectations: 39 & 40 Confidence: 41 & 42	6
Privacy education	Awareness: 43 & 44 Expectations: 45 & 46 Confidence: 47 & 48	6
Consent.	Awareness: 49 & 50 Expectations: 51 & 52 Confidence: 53 & 54	6
TOTAL NUMBER OF ITEMS IN THE INSTRUMENT		54

Source: Author's own compilation

Notwithstanding the fact that every component is measured in terms of the students' privacy awareness levels, privacy expectations and their privacy confidence in the university, there were two items for each component from each perspective. The students (respondents) were expected to fill in all the sections of the instrument, selecting from various options as depicted in the scales provided.

4.10.4.3 Description of the scale

The 5-point Likert scale was used because it is reliable, captures results based on many options and it generally provides stable results (Mathers et al., 2009). A Likert scale gives a range of options to a given statement or question (Cohen et al., 2011). Respondents only need to either check or circle their opinion (Salkind, 2017). Using a Likert scale, the respondent makes a choice to specify how they either strongly disagree or agree with a statement (Saunders et al., 2016). Thus, a Likert type scale is developed from a number of formulated statements that express an attitude that is favourable or unfavourable to how the respondent will react (Kothari, 2012). The IPPS instrument is a survey that permits self-evaluation and can be easily administered in groups or individually. The rating scales prompted the respondents to choose one alternative from a possible set of categories (Greenfield & Greener, 2016; Mathers et al., 2010). The participants in this research were obliged to rate the 54 items by selecting the most suitable alternative on the five-point Likert scale and the ratings were arranged as follows:

- Strongly disagree – this indicates that the respondent is in strong agreement.
- Disagree – this indicates that the respondent disagrees to some extent.
- Do not agree or disagree – this indicates that the respondent is neutral or uncertain.
- Agree - this indicates that the respondent agrees to some extent.
- Strongly agree - this indicates that the respondent is in strong disagreement.

The main advantage of using such a scale is that it becomes easy to understand the questions and consistency in the responses is needed (Banerjee, 2015). On the contrary, the main disadvantage of the Likert scale according to Mathers et al. (2009),

is that sometimes researchers succumb to the temptation of summing all the scales into one single score, which might be misleading.

4.10.4.4 General information for survey completion

The average completion time for the instrument was 20 minutes. Some students took lesser time than the prescribed 20 minutes and some took more. The personal information privacy perception instrument was designed as an electronic/online based survey and was administered using the Survey Tracker software. In the instrument, there was a Yes and No button where the respondents either could click on “Yes” if they consented and they would move to the next page or “No” and move to the last page.

Before the survey was conducted, the following information was availed to the respondents to conform to research ethics requirements:

- the research title;
- the researcher’s details;
- the research purpose;
- the benefits of participation;
- the assurance that the research was voluntary and the respondent had every right to disengage any time when they felt like doing so, and without any adverse consequence;
- the estimated time of completion of the instrument;
- assurance of confidentiality and anonymity of information provided;
- the assurance that the information supplied would be kept in a secured and protected environment;
- the indication that the researcher appreciated the participants for their willingness to assist in the research.

4.10.5 Instrument finalisation

To respond to the research questions in Section 1.4 and achieve the aims of the research in Section 1.5, two statements were summarised at the end of each component derived from the nine privacy components in Section 3.5. These were then

converted into instrument questions for the survey as summarised in Table 3.2. The instruments were aligned to the literature chapters (Chapters 2 and 3). These were then taken for expert review analysis.

4.10.5.1 Expert review

The experts sample is chosen for a specific purpose, as the name suggests (Cohen et al., 2011). This implies that the sampling technique relies more on the primary consideration of choosing an experts sample that will furnish the right information to accomplish set objectives of the study (Kumar, 2011). It is very useful when the sample is very small but informative, and a known indicative of the sample is to be intensively analysed (Greener, 2008; Kothari, 2012; Saunders et al., 2016). This was the case in the selection of four individuals into the experts' panel of this study.

The instrument is reviewed by experts in the field in the industry or by academics (Saunders et al., 2016). One way of improving questions in the instrument is to have an independent panel of experienced researchers review and critique the instrument (Neuman, 2014). They assist in undertaking a focused and a comprehensive directive on the questions and are expected to give feedback or make recommendations (Alnatheer et al., 2012; Kumar, 2011). An expert review in research is crucial as it improves the questions' content validity (Saunders et al., 2016). It is crucial to ask experts in the field for some comments, feedback and recommendations on the suitability, structure and representativeness of the designed items as seconded by Saunders et al. (2016). The instrument in this research is new and hence there was need to involve an expert panel. Lynn (1986) suggests that a comprehensive expert review must have between three and ten expert reviewers.

Expertise in the field of information privacy and privacy compliance is the criteria that was used to recruit the experts. The researcher had to contact them via email, indicating the objectives of the research and asking them to participate in this research. As a fundamental baseline, the experts, as participants in this research exercise, had to provide information that added value to the study. Using any number of experts, the level of error detection can be plotted as shown in Figure 4.4 below.

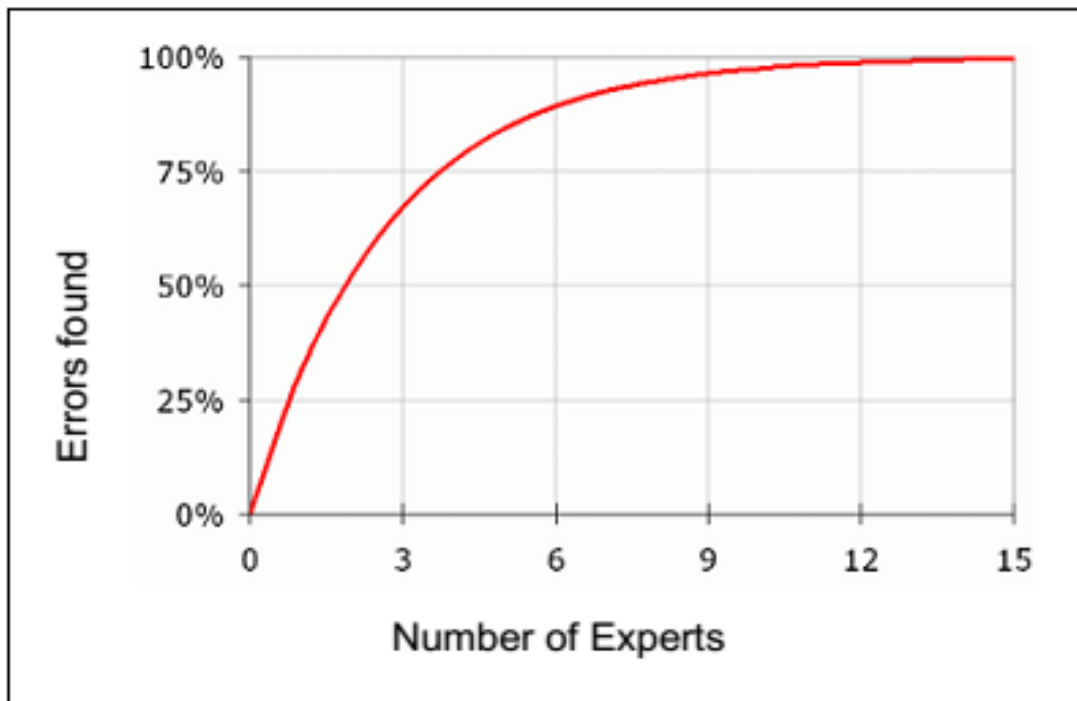


Figure 4.4: Error detection rates (Nielsen & Landauer, 1993)

As highlighted in Figure 4.3 above, the four experts used in this study can identify at least 75% of the existing errors (Nielsen & Landauer, 1993) and this is good enough, considering that if the number of experts increases (so does the effort and costs of getting them), it will not have an impact in terms of their effect on the research because it will have reached saturation. Therefore, the four chosen experts in this study were considered ideal.

The first criteria for expert reviewer selection was experience in privacy implementation with an IT focus and/or legal background. The expert review panel in this study was made up of 4 experts (expert sample space) who had experience beyond privacy consultancy (both legal and IT background), but also privacy consultancy in cyberspace, privacy advisory services as well as data protection and privacy compliance specialist. Another criterion was that the experts should have more than three years privacy related experience and should have a post graduate qualification. These were the key criterion for selecting the experts as they were people of known expertise in the field of privacy (Kumar, 2011). It was also a prerequisite to get their participation consent first. As such, each participant received a participant information sheet (see Appendix C1) and was requested to sign a consent document (see Appendix D1).

Table 4.2 below presents data on the expert panel participants relating to their field of expertise, job titles, their experience as well as their qualifications.

Table 4.2: Expert panel participants

Field of expertise	Job title	Experience (years)	Highest qualification
Expert 1: Privacy consultant - with both legal and IT background	Privacy Cyber-physical Analyst	3 years	PhD
Expert 2: Cyber insurance	Cyber Insurance Underwriter	6 years	Certifications: CAIB(SA) specialising in Finance, Certificate in Cyber Security, currently studying at ISACA
Expert 3: Privacy consultant	Senior Manager: Privacy Advisory Services	9 years	PhD
Expert 4: Data protection and privacy, privacy compliance, risk management, cyber security, data protection and cyber security law	Group Privacy Officer	7.5 years	MSc: BCOM (Information Systems, Law, Psychology), Post-Graduate Diploma in General Management, Masters in Business Administration (current), Fellow in Information Privacy, Certified Information Privacy Manager, Certified Information Systems Auditor, Certified Information Privacy Professional: EU, Certified Information Privacy Technologist,

			Certified Information Security Manager.
--	--	--	--

For the recruitment of the expert reviewers, each expert panel was contacted directly via phone and email. The expert reviewers were asked to provide their review responses electronically and to email them back to the researcher. A comment box was provided for general comments about the biographical section which the expert panel would like the researcher to consider or amend in order to improve the instrument. There was also a section that comprised of the 54 statements. The expert reviewer was to use a tick (✓) to indicate whether they believed the statement was essential to be included or not and whether it was clear or not. A comment box was provided at the end of the 54 statements for general comments about the statements which the expert panel would like the researchers to consider or amend in order to improve the instrument. The initially designed (original) instrument is included in Appendix E1.

a. Expert Review Comments Analysis

As prescribed by Saunders et al. (2016), there is need to engage and seek suggestions and comments from a cluster of experts on the representativeness and suitability of questions before doing the actual study. This enables content validity and to make the necessary amendments before piloting (Kumar, 2011). Although some experts pointed out that certain questions were not essential, the researcher did not remove them since they were part of the theoretical model. Instead of removing them, the researcher adjusted the questions so that they became clearer and more understandable.

The summarised overall percentages, based on the opinion of the experts from the perspective that the statements were essential or not and whether the statements were considered clear or not was done by the researcher. Each component had 2 statements which were measured based on the construct's awareness, expectations and confidence. This gives a possibility of 6 responses on each component. With 4 experts, there were 24 possible scenarios for either "Essential" or "Not Essential". The same rule was applied for whether the statements were "Clear" or "Not Clear". The selections made for all the components for the same aspect were then summed up

together to give a total, which was calculated as $24 \times 9 = 216$ for the essentiality and clarity of the statements. Table 4.3 below gives a summarised review of the comments of experts.

Table 4.3: Summary of expert review feedback

Component	Essential	Not Essential	Total	Clear	Not Clear	Total
A - Notice/Openness	15	9	24	12	12	24
B - Information Quality	18	6	24	12	12	24
C - Purpose Specification	16	8	24	18	6	24
D - Use Limitation	15	9	24	13	11	24
E - Collection Limitation	18	6	24	20	4	24
F - Individual Participation	18	6	24	13	11	24
G - Privacy Policy	17	7	24	24	0	24
H - Privacy Education	14	10	24	15	9	24
I - Consent	20	4	24	15	9	24
TOTALS	151	65	216	142	74	216
Percentage (%)	70	30	100	66	34	100

From the above table, it can be generalised for all reviewers that:

- 70% of the experts agreed that the items were essential, with 30% not being considered essential. These were then adjusted to increase their essentiality.
- 66% of the experts expressed that the questions were clear, with 34% of their views indicating that the questions were not clear. Based on the reviewers' comments, these were then adjusted to increase clarity.

Below is a discussion of the feedback from the expert reviewers based on their suggestions and comments on whether the questions were essential and clear or not.

b. Essential and Not Essential

The four expert reviewers gave their comments on the instrument based on their opinions for this category. Amongst the four reviewers, the average number of questions that were shown to be "Not Essential" was 30%. As highlighted above, these questions were not removed. Rather, the researcher adjusted the questions in accordance with the said comments. The following are some of the notable adjustments which were done to increase the relevance of the statements:

- Statement 5 was considered "Not essential" by one expert and suggested that it can be altered from, *"I am confident of privacy through privacy notices"* to, *"I am confident of universities' privacy practices through privacy notices"*.
- Statement 8 was considered too broad as it could be interpreted to refer to security safeguards and not information quality. This prompted two expert reviewers to consider it "Not essential". The statement was adjusted to, *"I am aware that the university should protect my personal information for information quality"* from, *"I am aware that the university should protect my personal information"*.
- In Statement 35, a privacy expert considered it "Not essential" because it was incomplete and the statement, *"I am confident of requesting from the university, a confirmation on what personal data the university has collected about myself"* was adjusted to *"I am confident of receiving upon request from the university, a confirmation on what personal data the university has collected or requesting copies of the record of personal information about myself"*.
- Statement 51 was altered from, *"I expect to have the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements among others.)"* to, *"I expect the university to enable me to exercise my right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements.)"*.

c. *Clear and Not Clear*

The four expert reviewers gave their comments on the instrument based on their opinions for this category. Amongst the four reviewers, the average number of questions that were shown to be "Not Clear" was 34%.

After going through their suggestions and comments, there are certain questions that were deemed "Not clear". The questions regarded "Not clear" by the expert reviewers were adjusted as per the reviewers' comments and suggestions. The following are some of the notable adjustments that were done to make the statements clear:

- Statement 4 was adjusted to *"I expect the university to publish a privacy notice" from, "I expect the university to publish a notice for privacy"*.
- Statement 17 was adjusted from *"I am confident that the university will specify the purpose when collecting my personal information at the point of collection"* to *"I am confident that the university will specify the purpose of collecting my personal information at the time of collection"*.
- Statements 19-24 had to be adjusted on the part, *"by the authority of" the law* to *"in line with" the law*.
- Statement 31 was adjusted from, *"I am aware that I can request from the university, a confirmation on what personal data the university has collected about myself"* to, *"I am aware that I should be able to request copies of the records of my personal information from the university"*.
- In Statement 52, an adjustment was done for clarity on the statement, *"I expect to have the right to opt out for the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements among others.)"* and it became, *"I expect the university to enable me to exercise my right to opt out on the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements among others.)"*.

After receiving the feedback and adopting the recommendations and suggestions, the instrument was subjected to pilot testing to ascertain it was measuring what it was supposed to measure and in a reliable manner (Kazi & Khalid, 2012). Refer to Appendix E2 for the updated instrument for the pilot study.

4.10.5.2 Pilot study

After the expert reviews, the instrument can be piloted. This helps in improving the instrument before the actual survey is conducted. By definition, a pilot study is an informal study that acts as a preamble for the actual survey, and it is used to try the feasibility of the survey fieldwork and assists in calculating the sample size (Kumar, 2011; Molenberghs, 2010; Teijlingen & Hundley, 2002). It is done to also increase reliability and validity when the data extraction process is being done (Mohammed & Tejay, 2017; Saunders et al., 2016; Tricco et al., 2011) and to ensure that it is operationalised properly (Almadhoun et al., 2011; Bhattacharjee, 2012). As pointed out by Bhattacharjee (2012), a pilot study aids in assessing if the questions asked are understandable to the targeted audience (respondents), ensuring that the instruments in the study are reliable as well as valid measures with respect to the concepts of interest. These were done through face validity and construct validity which was discussed in section 4.10.7. This is also indicated by Creswell and Creswell (2018) who posits that a pilot review is prudent in that it increases content validity of the instrument as well as improves the items, their format and the scales used. The instrument must be piloted for its comprehensibility and its legibility (Jain et al., 2016).

In a pilot study, the participants provide feedback and this might result in certain items either being deleted from the list of items or altered (Vail et al., 2008). A pilot test gives a remedy in detecting potential problems within a research design like detecting if the questions makes sense to the targeted sample (Bhattacharjee, 2012; Saunders et al., 2016). According to research (Almadhoun et al., 2011; Bhattacharjee, 2012; Jain et al., 2016; Kazi & Khalid, 2012; Saunders et al., 2016), the reasons for a pilot study can be summarised as:

- determining how long it will take to complete the instrument;
- ascertaining if the participants follow and understand the instructions to complete the instrument;
- aligning the researcher's understanding with that of the participants;
- diffusing the aspect of uneasiness on the part of the respondents, and
- validating the structure and layout of the instrument.

For a student to participate in piloting, they were supposed to be a student at the Zimbabwean university studied, with a valid customised university email address and be older than 18 years. The researcher approached students who were in different classes and invited them to join the presentation for piloting. Only students who were proficient in English were included. A total of 15 students were from the various departments of the institution. This was done so that the population selected in the sampling process represents the views of the main respondents of this study, namely students. As indicated in Section 4.9.4, the sampling technique used to get the pilot study respondents was convenience sampling. The pilot group was selected on a voluntary basis with the condition that the participant must be a student at the private institution, with a valid customised university email address and must be older than 18 years. Only students who were proficient in English were selected.

Pilot study feedback

After conducting the pilot study, a few notable comments included:

- Most of the respondents felt 15 minutes were adequate to complete the questions. It was the researchers' assessment that most of the respondents finished in between 10 to 13 minutes. Only 2 finished in 15 minutes. Therefore, 15 minutes was deemed an adequate time to complete the instrument.
- One respondent questioned why on the nationality, there was Zimbabwe and Africa as options, yet Zimbabwe is in Africa. To the respondent, it appeared as repetition. The researcher proposed to edit it to "Other parts of Africa".
- The instructions were clear and understandable to the respondents. All were in agreement that they understood the questions.
- Respondents felt easiness when they were responding to the questions.
- There were two respondents who felt the questions seemed like they were repeating. To this, the researcher had to explain that it might seem so because the questions were being asked from three perspectives (awareness, expectations and confidence), measuring the same concept. The researcher therefore added a sentence to the instrument to explain that "*There are 9 components for the Student Personal Information Privacy Perception (SPIPP). Each will be measured from three dimensions, i.e., the awareness, the expectations and the confidence*".

After the pilot study, a few comments and recommendations were added onto the instrument for the final survey instrument.

4.10.6 Data collection and administering the survey

This section discusses the development of the final html survey as indicated in Appendix E3. The output of a successful pilot test is normally adjusted if need be and converted into the html format, after which it will be used for collecting data on the sampled population in the final research (Bhattacharjee, 2012). Data has to be collected in the same way for all the respondents (Molenberghs, 2010). According to Gilliland (2014), a successful data collection will have the goal of the data collection clearly known and understood. There are various ways of sending the developed instrument to the respondents.

In this study, the instrument invite with a hyperlink to the html instrument was broadcasted to the participants through emailing as the main method for sending out the survey. The invitations were sent to respondents using emailing because of the nature of the respondents; most students spend their time online either on their laptops or mobile devices and internet is easily accessible to them.

For the data collection process in this study, at least 270 students sample size was needed for the survey. Students were communicated with as per the ethical considerations (section 4.13) and received the instrument via their email addresses. Students were to respond to the instrument within a period of 5 weeks in total as discussed in Section 4.8. Having obtained the permission to do the research from the UNISA Research Ethics Committee as shown by the Ethical Clearance: 030/KM/2019/CSET_SOC (Appendix A2) and permission granted by the university Research Committee (Appendix B), the instrument was uploaded onto the SurveyTracker application and it was hosted by Organisational Diagnostics. This data collection procedure was considered ideal since the sample population (students) spent most of their time online and are computer literate, having access to their emails as well as the internet (Plessis, 2018). To the students who could not access the internet, hard copies were also made available for them to complete. These were manually completed and returned to the researcher. During data collection, the

researcher needs to make sure that there is no bias when data is being collected (Jackson, 2009).

The survey application had a cover letter describing the purposes and perceived benefits of the survey as well as the set of questions which solicited biographical information as outlined in Section 4.10.4.1. The cover letter was included in the email that was sent to the sample invited to participate using the bulk e-mail message.

Some unforeseen events during the data collection process forced the researcher to adopt another plan to send the survey instrument to the students. There were continuous power cuts which affected the whole nation of Zimbabwe, and many students indicated that they had seen the invitation link but would not be able to complete the instrument online. This prompted the researcher to avail the survey in hard copy. Even for hard copies on survey, the researcher had to adhere to the ethical code of conduct. The researcher gave a presentation first before distributing the hard copies to students. During the presentation, the researcher explained the purpose of the research, sought consent for participation and assured the respondents that their feedback would be anonymous and confidential. Students completed the hard copies and the researcher had to manually capture the students' responses into the SurveyTracker software.

In conducting research, it is important to ascertain if the research instruments are measuring what they are intended to measure so that it fulfils the objectives of the research. This is done through the process of reliability.

4.10.7 Reliability

Reliability is the ability of the test instrument to be repeated multiple times by different researchers in the same manner, measuring the same instrument and giving a consistent result (Field, 2009; Gerber & Hall, 2017; Jain et al., 2016; Kothari, 2012; Neuman, 2014; Oats, 2012; Salkind, 2017; Saunders et al., 2016). According to the Survey Methods (2017), reliability is a key attribute of quality research and a very important tool as it helps avoid the risks of executing erroneous conclusions from the data (unreliable data yield meaningless conclusions). For the research instrument's

reliability to properly increase, it is also imperative to appreciate various threats to reliability.

Some of the threats to reliability noted by Jain et al. (2016) and Saunders et al. (2016), and which applied to this study, include:

- Participant error (anything that might affect the way a respondent performs),
- Participant bias (any aspect that can induce a false response to the participant),
- Researcher error (anything that alters the researcher's interpretation),
- Researcher bias (anything that induces bias when the researcher is recording some responses).

Saunders et al. (2016) suggests that the common approaches for assessing reliability after data collection is undertaken include considering the following stages in the instrument design phase:

- test re-test
- internal consistency (which was adopted and used in this study)
- alternative form

Some of the ways used to increase reliability in this research, as adopted from Salkind (2017), include:

- Having a large sample which is most likely to be a representation of the population. A population of at least 270 students was used as the sample.
- Removing all unclear items because respondents could end up interpreting them differently and ultimately respond differently.
- Making sure that all the instructions are standardised.
- The study was done when there were no external events to influence true reflection of the respondents' views.
- Scoring procedures were maintained using the same 5-point Likert scale.
- Questions were moderated in terms of their difficulty.

The approach adopted in this research process to test reliability was *internal consistency* and it involves correlating the instrument responses with each other (Hair, Black, Babin & Anderson, 2014; Saunders et al., 2016). This means that it measures consistency of all the responses, either all the questions from the instrument or from a subgroup of the questions (Saunders et al., 2016). Cronbach alpha was applicable in the calculation of the internal consistency (reliability) of the study. Cronbach alpha coefficient is discussed under data analysis.

Besides focusing on the reliability of research items, validity increases relevance of questions in research. This is discussed in the next section.

4.10.8 Validity

According to researchers (Evergreen, Gullickson, Mann & Welch, 2011; Gilliland, 2014; Jain et al., 2016; Kazi & Khalid, 2012; Kothari, 2012; Saunders et al., 2016; Tricco et al., 2011), validity is regarded as the degree to which an assessment is measuring what it is expected to measure in relation to the investigation being made. It also gives the truthfulness of results and suggests how well an idea aligns with the actual reality, addressing questions of how we can measure social reality making use of constructs about it (Neuman, 2014). In quantitative research, validity is attained through objective numerical and statistical measurements (Gilliland, 2014). To begin with, an instrument's validity can be enhanced through the crafting of sound questions and checking their appropriateness for the targeted respondents (Evergreen et al., 2011). There are four common forms of validity (face, content, construct and criterion). This study adopted the content validity, face and construct validity.

Content validity is defined by Kothari (2012) and Saunders et al. (2016) as the degree to which the instrument sufficiently provides coverage of the questions under investigation. Content validity was considered by ensuring that the instrument was developed following theory (Chamroonsawasdi et al., 2017). Validity was also ascertained through the pilot study that was conducted. The following were key:

- Under content validity, questions ought to be developed from various dimensions of the concept being studied, and these were thoroughly investigated during the literature review in chapters 2 and 3.

- Use of theories and models that align with the research topic, problem statement and objectives as the vanguards of the research.
- Development of measuring instruments and concepts which are applicable to the model and in this study, these were adopted from the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data privacy model of 2013, GDPR and the ZDPA bill.
- Pilot testing of the instrument, which increases the internal validity, leading to less ambiguity of the instrument (Oats, 2012).

The second type of validity is face validity, and it looks at whether a particular test is valid from its surface, to those who chose it and the ones who will take it (Jackson, 2009). From a different viewpoint, face validity is when an indicator in the scientific world is perceived to make sense in measuring a particular construct based on its face value (Bhattacharjee, 2012; Neuman, 2014). In this study, face validity was achieved through expert reviews, which led to some adjustments being made.

The last validity type used in this research was construct validity. It is considered to be the most important type of validity in any recent research (Creswell & Creswell, 2018; Jackson, 2009). Construct validity refers to "how well a given measurement scale is measuring the theoretical construct that it is expected to measure" (Bhattacharjee, 2012, p. 37). It looks at the measuring instrument and assesses the degree to which it precisely measures the hypothetical construct that it was meant to measure (Jackson, 2009). Construct validity tries to ascertain whether test results relate to some elementary set of analogous variables and it connects the empirical test components score to some fundamental theoretical behaviour (Salkind, 2017). Creswell and Creswell (2018) also acknowledge that construct validity also assists in the identification of any positive consequences from the scores when they are put in the realm of practice.

Construct validity was achieved in this study through the following:

- According to Plessis (2018), assessment of content validity in an instrument is a step towards augmenting for its construct validity. This study considered content validity first, and this enhanced construct validity.

- Construct validity was also supported by the exploratory factor analysis (EFA), which is discussed in section 4.11.4.1.

The next section discusses the various statistical techniques used for data analysis in this study.

4.11 DATA ANALYSIS

After (sometimes during) the completion of data collection, the results need to be analysed and interpreted so that they can be useful and possibly contribute towards any conclusion (Gilliland, 2014; Oats, 2012). Data analysis is independent of the techniques used to collect the data. This is done to ascertain how the theory will inform the researcher's approach to data analysis and interpretation (Chilisa, 2012). The Statistical Package for Social Sciences version 25 (SPSS) was used for analysing the quantitative data. The following data analysis processes and approaches were used in this study:

- Data management
- Descriptive statistics
- Inferential statistics
- Factor and item analysis
- Structural equation modelling

4.11.1 Data management

The instrument was designed in HTML format in SurveyTracker. Before getting the logic of the data, a precursor to analysing data is the coding, entry and checking of the data (Kumar, 2011; Salkind, 2017). It is crucial to establish the data type within the main measuring outcome like the interval, nominal or ordinal, and these data types, as suggested by Mathers et al. (2009), will in turn determine which statistical test type is more appropriate, which will in turn have some implications for the required sample size. According to Mathers et al. (2010), data is assigned some numerical code and once done, it has to be entered in the data analysis software for data analysis. In this study, the SPSS software package was used to enter the data. The section below discusses the descriptive statistics that were used for statistical analysis.

4.11.2 Descriptive statistics

Descriptive statistics gives reporting, graphical and numerical procedures in summarising a data set in an understandable way (Oats, 2012; Rossiter, 2017; Wiley and Pace, 2015). It provides the numerical and graphic procedures in summarising the collection of data that it is clear and understandable (Hair et al., 2014; Jackson, 2009; Wiley and Pace, 2015). Descriptive statistics is centred on the exhaustive measurement of population features (Lehman et al., 2005). Assessment of the university population for this study included computing the mean (measure of the central tendency) and standard deviation of various parameters and concepts according to the designed instrument. In summary, descriptive statistics include the mean, mode (measure of central tendency), median, the frequency, range and standard deviation (measures of variation) (Jackson, 2009). Neuman (2014) argues that descriptive statistics is used for describing any numerical data. A positive aspect about descriptive statistics is that it permits the researcher to obtain an apprehension of how the data looks (Salkind, 2017) .

In this research, descriptive statistics took the form of mean and standard deviation. The mean values were used to ascertain potentially positive and negative perceptions on privacy of student personal information, based on a set cut-off point. The standard deviation would show how far the individual responses were from the mean values as indicated by Salkind (2017). A discussion of inferential statistics that were used in this research is done in the section below.

4.11.3 Inferential statistics

Inferential statistics give procedures to draw some inferences on a sample from the population (Wiley and Pace, 2015; Oats, 2012). Inferential statistics focus on using information from a large sample to estimate or make inferences about the whole population (Salkind, 2017). According to Lehman et al. (2005), the main value of inferential statistical analysis is that they allow one to review information gathered from a small sample and enable them to make inferences around the population. Hence, inferential statistics are useful when making inferences to situations generalised from the data. The inferential statistics used in this research include t-test, analysis of

variance (ANOVA) correlation analysis, specifically the Pearson Product-moment correlation (PPMC), and Spearman rho. These are discussed below.

4.11.3.1 The t-test

A t-test is usable when one wants to test whether two categories (groups) are different (Oats, 2012; Saunders et al., 2016). It is generally used for statistical significance (Kothari, 2012). In addition, Gerber and Hall (2017) argue that a t-test can be useful for the testing for differences amongst two groups for a continuous variable. Assumptions made when using a t-test include: assume that the population sample is approximately normal; it is a random sample; independent observations are made; there is no measurement error and population variances are equal (Kothari, 2012; Oats, 2012). In this study, a t-test was used to test the probability of student gender being different in terms of their opinions on privacy.

4.11.3.2 The Analysis of Variance

The Analysis of Variance (ANOVA) is used for testing whether the association between more than two variables is the same across multiple populations (Gerber & Hall, 2017; Greener, 2008; Kothari, 2012; Lehman et al., 2005; Walliman, 2014). ANOVA are a set of techniques that permits the comparison of three or more means simultaneously (Saunders et al., 2016; Weiers, 2011). The ANOVA also makes the assumption that the populations from where the sample is being drawn is approximately normal. In addition, it assumes homogeneity of the variances and independence of observations (Oats, 2012). The ANOVA tests whether the categories being tested are different (Rossiter, 2006; Saunders et al., 2016). ANOVA analyses the way in which data values are spread between and within data groups by making comparisons of means (variance) (Saunders et al., 2016). The ANOVA looks at the means from various independent categories and it is regarded as an extension of the t-test (Oats, 2012).

For this research, ANOVA was used for testing the perceptions of different age bands (the generation Z, the millennials, the Generation X, the baby boomers and the silent generation) on privacy, the perceptions of students from different learning modes

(conventional, parallel and block) on privacy and for the perceptions of students pursuing various degree programmes on privacy.

For the analysis of relationships that exist within variables, correlation analysis was done. The procedures followed are discussed below.

4.11.3.3 Correlation analysis

A correlation research in general is designed to show relationships that exist among the variables (Gerber & Hall, 2017). Correlation coefficient, according to Saunders et al. (2016), enables the quantification of strength between two numerical values. The correlation within research is defined as the extent to which two variables are related (Saunders et al., 2016). It is normally used to execute the estimation degree of relation of any two measures (Jain et al., 2016). The correlation can take values between +1 and -1 where a +1 signifies a perfect positive correlation (precise relation between the variables with a direct relationship), a value of 0 signifying the independency of the variables and -1 signifying a perfect negative correlation (precise relation between the variables with an indirect relationship) (Greener, 2008; Rossiter, 2006; Saunders et al., 2016; Weiers, 2011).

For the interpretation of the correlation analysis, effect sizes were used. According to Creswell and Creswell (2018), effect sizes are descriptive statistics that discover the potency of endpoints about group differences or relationships amongst the variables in quantitative studies. Every statistical technique can have the effect sizes calculated in order to ascertain its practical significance (Gerber & Hall, 2017). The effect size gives an estimated degree that a phenomenon under study like correlation exists in the population (Hair et al., 2014). Hair et al. (2014) posit that large effect sizes are easier to discover in bigger sample sizes and have more power as compared to smaller effect sizes. Salkind (2017) also submits that as the effect size gets bigger, it means that there is a big difference between the groups under study.

The most commonly used way of measuring the correlation amongst the variables is the **Pearson Product-moment correlation coefficient (PPMCC)** (Jackson, 2009; Neuman, 2014). The Pearson Product-moment correlation coefficient (r) is computed, indicating the variables' relationship. To assess the strength of relationships that exist

between two variables, the PPMCC was used in this research (Saunders et al., 2016). Sedgwick (2012) submits that Cohen (1998), the statistician who came up with the idea of effect sizes, suggested that for the effect size criteria for Pearson correlation, coefficients of 0.1 is considered to have a small effect, 0.3 is considered to have a medium effect and 0.5 is considered to have a large effect. Using a range from 0 (for no relationship) up to 1 (for a perfect relationship), this is used to ascertain the relationship strength (Greener, 2008; Salkind, 2017). A +1 indicates a perfect positive relationship, meaning that all variables will influence each other directly, that is, as one variable is increased, so is the other (Salkind, 2017). Conversely, Salkind (2017) points that a -1 indicates a perfect negative relationship indicating that the variables will influence each other inversely, that is, as one variable is increased, the other one decreases.

The PPMCC is useful for the analysis of the variables (awareness, expectations and confidence)' inter-factor association and if the correlated variables are numeric and relatively symmetric (Akpojivi & Bevan-Dye, 2014; Rossiter, 2017). This implies that the Pearson correlation coefficient tests the relationship strengths of continuous variables (symmetric relationship). The study assumed that relationships could exist between the various age bands and perceptions on awareness, expectations and confidence and between the nine components.

4.11.3.4 Spearman's correlation

The Spearman correlation measures the association degree amongst two ordinal variables (Cohen et al., 2011; Saunders et al., 2016). It is used provided there exist at least an ordinal variable (Greener, 2008). According to Kothari (2012), the prime objective of the Spearman's coefficient of correlation is to obtain the extent to which two or more sets of ordinal data ranking are similar or not similar. The statistical technique measures the association based on ranks of the observation, and not using the mathematical values of the data (Kothari, 2012).

Greener (2008) adds that just like the PPMC, Spearman's coefficient gives a relationship that is either positive or negative, with 0 indicating no relationship and 1 indicating a perfect relationship. This means that a value of the Spearman's correlation coefficient will vary between -1 to +1. A -1 will be a representative of a perfect negative

correlation, with a +1 also a representative of a perfect positive correlation between the variables concerned. The Spearman's correlation was used in this research in ascertaining the influence of year of study, as a biographical variable, on privacy, expectations and confidence of students.

4.11.4 Factor analysis

Factor analysis measures inter-relations between a variable set (Rossiter, 2017; Weiers, 2011). Ideally, factor analysis is a method that seeks to resolve a bigger set of measurable variables with respect to relatively few categories (factors) (Gerber & Hall, 2017; Hair et al., 2014). The ultimate objective of using factor analysis is that it enable the summarising data in order for patterns and relationships to be effortlessly understood and interpreted and is used for regrouping variables into reduced cluster sets on shared variance (Gie & Pearce, 2012). The two main types of factor analysis are the exploratory factor analysis (EFA) and the confirmatory factor analysis (CFA) (Decoster, 1998; Gerber & Hall, 2017; Gie & Pearce, 2012). Whilst the EFA attempts to unravel the complex patterns through exploring the dataset and testing the predictions, the CFA tries to confirm some hypothesis through using path analysis for the representation of factors and variables. In this research, both EFA and CFA were used in the manner discussed below.

4.11.4.1 Exploratory factor analysis (EFA)

The EFA is a technique used to unravel composite patterns and does this by traversing the data repository and proving predictions (Gie & Pearce, 2012). Gerber and Hall (2017) submit that EFA as a data reduction technique can be used to identify underlying or hidden dimensions in constructs that might or might not be observable from direct analysis. EFA is performed to ascertain if the distinct questions contribute (load) onto the dimensions as in the instrument (Gerber and Hall, 2017).

The first step is the determination of whether there is viability in conducting the EFA on the instrument items (Gerber & Hall, 2017). One technique for ascertaining the appropriateness of factor analysis is the Bartlett test of sphericity (BTS). The BTS is a statistical measurement for analysing the implication and significance of all the correlations in a correlation matrix (Hair et al., 2014). Hair et al. (2014) implies that

whilst the BTS affords for the statistical significance for the correlation matrix's significance correlations in at least some variables, increasing the sample size causes an increase in the sensitivity of the BTS to detect correlations in variables. The BTS was used in this study and it is considered significant and relevant at $p < 0.05$ (Cohen et al., 2011; Gie & Pearce, 2012).

The Kaiser-Meyer-Olkin (KMO) is a statistical techniques used to measure sampling adequacy and it is normally automatically calculated by the statistical package (SPSS) (Cohen et al., 2011). Schwarz (2014) posits that the KMO index represents how variables combine, which will aid in determining whether factor analysis is suitable or not. This is a measure used to ascertain the viability of conducting an EFA on the statements in the instrument (Gerber & Hall, 2017; Riley-Tillman & Reinke, 2011). If there is any strong correlation structure, the significance is that distinct items associate well and items can be grouped in factors and the opposite is true (Gerber & Hall, 2017; Gie & Pearce, 2012). Whilst the KMO value ranges from 0 to 1, the recommended KMO value that implies a strong correlation structure for EFA (where one should proceed with EFA) is believed to be higher than 0.5 and was used in this study (Gerber & Hall, 2017; Gie & Pearce, 2012; Riley-Tillman & Reinke, 2011).

Communality is defined as the sum of variance of a variable that is explainable by all the factors, that is, how well the variable can be explained by means of other factors (Gie & Pearce, 2012; Schwarz, 2014). Communalities indicate the stretch of association of individual items with others (Gerber & Hall, 2017; Hair et al., 2014). As clarified by Plessis (2018), an item without any unique variance has a communality of one, and conversely that which does not share its variance with any variable will have zero communality. Hair et al. (2014) submits that communalities must have a value of 0.5 or higher, which guarantees its return for analysis. However, in this study the researcher opted for 0.4 as the cut-off for the communalities and this was done after an intensive review of the items to ensure face validity. There is also need to analyse the reliability of the instruments and this is normally done using the item analysis technique.

Item analysis is a technique in statistics that assists in identifying the effectiveness of the test items (Cohen et al., 2011; Gerber & Hall, 2017; Kothari, 2012; Saunders et al., 2016). In a simplified manner, it is an assessment of who answered the question

or item correctly. The item analysis technique helps to analyse the internal reliability of an instrument e.g. questionnaire (instrument), survey and test (Gerber & Hall, 2017). An item analysis uses many statistical tactics to provide valuable information for improving the accuracy and quality of questions (Westwick, 1976). It is a technique that assists in identifying the effectiveness of test items and contributes to the fairness and discovering areas that have a potential to be problematic to students when they respond (Penfield, 2013). Item analysis is useful in that it assists in ascertaining which items to keep, to discard or to modify for improving the quality and accuracy of items (Field, 2009). Once the item quality is improved, it will also improve the test quality and consequently improve the validity and reliability of the test (NCSS, 2019). The widely used technique for calculating the item analysis is the Cronbach alpha (Gerber & Hall, 2017).

Item analysis produces the Cronbach's alpha coefficient value that measures the reliability of an item construct (Gerber & Hall, 2017). The objective of item analysis, according to Salkind (2017), is to have some numerical indices representing how good response items are and items analysis uses two such indices, namely item difficulty and item discrimination. Cronbach alpha is a measure of reliability (Hair et al., 2014). This research used the Cronbach alpha coefficient analysis to ascertain the reliability of the research. Cronbach's alpha is assumed to measure of the scale's "internal consistency" (Schwarz, 2014).

According to Gerber and Hall (2017) and Saunders et al. (2016), Cronbach alpha values are interpreted between 0 and 1 as follows:

- reliability is considered good for values above 0.8;
- reliability is considered acceptable for the values in the range 0.6 and 0.8, and
- reliability is unacceptable for values below 0.6.

Using the criteria highlighted above, a 0.7 Cronbach alpha coefficient was considered adequate for the analysis of data in the determination of the IPPS measuring instrument's acceptable reliability coefficient. The same technique was applied to the newly developed instrument.

In summary, and as discussed in this section, the EFA is a useful statistical analysis technique for the development and validation of instruments. It was used in this research for the reduction of items and to determine the validity of concepts and components. The next step is the discussion of confirmatory factor analysis (CFA).

4.11.4.2 Confirmatory factor analysis (CFA)

The CFA technique is generally used to ascertain the capability of predefined factor model to fit in an observed data set (Decoster, 1998). Analysis of Moment Structures (AMOS), also known as analysis of covariance, which is an extension of the SPSS package, (Decoster, 1998; Hair et al., 2014) was used for CFA.

CFA tests various factors in comparison to some hypothesised model, with certain groups and relations (Cohen et al., 2011; Ellis, 2017). This implies that the CFA allows for the confirmation or rejection of some preconceived theory; it is used for the provision of confirmatory test of some measurement theory (Hair et al., 2014). One of the principal goals of CFA is to ascertain construct validity of any proposed measurement theory (Ellis, 2017; Ma & Shek, 2018). According to Gerber and Hall (2017), CFA is used to increase the validity of the research items. Confirmatory analysis tries to answer the questions that drive a research forward (Greenfield & Greener, 2016). This is normally the null hypotheses with the alternative hypotheses as discussed in section 4.12.

In this study, the researcher used both fit indices i.e., absolute and incremental. Absolute fit indices, as a measure of model goodness-of-fit, assesses how an assumed model fit the data (Hair *et al.*, 2014; Ma and Shek, 2018). They do not compare the model goodness-of-fit to any other model, but they rather evaluate the model without relying on other probable models (Hair *et al.*, 2014). There are many absolute fit indices, but in this research the Chi-Square (CMIN), the Relative Chi-square (CMIN/ DF), the Root mean squared error of approximation (RMSEA), Standardized root mean squared residual (SRMR) and PCLOSE were used. The other type of a fit index is incremental, and it analyses how well the researcher's predicted or improved model fits to some alternate baseline (Hair *et al.*, 2014; Kline, 2011). Because they make comparison to the baseline model, they are sometimes called comparative fit indices (Hooper, Coughlan and Mullen, 2008; Kline, 2011). For

incremental fit indices, the researcher used the Comparative fit index (CFI) and the Tucker-Lewis index (TLI).

Table 4.4 below summarises the various CFA fit indices measurements, description and the expected threshold as acceptable fit in the study.

Table 4.4: CFA model fit measurements, descriptions and acceptable fit of variables

Criterion	Description	Acceptable fit
Chi-Square (CMIN)	This is the original fit index for structural models and it assesses the extent of divergence between the model and close-fitting covariance matrices (Hair et al., 2014; Hooper et al., 2008; Newsom, 2018).	
Relative Chi-square (CMIN/ DF)	This is a statistical analysis that reduces the effect of the sample size on the chi-square (Hooper et al., 2008). Because of its limited statistical relevance, relative chi-square must not be over relied on for the assessment of model fit (Kline, 2011).	<3 = Good < 5 = Sometimes permissible
Root mean squared error of approximation (RMSEA)	The RMSEA gives an idea of how well the model would fit the populace covariance matrix and allows for its confidence interval to be derived around its value (Hooper et al., 2008). Using the model fit technique, a value close to zero would represent the best fit model (Kline, 2011).	≤ 0.08
Standardized root mean squared residual (SRMR)	The SRMR measures the overall difference between the observed and projected correlations (Kline, 2011). It is used to assess the overal fit of a model (Maydeu-Olivares & Garcia-Forero, 2010). A zero	≤ 0.08

	value on SRMR would represent a perfect fit model (Hooper et al., 2008).	
PCLOSE	The statistics gives the possibility of a hypothesis assessment that the population RMSEA is not greater than 0.05, indicating that the predicted moments are close to the moments in the population (Hu and Bentler, 1999).	> 0.05
Comparative fit index (CFI)	The CFI investigates the model fit through the examination of the differences between the facts and the hypothesised model, whereas also adjusting to the matters of the sample size intrinsic in the CMIN test of model fit (Hu and Bentler, 1999; Kline, 2011). Values range from 0.0 to 1.0, with values that are closer to 1.0 representing a good fit (Hooper et al., 2008; Newsom, 2018).	> 0.90
Tucker-Lewis index (TLI).	The TLI gives a comparative analysis of CMIN/df values for specified and null model (Hair et al., 2014). Due to the fact that the TLI is not normed, its value can either be below 0.0 or above 1.0, although values approaching 1.0 are considered good fit (Hair et al., 2014). Thus, a TLI value of 0.9 or more is perceived to be acceptable (Hu and Bentler, 1999).	≥ 0.90

(Sources: Hair et al., 2014; Hooper et al., 2008; Kline, 2011; Sabbagha, 2016).

Hair et al. (2014) also alludes that in a CFA, the researcher has the luxury of assessing the contribution of separate scale items and ascertaining how the scale measures well that particular concept. This was the case in this research. Factor scales were constructed for the intercorrelation of items and these showed that a common factor accounts for some relationship that exist between items (Kothari, 2012).

4.11.5 Structural equation modelling (SEM)

Structural equation modelling (SEM) is considered a hybrid of factor analysis and path analysis (Hox & Bechger, 1998; Weston, 2018). According to Raykov and Marcoulides (2000), SEM is a technique in statistics that affords researchers a comprehensive way of quantifying and testing theories. SEM fits the implied covariance matrix to the empirically deduced covariance matrix (Schermelleh-engel & Moosbrugger, 2014). The model fit will determine the degree under which SEM must fit the sample data. The CFA discussed in section 4.11.4.2 is a good example of SEM which was conducted in this study, as supported by Raykov and Marcoulides (2000). SEM allows measurement of both the direct and the indirect effects of the variable within a model (Kline, 2011). In this research, AMOS was used for conducting SEM (Kline, 2011). Weston (2018) posits that SEM gives a summary of the interrelations amongst the variables as well as testing of some hypothesised relationships amongst constructs.

In this study, SEM was applied to the three main constructs (awareness, expectations and confidence) for establishing the relationships amongst the concepts for validating the empirical model (Kline, 2011; Weston, 2018). These are discussed in section 5.4.2. The next section discusses the formulation of the hypothesis testing in this research.

4.12 RESEACH HYPOTHESES FORMULATION

A hypothesis is an "empirically testable version of a proposition or a tentative statement about a relationship" (Neuman, 2014 p.68). Kumar (2011) adds that a hypothesis is a tentative proposition, has an unknown validity and it specifies the association amongst at least two variables. Hypothesis testing is done for the confirmatory factor analysis (Ellis, 2017). The two types of research hypotheses are the null hypothesis and alternative hypothesis (often called the research hypothesis) (Saunders et al., 2016). Whilst the null hypothesis predicts the non-existence of a significant variation or relationships linking the variables, the alternative hypothesis predicts the existence of a significant difference or relationship linking the variables (Saunders et al., 2016). Therefore, hypotheses are rejected if the formulated hypothesis statements cannot be confirmed through some systematic observations and, conversely, hypotheses can be accepted if they are statistically confirmed.

The formulation of the research hypotheses was done to accomplish the empirical aims of the research and these are summarised in Table 4.5 below.

Table 4.5: Research hypotheses

Research aim	Research hypotheses		Statistical methods
Research aim 1: To develop and validate an instrument for measuring privacy awareness, expectations and confidence of students?	H ₀ 1	The nine-dimensional Information Privacy Perception Survey is not expected to measure the three privacy concepts (awareness, expectations and confidence) based on the nine-privacy concepts.	EFA (KMO, BTS and communality), factor and item analysis and Cronbach alpha
	H _a 1	The nine-dimensional Information Privacy Perception Survey is expected to measure the three privacy concepts (awareness, expectations and confidence) based on the nine-privacy concepts.	
Research aim 2: To determine the expectations of students when the university processes their personal information.	H ₀ 2	Students do not expect privacy when the university processes their personal information.	Descriptive mean values and percentages
	H _a 2	Students expect privacy when the university processes their personal information.	
Research aim 3:	H ₀ 3	Students are not aware of privacy when the university	Descriptive mean values

To determine the privacy awareness levels of students when the university processes their personal information.		is processing their personal information.	and percentages
	H _{a3}	Students are aware of privacy when the university is processing their personal information.	
Research aim 4: To determine the privacy confidence levels of students in the university observing the privacy of their personal information.	H ₀₄	Students do not have confidence in the university observing the privacy of their personal information.	Descriptive mean values and percentages
	H _{a4}	Students have confidence in the university observing the privacy of their personal information.	
Research aim 5: To determine the relationship between the 3 concepts (expectations, awareness and confidence) using correlation analysis.	H ₀₅	There are no relationships between the concepts and dimensions of the model.	Pearson product-moment correlation coefficient (PMCC)
	H _{a5}	There exist some relationships in the concepts and dimensions of the model.	
Research aim 6: To determine whether different biographical variables influence privacy awareness, expectations and confidence of students.	H ₀₆	The different biographical variables do not influence privacy awareness, expectations and confidence of students.	t-tests, ANOVA and Spearman rho
	H _{a6}	The different biographical variables influence privacy awareness, expectations and confidence of students.	

Key: H₀: Null hypothesis and H_a: Alternative hypothesis

Source: Own compilation

The next section discusses the ethical issues which were applied as the research was executed.

4.13 ETHICAL CONSIDERATIONS

As this research focused on human participants, namely students, a number of ethical considerations apply to the research. In the research, keeping the confidentiality and anonymity of participants was a prerequisite. Researchers need to protect the respondents regards their rights, ethical issues and integrity (Creswell & Creswell, 2018). Greenfield and Greener (2016) argues that before the commencement of any research, the researcher has the obligation of facilitating a cautious check on the ethical issues that can impact on participants. The ethics are categorised into four parts, namely participants' consideration, right of privacy, debriefing participants and honesty with the working colleagues (Leedy & Ormrod, 2010).

Saunders et al. (2016) suggest that the first part for research approval is getting the ethical clearance approved by the committee of research ethics. The researcher also needs to respect the needs, rights, desires and values of the respondents. Creswell and Creswell (2018) state the following safeguards as some of the ways of ensuring the protection of the respondents in a research: clearly articulate the research objectives so that the respondent understands them; the need for a written permission to go ahead with the empirical research; informing the recipient of the data collection methods, devices and activities; prioritising the respondent's rights, needs, wishes and interests when reporting the data; respecting the anonymity of the respondent. There are some ethical principles that are worth noting in "humans research" (Saunders et al., 2016) and some of them include openness, truthful, integrity and avoiding deception, misinterpretation and dishonesty especially on research findings; respect of the rights of others (participants); avoidance of harm to participants; privacy and confidentiality of the participants; ensuring that participation is purely voluntary and without any harassment; securing informed consent from those partaking in the study; ensuring and maintaining anonymity for those participating in the study and ensuring the safety of the researcher.

The following ethical aspects were applied in this research, in line with the principles stated by (Creswell & Creswell, 2018; Saunders et al., 2016):

- Two research ethics certificates were obtained for this study: a “No-Humans involved” ethical clearance (057/K/2018/CSET_SOC) for the conceptual work relating to the literature study and related conference paper and a “Humans involved” ethical clearance (030/KM/2019/CSET_SOC) for the fieldwork where the survey was conducted. The approval was obtained from the University of South Africa (UNISA)’s Research Ethics Committee. For the approval certificates, please refer to Appendix A (both A1 and A2);
- Permission was attained from the Research Board Ethics Committee Chairperson of the private university to conduct research on various campuses within Zimbabwe (Appendix B). The researcher pledged to make available a copy of the finished report to the library of the university at the time of submitting the final research findings to the institution;
- A participant information letter (for the participants of the expert panel and student pilot group) was issued with the instruments to explain the ethical considerations in the research (Appendix C). The participant information letter explained the nature of the study, the participation requirements like the activities and duration, the confidentiality, anonymity (the voluntary nature), use of information and contact information of the researcher amongst other aspects;
- Informed consent was obtained from expert panel and pilot participants using a consent form (Appendix D);
- The informed consent form for the students participating in the electronic survey was encompassed in the anonymous survey front page. There was a sentence that gave a prescription and assumption that by proceeding with the survey, the student is in consent to taking part in the research and has been told about the nature, potential benefits, procedure and anticipated inconveniences of participation;
- All respondents and participants were not by any chance exposed to any form of risk of unfamiliar stress, reduced self-esteem or embarrassment.
- The researcher assured and guaranteed that all respondents and participants remained anonymous;
- The issue of right to privacy and the confidentiality of information collected was guaranteed and a written declaration in the cover letter was drafted;
- The study was ethically conducted in harmony with the ethical obligation to report the discoveries in an honest and comprehensive way.

Ethical matters and considerations are largely to do with the permission granted to carry out the research, the respondent's participation, the public (and community) as well as the methods/techniques followed in data analysis. This was adhered to and observed in the execution of this research.

4.14 CHAPTER SUMMARY

In this chapter, the researcher started by highlighting the adoption of the positivism research philosophy, discussed the adoption of the deductive research approach and discussed the quantitative research design with the rationale for its adoption. The chapter also discussed the suitability of adopting the survey as the research strategy in this research. The university community, namely students, was the targeted population, with the sample being at least 270 students from the university under study in Zimbabwe. These were from any department. The data collection process was well articulated, with the instrument being the data collection tool. The chapter also explained the instrument development process. The necessary steps in the design of the instrument included an expert panel, pilot review and the distribution of the survey in electronic format. Validity and reliability aspects were discussed. This section achieved empirical objective number 1, as discussed and shown in section 4.10.

How the data was managed was explained and the chapter concluded by explaining various ethical issues that were observed in the accomplishment of this study. The chapter discussed the data analysis assumed in this research that comprised the descriptive statistical analysis not limited to the mean, the standard deviation and frequency as well as inferential statistical analysis like the t-test, ANOVA, correlation analysis (PPMCC) and Spearman rho. Factor analysis (both EFA and CFA) were explored. For establishing the relationships amongst the concepts and validating the empirical model, SEM was used. The next chapter discusses the research findings.

CHAPTER FIVE: RESEARCH RESULTS

5.1 INTRODUCTION

This chapter describes the empirical research findings based on the statistical results. The statistical results are reported as descriptive and inferential statistics using both exploratory and confirmatory factor analysis (EFA and CFA). Structural equation modelling was also used in terms of reporting.

The empirical objectives to be met were:

- To determine the students' expectations when the university processes their personal information;
- To determine the privacy awareness levels of students when the university processes their personal information.
- To determine the privacy confidence levels of students in the university observing the privacy of their personal information.
- To validate the instrument using factor and item analysis.
- To determine the relationship between the three concepts (expectations, awareness and confidence) using correlation analysis.
- To validate the model using structural equation modelling (SEM).
- To determine whether different biographical variables influence privacy awareness, privacy expectations and privacy confidence of students.

The results discussed in this chapter concentrate on:

- The survey results in terms of the number of responses, the age band of the respondents, their gender distribution, nationality of the respondents, their year of study and the programmes being studied by the respondents;
- Descriptive statistics per subscale reporting the means and the standard deviations;
- Instrument validation reporting the Kaiser-Meyer-Olkin (KMO) and the Bartlett's test of Sphericity (BTS), communalities, factor analysis and the Cronbach alpha analysis;

- Inferential statistics including the Pearson product moment correlation coefficient, Spearman correlation, t-tests and ANOVA.
- Structural Equation Modelling (SEM) for the validation of the model.

This is summarised in the chapter summary flowchart shown in Figure 5.1 below.

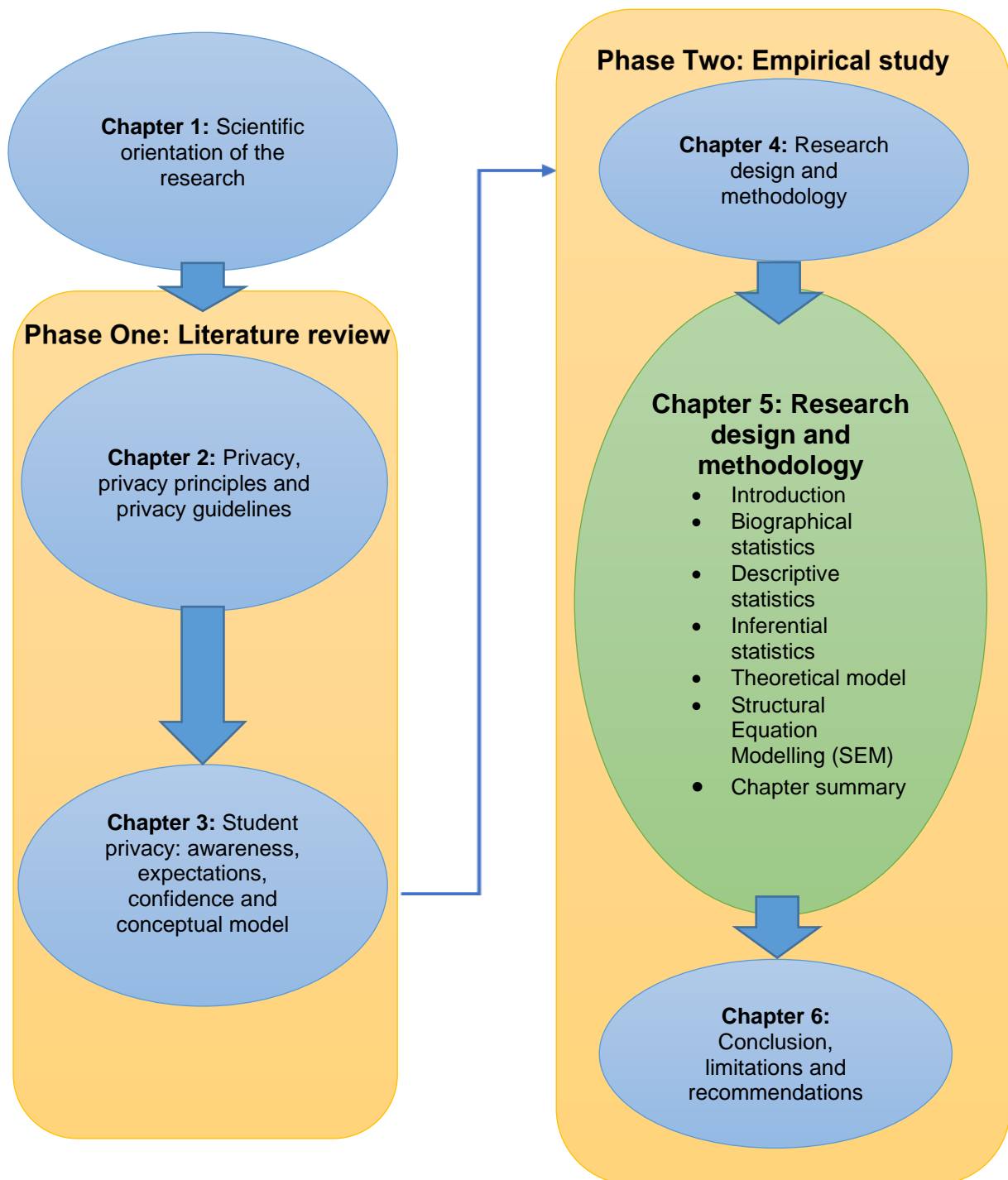


Figure 5.1: Chapter summary flowchart diagram (Source: Author's own compilation)

5.2 BIOGRAPHICAL STATISTICS

The biographical statistics of the students are presented based on the demographical questions included in the instrument, which include the ages of the respondents, their gender distribution, the nationality of the respondents, their learning mode, the year of the respondents' study and the specific programme being done by the students.

5.2.1 Survey responses

The age bands of the respondents were categorised as follows: born from 1996 to date (Generation Z or iGeneration or Centennials); born between 1977 - 1995 (Millennials or Generation Y); born between 1965 - 1976 (Generation X); born between 1946 - 1964 (Baby Boomers) and born 1945 and before (Traditionalists or Silent Generation) according to Harber (2011). The total number of respondents was 287 against a minimum target of 270 as indicated in section 4.9.4, resembling a sufficient response rate. The results are shown in Table 5.1 below.

Table 5.1: Age categories

Response	Frequency	Percent
1996 - Date	67	23.34%
1977 - 1995	177	61.67%
1965 - 1976	41	14.29%
1946 - 1964	1	0.35%
Born 1945 or earlier	1	0.35%
No response	0	0.00%

From the above table, it can be observed that most respondents were Millennials (177), representing 61.67% of the total sample. This represents the majority of the university students who are doing undergraduate studies. There were also a number of students in the Generation Z band (67), representing 23.34%. There was one student in each case for the baby boomers and the traditionalists who responded to the instrument. The assumption is, these are postgraduate students doing either the

project management short course, MSc or PhD and are always fewer than those in other programmes.

5.2.2 Gender distribution

The gender distribution of the respondents was between male or female, with any other gender being deemed “Other”. The results are shown below in Table 5.2.

Table 5.2: Gender distribution

Response	Frequency	Percentage
Male	140	48.78%
Female	143	49.83%
Other	4	1.39%
No response	0	0.00%

There were 140 male respondents, constituting 48.78% and 143 females (49.83%). Only four students indicated “Other”. This also gives a good gender parity index, which almost aligns with the Zimbabwe population distribution of 48% males and 52% females (ZIMSTAT, 2017). The "Other" category was excluded from statistical analysis due to low response rate (i.e., it only had 4 responses).

5.2.3 Nationality distribution

National distribution indicates where the respondents originate from. The research was conducted in Zimbabwe and therefore the majority of the respondents were Zimbabwean (99%). The study was also open to participants originating from other African countries, or Europe, America, Australia and Asia

Table 5.3: Nationality distribution

Response	Frequency	Percentage
Zimbabwean	284	99.0%
Another African country	3	1.0%
European	0	0.0%
American	0	0.0%
Australian	0	0.0%
Asian	0	0.0%
Other	0	0.0%
No response	0	0.0%

Three students originated from other countries. There were no students from outside Africa.

5.2.4 Mode of study distribution

The mode of study distribution shows the way students were engaged in lectures. Some attended classes during the day (conventional), others during the night and weekends (parallel), or for two weeks during school holidays (block) and any other modes of study. These options and their distribution are shown in Table 5.4 below.

Table 5.4: Mode of study distribution

Response	Frequency	Percent
Conventional	141	49.13%
Parallel	89	31.01%
Block	47	16.38%
Other	10	3.48%
No response	0	0.00%

The biggest number of respondents came from the conventional students (141) constituting 49.13%. There were also many parallel students (89), constituting 31.01%. Forty-seven students (16.38%) indicated they were in the “Block” option and

10 (3.48%) students the “Other” option. Many conventional students were present during the research orientation presentation, which was conducted during the day, hence the higher percentage of responses from this group.

5.2.5 Year of study distribution

The distribution of students in terms of the year of study was also done. Seven options (1st year, 2nd year, 3rd year, 4th year, Masters, Doctorate, six-month certificate) were given. An option for those who did not want to respond was also available as shown in Table 5.5 below.

Table 5.5: Year of study distribution

Response	Frequency	Percentage
1 st year	57	19.86%
2 nd year	81	28.22%
3 rd year	28	9.76%
4 th year	91	31.71%
Master’s	0	0.00%
Doctorate	11	3.83%
6-month certificate	19	6.62%
No response	0	0.00%

From the table above, it is clear that most of the students who responded were 4th year students, constituting 31.71%. This could be attesting to the appreciation of the concept of research by students are doing their final year of study and who are therefore also in the process of doing research. Second year students also contributed fairly, representing 28.22%, and it could be attributed to the fact that they will be doing a Research Methods module, which put more emphasis on the importance of responding to the instrument. The lowest response was from post graduate students, most probably because the institution has very few PhD and Masters students.

5.2.6 Programme distribution

The programme distribution within the institution (as described in section 4.9.4) include BBM&IT, BAcc, BBM Finance, BBM Marketing, BA Development Studies, BA Dual Honors, BA Theology, MBA, DPhil and six months courses (various). The distribution of these is shown in Table 5.6 below.

Table 5.6: Programme distribution

Response	Frequency	Percentage
BBM & IT	164	57.14%
BAcc	15	5.23%
BBM Finance	21	7.31%
BBM Marketing	16	5.57%
BA Development Studies	22	7.67%
BA Dual Honors	15	5.23%
BA Theology	2	0.70%
MBA	0	0.00%
DPhil	11	3.83%
6-month certificate	19	6.62%
Other	2	0.70%
No response	0	0.00%

From the results, 164 students from BBM & IT took part in the survey, representing 57.14%. The larger response rate by BBM & IT students can be attributed to the fact that the researcher was also a lecturer within the department, which might have influenced a high response rate. BA Development studies had 22 responses (7.67%), which was closely followed by BBM Finance responses, which had 21 (7.31%). BA Theology students did not respond to the survey.

The following section explains the various exploratory factor analysis (EFA) statistical processes which were used for the evaluation of individual items performance and further refinement of the instrument.

5.3 EXPLARATORY FACTOR ANALYSIS (EFA)

EFA is used as a reduction method to identify large numbers of items in reduced sets of new factors (Gerber and Hall, 2017). The researcher followed a set of steps before arriving at the final factors. These include checking communalities, which were used to determine the amount of variance each variable share with other variables. To ascertain the sample adequacy and significance, the Kaiser-Meyer-Olkin (KMO) and Bartlett's test of Sphericity (BTS) were used. The Cronbach alpha coefficients for the adopted dimensions were also analysed so as to determine the instrument's internal reliability. Finally, the means and the standard deviations were analysed as measured by the Information Privacy Perception Survey (IPPS) within the university context.

5.3.1 Communalities

The association of items in this study was indicated by the communalities of the data. Communalities show the stretch of association of individual items with others in the sample population (Gerber & Hall, 2017; Hair et al., 2014). Although Hair et al. (2014) prescribe that communalities must have a value of 0.5 or higher, which guarantees its return for analysis, in this study the researcher opted for 0.4 as the cut-off for the communalities (Sabbagha, 2016) and this was done after a review of the items to ensure face validity.

From the results, it is clear that no item was identified not to be associated with the underlying factors. This means that the items under study are all correlated. The values of the communalities in the study ranged between 0.441 and 0.960. From the analysis, around 65% (35 out of 54 items) of the communality values were more than 0.80, which is close to 1, showing that most of the items correlated highly with each other as posited by Gerber and Hall (2017). Only one item (*Q8: I am aware that the university should publish a privacy notice (e.g., the privacy policy on the university website or privacy terms and conditions)*) showed a slightly weak association with other items (0.441), but it was enough to fit within the selected items. The statement was kept because from the review of literature (Chua et al., 2017; Kurkovsky & Syta, 2011; Nwaeze, Zavorsky & Ruhl, 2018; OECD, 2013a) indicated that a privacy policy is fundamental in guiding the collection and use of personal information within organisations/ institutions and, as such, removing it would prove futile to privacy

advocacy. The conclusion here is that all the items are strong enough to associate completely with each other and therefore none of them should be reconsidered. The communalities for this research are shown in Appendix F.

5.3.2 Sample adequacy and sphericity

To test for sample adequacy and Sphericity, the Kaiser-Meyer-Olkin (KMO) and Bartlett’s test of Sphericity (BTS) are used respectively. According to Cohen, Manion and Morrison (2007), the KMO is a statistical technique that is used to measure sample adequacy. The KMO values range from 0 to 1, and the recommended threshold value of KMO that signifies a strong correlation structure for an EFA (where one should proceed with EFA) is 0.5 or more (Gerber & Hall, 2017; Gie & Pearce, 2012; Riley-Tillman & Reinke, 2011). On the other hand, the BTS is used to ascertain the existence of correlations and the significance amongst the variables and it is considered significant when $p < 0.05$ (Cohen et al., 2007; Gie & Pearce, 2012). Table 5.7 below depicts the KMO and BTS values for this research.

Table 5.7: Sample adequacy and significance

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling		0.647
Bartlett's Test of Sphericity	Approx. Chi-Square	231.517
	df	6
	Sig.	0.000

The KMO with the value of 0.647 is above the threshold value (0.50) and is considered sufficient (Gerber & Hall, 2017; O’Rourke & Hatcher, 2013), which signifies the presence of a strong correlation structure, permitting the researcher to proceed with EFA. Large scores of KMO values demonstrate that the factor analysis clearly extracts reliable and separable factors and that there is a relatively compact correlation pattern. Furthermore, the BTS was 0.00 for overall significance, showing strong significance for the conduct of EFA. Such a value shows that a proper and meaningful factor analysis was properly conducted as confirmed by Hair et al. (2014).

To determine the total number of factors to retain for rotation in the Eigenvalues, the criteria used were:

- Checking and interpreting the Scree plot;
- The cumulative percentage explained by factors with more than 60%, and
- The Eigenvalues to be greater than one.

The scree plot was useful in determining the factors that must be encompassed in the measurement; it calculates the number of valid factors by plotting Eigenvalues in a graph (Hair et al., 2014). It identifies the amount of components/factors to be extracted before the total of unique variables starts dictating the common variance structure (Hair et al., 2014). The scree plot for this study starts levelling out after the eighth eigenvalue, which explains a variance cumulative percentage of 60.750% of the total variance (shown in Figure 5.2 and Table 5.8). This represents the variance in the original 54 items which was perceived to be good enough because according to Hair et al. (2014), a threshold of 60% of the total variance is considered satisfactory.

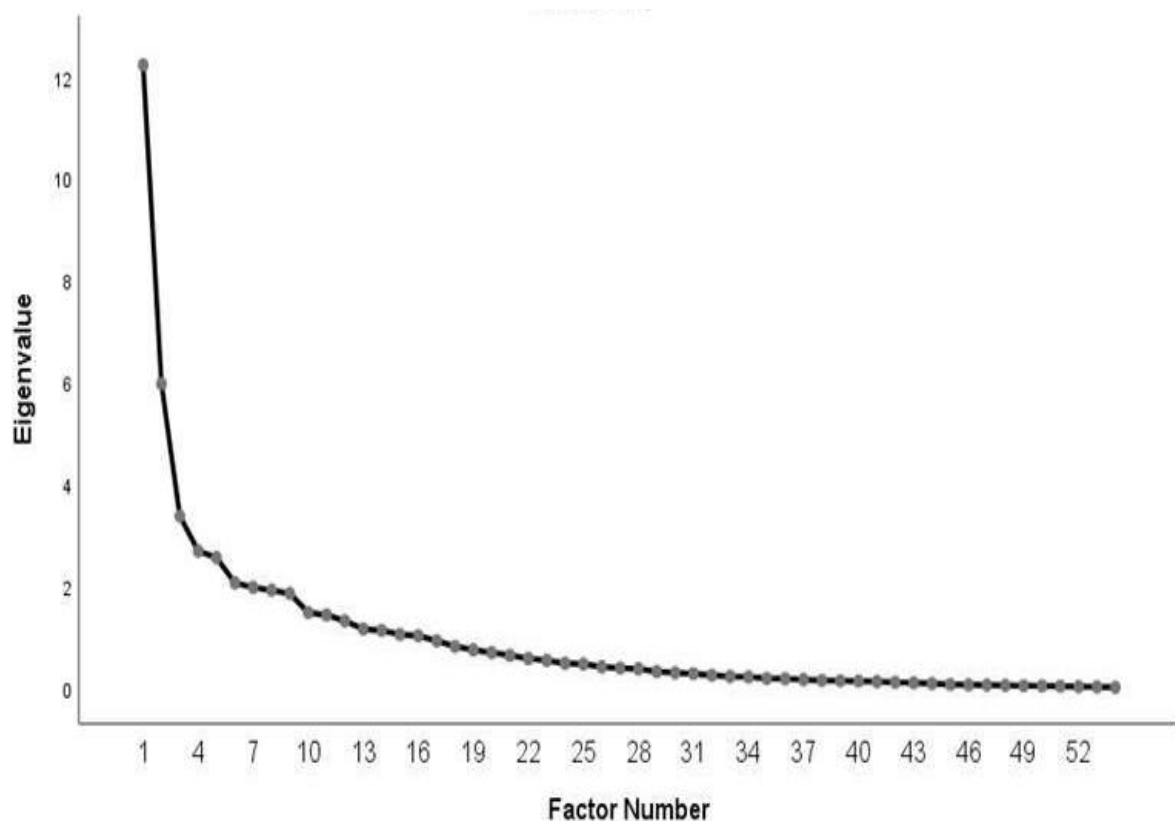


Figure 5.2: Scree plot graph

Table 5.8 below outlines the total variances with the Eigenvalues.

Table 5.8: Total variance with Eigenvalues

Total Variance Explained				
Factor	Initial Eigenvalues			Rotation Sums of Squared Loadings^a
	Total	% of Variance	Cumulative %	Total
1	12.227	22.644	22.644	7.922
2	5.973	11.061	33.704	4.248
3	3.377	6.254	39.959	5.174
4	2.693	4.986	44.945	4.564
5	2.564	4.748	49.693	2.645
6	2.067	3.828	53.521	3.132
7	1.980	3.666	57.188	6.988
8	1.924	3.562	60.750	4.596
9	1.858	3.441	64.190	3.339
10	1.486	2.751	66.942	
11	1.438	2.664	69.605	
12	1.322	2.448	72.053	
13	1.163	2.153	74.206	
14	1.135	2.102	76.309	
15	1.054	1.952	78.261	
16	1.031	1.910	80.171	
17	0.931	1.725	81.896	
18	0.823	1.525	83.420	
19	0.755	1.398	84.819	
20	0.699	1.295	86.114	
21	0.647	1.198	87.312	
22	0.583	1.080	88.391	
23	0.548	1.015	89.406	
24	0.488	0.903	90.309	
25	0.475	0.880	91.190	
26	0.422	0.781	91.971	

Factor	Total	% of Variance	Cumulative %	Total
27	0.396	0.733	92.703	
28	0.382	0.707	93.410	
29	0.329	0.609	94.019	
30	0.305	0.565	94.585	
31	0.286	0.529	95.114	
32	0.255	0.473	95.587	
33	0.232	0.429	96.016	
34	0.223	0.413	96.429	
35	0.194	0.359	96.788	
36	0.188	0.348	97.135	
37	0.171	0.317	97.452	
38	0.155	0.287	97.739	
39	0.148	0.273	98.012	
40	0.142	0.263	98.275	
41	0.131	0.242	98.517	
42	0.118	0.219	98.736	
43	0.107	0.199	98.936	
44	0.093	0.172	99.108	
45	0.076	0.141	99.249	
46	0.066	0.123	99.372	
47	0.063	0.117	99.489	
48	0.057	0.106	99.595	
49	0.050	0.092	99.687	
50	0.048	0.089	99.775	
51	0.042	0.077	99.852	
52	0.031	0.057	99.910	
53	0.029	0.053	99.963	
54	0.020	0.037	100.000	

Extraction Method: Principal Axis Factoring.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

The responses to 54 items were correlated, extracted using the Principal Axis Factoring and rotated by using Oblimin with Kaiser Normalisation. The table shows 60.725% of the variance for the first eight factors.

5.3.3 Determining the internal consistency of scale

The 54-item instrument rotated pattern matrix is depicted in Table 5.9 below.

Table 5.9: Rotated pattern matrix for the 8-factor model

Pattern Matrix ^a all items 8 factors								
Item Number	Factor							
	1	2	3	4	5	6	7	8
q30	0.772							
q19	0.764							
q18	0.733							
q24	0.622							
q31	0.618							
q13	0.603							
q25	0.601							
q12	0.563							
q10								
q28		0.631						
q29		0.598						
q46		0.586						
q47		0.583						
q34		0.539						
q58		0.437						
q11		0.417						
q9								
q35								
q56			-0.892					
q57			-0.868					
q27			-0.463					

Item Number	1	2	3	4	5	6	7	8
q38			-0.445					
q39			-0.441					
q33								
q8								
q20				-0.796				
q21				-0.677				
q26				-0.472				
q59			-0.400	0.466				
q32								
q51					0.703			
q50					0.700			
q52					0.575			
q53					0.561			
q37.								
q41		0.458				0.612		
q40						0.561		
q36						0.404		
q61							-0.836	
q54							-0.805	
q60							-0.804	
q55							-0.740	
q43							-0.647	
q49							-0.576	
q48							-0.544	
q42							-0.526	
q16								-0.753
q22								-0.630
q17								-0.575
q14								-0.532
q23								-0.478
q45								-0.451
q44								

q15								
Extraction Method: Principal Axis Factoring.								
Rotation Method: Oblimin with Kaiser Normalization.								
a. Rotation converged in 25 iterations.								

From Table 5.9, there are two cases of cross-loadings. These are found in items 59 and 41. In factor analysis, if the difference between the items with cross loadings (with loading on the two factors) is less than 0.20, then the items should be eliminated (Hair et al., 2014). Items that have factor loadings less than the prescribed and agreed threshold of ≤ 0.40 (Hair et al., 2014) and also those with higher cross loadings (usually with < 0.20 difference) within a single factor should be eliminated. Consequently, items 59 and 41 were excluded from the final factor analysis as the difference was less than 0.20. After exclusion due to cross-loadings, factor 6 remained with 2 items and was therefore excluded because the adopted criterion was to group at least three items per factor. Therefore, factor 6 was eliminated from the final rotated matrix in the eight-factor model. The items in Table 5.9 were grouped accordingly and this resulted in seven valid factors.

5.3.4 Adoption of new factors

Using the criteria directed by Hair et al. (2014), items 8, 9, 10, 15, 32, 33, 35, 37 and 44 had very low factor loadings (< 0.4) and therefore were also not included in the final eight-factor model rotated pattern matrix. Their loadings were excluded from the table by SPSS software. SPSS was configured in such a way that all factor loadings that were less than 0.4 were not considered from the output, leaving the blanks representing low loadings. The 0.4 represents an absolute value without considering the sign (either positive or negative).

5.3.4.1 Final factors

After successfully combining the factors, a summarised rotated pattern for the eight-factors is shown in Appendix G.

Eight items were loaded in factor 1 (items 30, 19, 18, 24, 31, 13, 25 and 12), seven items in factor 2 (Items 28, 29, 46, 47, 34, 58 and 11), five in factor 3 (items 56, 57, 27, 38 and 39), three in factor 4 (items 20, 21 and 26), four in factor 5 (items 51, 50,

52 and 53), eight in factor 7 (items 61, 54, 60, 55, 43, 49, 48 and 42) and six items loaded in factor 8 (items 16, 22, 17, 14, 23 and 45). The factors were then labelled by considering the items in the corresponding factors.

Factor 1

The eight factors loaded positively in factor 1. The items were all designed to measure various students' confidence levels with the university, producing an atmosphere that nurtures the upholding of personal information privacy.

Factor 2

Although eight items loaded in factor 2, only seven loaded successfully. The factors also loaded positively. The factor focused on student expectations on use limitation, consent, collection limitation, notice/ openness and privacy policy privacy components.

Factor 3

Five factors loaded successfully in factor 3. The sign before the loading (either negative or positive) must be ignored (Gerber & Hall, 2017). The factor had much emphasis on the awareness of students with regards to consent, individual participation and use limitation privacy components.

Factor 4

Four items loaded in factor 4 although only three were considered. The factor is described as external because the items that constitute the factor focus on what the university has to do in instilling awareness for purpose specification and use limitation of students' personal information.

Factor 5

All four items in factor 5 loaded successfully. The items emphasised the expectations and awareness of privacy education within universities as part of best practices.

Factor 7

Eight items loaded successfully in factor 7. The factor focused on positive student confidence in consent, individual participation, privacy education and privacy policy components.

Factor 8

The last component (factor 8) had six items successfully loading. The factor focused on the expectations and awareness of students in terms of information quality, purpose specification, and privacy policy components.

In summary, a total of 41 items were retained after the EFA process.

5.3.5 Reliability of the instrument

Based on the discussion in section 4.11.4, the Cronbach alpha measures a scale's internal consistency (Hair et al., 2014; Kothari, 2012). The new components' Cronbach alpha values and their mean inter-item correlation were calculated and are shown in Table 5.10 below. The new factors are university confidence (UC) for factor 1, privacy expectations (PE) for factor 2, individual awareness (IA) for factor 3, external awareness (EA) for factor 4, privacy awareness (PA) for factor 5, practice confidence (PC) for factor 7 and correctness expectations (CE) for factor 8.

The Cronbach alpha value for factor 6 gave a loading of 0.225, which was very low. According to Hair *et al.* (2014) and Gerber and Hall (2017), the value of the Cronbach alpha coefficient must be at least 0.7 (Cronbach value ≥ 0.7) to enable the conduct of an EFA. This was also supported by the presence of cross loadings of <0.20 as discussed in section 5.3.3. Therefore, factor 6 was removed. The final seven factors with their Cronbach alpha values and mean inter-item correlation are all revealed in Table 5.10 below.

Table 5.10: Cronbach alpha values and inter-item correlations per factor

Factor/ Dimension	Number of Items	Cronbach alpha	Mean inter-item correlation
University confidence (UC)	8	0.922	0.596
Privacy expectations (PE)	7	0.789	0.326
Individual awareness (IA)	5	0.820	0.485
External awareness (EA)	3	0.807	0.589
Privacy education (PEd)	4	0.737	0.418
Practice confidence (PC)	8	0.917	0.589
Correctness expectations (CE)	6	0.781	0.383
Total	41		

From the table above, it is shown that the seven Cronbach alpha values recorded were greater than 0.7, indicating a strong and solid item covariance (Gerber & Hall, 2017; Saunders et al., 2016). In fact, they were between the range 0.7 and 0.9, signifying that the values were adequate as posited by (Creswell & Creswell, 2018). As a result, the Cronbach alpha values were considered appropriate and acceptable for the objective of this research. Therefore, a reliable measure of the student perceptions on privacy. For newly developed instruments, even a value of 0.60 for the Cronbach alpha values is deemed appropriate and acceptable (Banerjee, 2015). The seven factors considered constituted a reduction in the number of factors.

In contra, the mean inter-item correlation measures the consistency scores in one item being correlated to the other items' scores within the scale. The threshold for the inter-item correlation for an item set must be in-between 0.20 and 0.40 (Pallant, 2011). Furthermore, if the mean inter-item correlation value is 0.20 or lower, the implication is that the items do not represent similarly the content domain and thus, they are discarded. Pallant (2011) also notes that if the mean inter-item correlation value is greater than 0.4, they are believed to only grasp a minute bandwidth of the component. The mean inter-item correlation values for privacy expectations (0.326) and correctness expectations (0.383) privacy components fell within the prescribed threshold, that is between 0.20 and 0.40. University confidence (0.596), individual awareness (0.485), external awareness (0.589), privacy awareness (0.418) and practice confidence (0.589) were above the suggested threshold of 0.4, indicating that

the items could have seized a miniature bandwidth of the component construct. These figures were deemed acceptable.

5.3.6 Means and standard deviations of the factors' interpretation

Considering the value of information security and privacy, a cut-off point of 4.0 was deemed acceptable in this research (Da Veiga & Martins, 2014). Potentially positive and negative perceptions on privacy of student personal information were decided based on the 4.0 cut-off score. The implication of this is that any score that is above 4.0 indicates a positive perception in terms of awareness, expectations of students on the privacy of their personal information whereas any mean score lower than 4.0 (except the neutral score of 3.0) indicates a negative perception of the measured dimensions.

All the factors had a maximum of 5.00 since the Likert scale had a maximum of 5 responses [Strongly disagree (1), Disagree (2), Do not disagree or agree (3), Agree (4) and Strongly agree (5)]. The descriptive statistics shown in Table 5.11 are the mean and the standard deviation values for the reduced seven factors.

Table 5.11: Descriptive statistics

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
University confidence	287	1.25	5.00	3.5740	.90282
Privacy expectations	287	2.86	5.00	4.5610	.41050
Individual awareness	287	1.80	5.00	4.0774	.75485
External awareness	287	1.67	5.00	4.1429	.77054
Privacy education	287	1.75	5.00	4.1254	.73406
Practice confidence	287	1.63	5.00	3.4194	.88332
Correction expectation	287	2.33	5.00	4.5296	.45205
Valid N (listwise)	287				

The mean scores for five factors are above the 4.0 cut-off value (Da Veiga & Martins, 2014). These were privacy expectations (mean = 4.56), individual awareness (mean = 4.07), external awareness (mean = 4.14), privacy awareness (mean = 4.13) and

correction expectation (mean = 4.53). The factors that failed to meet the minimum ut-off point were university confidence (mean = 3.57) and practice confidence (mean = 3.42). The summarised bar graph for the factors' mean values is shown in Figure 5.3 below.

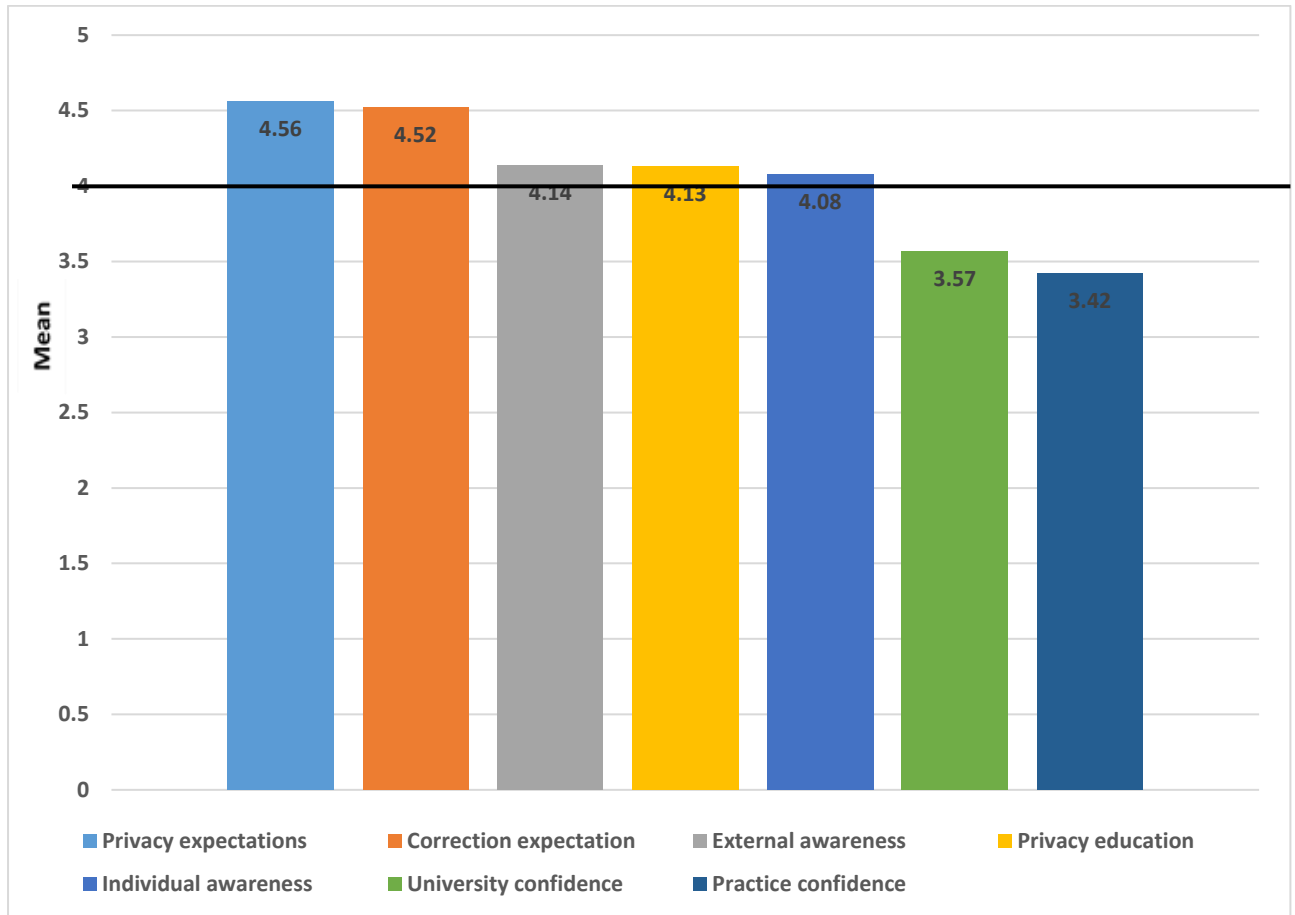


Figure 5.3: Mean values for the factors

From the above figure, it can be drawn that:

- A 4.56 mean value was recorded for factor 2 (privacy expectations), which is greater than the prescribed 4.0 cut-off value (Da Veiga & Martins, 2014). This signifies positive perceptions by students on how the university handles and uses their personal information. Students had positive perceptions and expectations on use limitation, consent, collection limitation and notice/openness and privacy policy privacy components.
- A 4.53 mean value was recorded for factor 8 (correction expectation), which was also regarded as highly positive with respect to students' perceptions, about student expectations on the university on how the it should develop

privacy policies as well as notices that can be easily understandable, that the university will only use student personal information for genuine reasons like the legal requirements, which must be done with the consent of the student.

- A 4.14 mean value was recorded for factor 4 (external awareness). This also signifies positive perceptions. It also gives students' awareness levels perceptions with regards to the limitations of information use and in specifying the purpose of collection.
- A mean value of 4.13 was recorded for factor 5 (privacy education), and this is also higher than the cut-off. This also showed positive perceptions by students on the expectations and awareness of privacy education within universities.
- A mean value of 4.08 reflected in factor 5 (individual awareness), giving relatively positive perceptions by students on awareness with regards to consent, individual participation and use limitation components.
- Factor 1 (university confidence) recorded a mean value of 3.57, which was below the cut-off value. This represents negative perceptions by students, meaning that they were not confident with the how the university implemented privacy practices especially in fostering an environment that is conducive for upholding their personal information privacy.
- The lowest mean value in this study of 3.43 was recorded in factor 7 (practice confidence). This reflects on the dimension which is lower than the cut-off value. It means that students do not have confidence in the university practices in terms of consent, individual participation, privacy education and privacy policy components. This represents an area of improvement that the university has to focus on in addressing privacy practises that increase student confidence.

The seven factors were subjected to inferential statistics to further derive more useful information from the data.

5.4 INFERENCE STATISTICS

The following section discusses the results of the CFA, SEM, PPME, t-test, ANOVA and the Spearman rho.

5.4.1 Confirmatory factor analysis (CFA)

After the successful conduct of EFA, the data reported reliable and valid factors that could also be tested for confirmatory factor analysis (CFA). The CFA was conducted to test the overall measurement model.

i. Reporting on CFA for university confidence

The first factor that loaded in the previous EFA was university confidence. This is presented in Figure 5.4 below, followed by the statistics for model fit in Table 5.12.

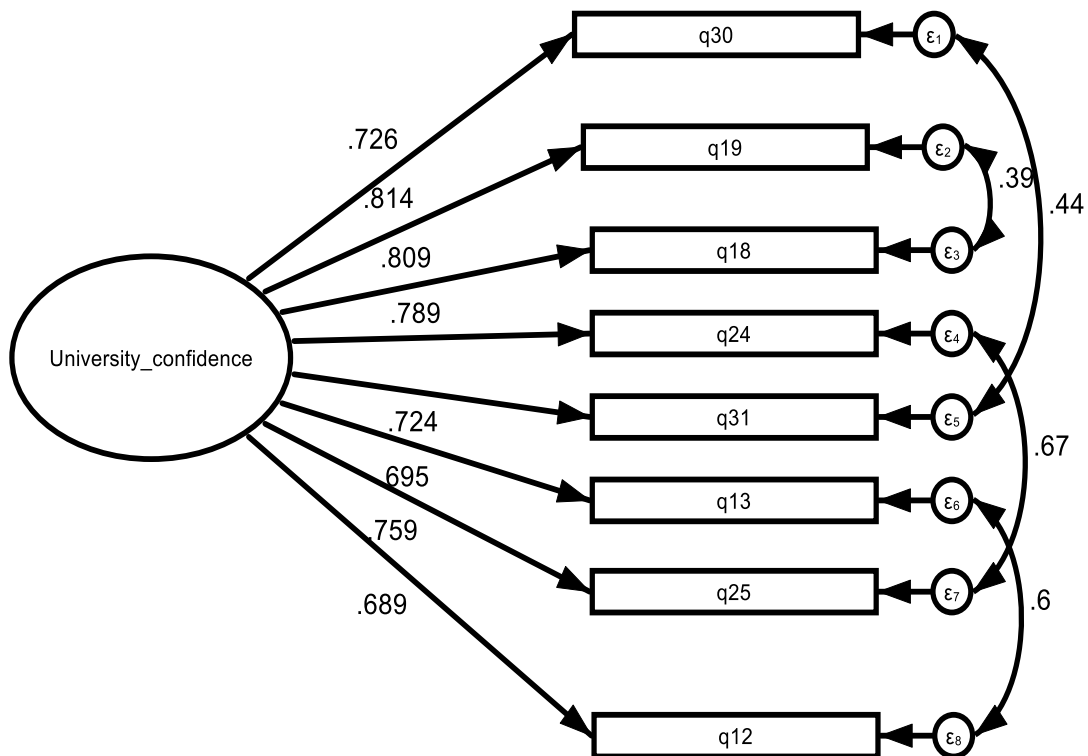


Figure 5.4: Model fit for university confidence

Note: Direct causal relationship = \longrightarrow Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \bigcirc e

The corresponding model fit statistics for the university confidence factor are shown in Table 5.12.

Table 5.12: Model fit indices for university confidence

Fit Index	Obtained value	Prescribed threshold	Meeting criteria Yes/ No
Absolute fit indices			
Chi-Square (CMIN)	57.69		
Degree of Freedom (DF)	16		
Relative Chi-square (CMIN/ DF)	3.61	<3 = Good <5 = Sometimes permissible	Yes
Root mean squared error of approximation (RMSEA)	0.095	≤ 0.08	No
Standardized root mean squared residual (SRMR)	0.026	≤ 0.08	Yes
PCLOSE	0.003	> 0.05	No
Relative/incremental fit indices			
Comparative fit index (CFI)	0.977	> 0.90	Yes
Tucker-Lewis index (TLI)	0.959	≥ 0.90	Yes

A summarised overview of the statistical fit analysis for the university confidence model in Table 5.12 above was done using the following fit indices:

- The model had a CMIN value of 57.69 with 16 degrees of freedom, giving a CMIN/df of 3.61, which according to Hooper et al. (2008) is permissible and acceptable for model fit.
- The RMSEA value of 0.095 was obtained and does not meet the minimum acceptable fit of $RMSEA \leq 0.08$.
- A SRMR value of 0.026 was obtained, which is within the prescribed cut-off of ≤ 0.08 . This is within the acceptable levels of goodness of fit.

- PCLOSE of 0.003, less than the threshold value of $p > 0.05$, was obtained, which does not meet the minimum criteria.
- The value of CFI obtained was 0.977, which was above the threshold value of more than 0.90 and it is therefore an acceptable fit.
- The TLI of 0.977 is above the model fit requirement of ≥ 0.9 , which is acceptable.

The model has two absolute indices that were within the prescribed threshold (CMIN/df and SRMR). The tested relative/ incremental fit indices for this research (CFI and TLI) were above the minimum threshold. Therefore, using criteria that a model can be accepted if it has an absolute fit index (at least one) and an incremental fit index (at least one) (Hair et al., 2014; Hooper et al., 2008), the model was deemed acceptable.

ii. Reporting on CFA for privacy expectations

The second factor to load was privacy expectations. This is shown in Figure 5.5 below, followed by the statistics for model fit in Table 5.5.

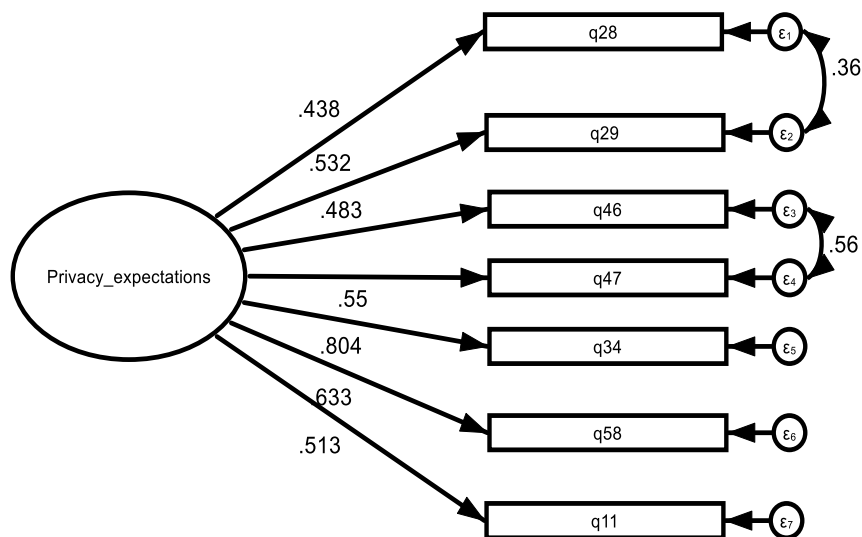


Figure 5.5: Model fit for privacy expectations

Note: Direct causal relationship = \longrightarrow Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \bigcirc e

The corresponding model fit statistics for the privacy expectations factor are shown in Table 5.13 below.

Table 5.13: Model fit indices for privacy expectations

Fit Index	Obtained value	Prescribed threshold	Meeting criteria Yes/ No
Absolute fit indices			
Chi-Square (CMIN)	28.57		
Degree of freedom (DF)	12		
Relative Chi-square (CMIN/DF) CMIN/DF	2.38	<3 = Good <5 = Sometimes permissible	Yes
Root mean squared error of approximation (RMSEA)	0.037	≤ 0.08	Yes
Standardized root mean squared residual (SRMR)	0.042	≤ 0.08	Yes
PCLOSE	0.148	> 0.05	Yes
Relative/incremental fit indices			
Comparative fit index (CFI)	0.971	> 0.90	Yes
Tucker-Lewis index (TLI)	0.949	≥ 0.90	Yes

A summarised overview of the statistical fit analysis for the privacy expectations model in Table 5.13 above was done using the following fit indices:

- The model had a CMIN value of 28.57 with 12 degrees of freedom, giving a CMIN/df of 2.38, which according to Hooper et al. (2008) is good and acceptable for model fit.
- The RMSEA value of 0.037 was obtained, which is lower than the minimum acceptable fit of $RMSEA \leq 0.08$, thus an acceptable fit.
- A SRMR value of 0.042 was obtained, which is within the prescribed cut-off of ≤ 0.08 . This is within the prescribed and acceptable ranges of goodness of fit.
- PCLOSE of 0.148, higher than the threshold value of $p > 0.05$, which is a good and an acceptable fit.

- The value of CFI obtained was 0.971, which is above the threshold value of more than 0.90 and it is an acceptable fit.
- The TLI of 0.949 is above the model fit requirement of ≥ 0.9 , which is acceptable.

The model satisfied all the fit indices tested for privacy expectations i.e., CMIN/df, RMSEA, SRMR, PCLOSE, CFI and TLI, meaning that the model is deemed acceptable.

iii. Reporting on CFA for individual awareness

The other factor to load was individual awareness. This is presented in Figure 5.6 below, followed by the statistics for model fit in Table 5.14.

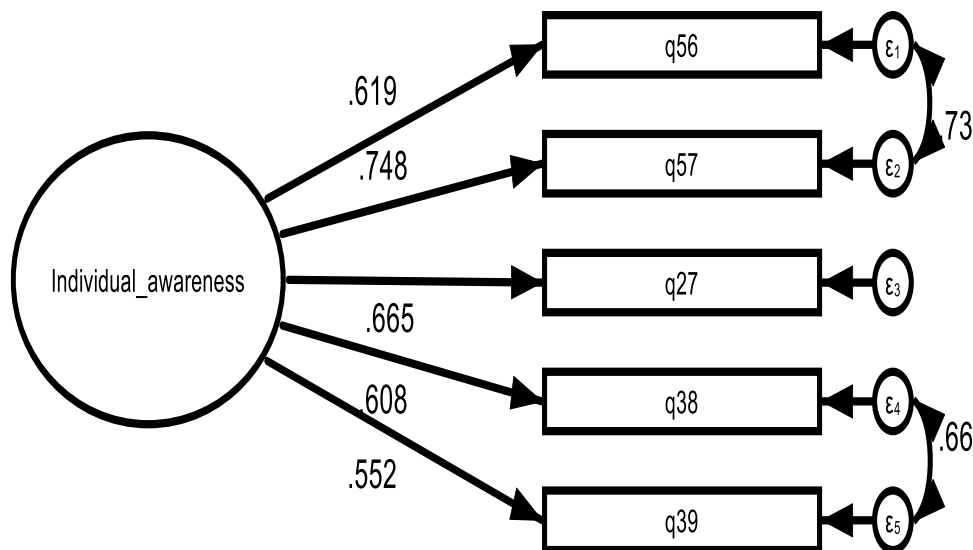


Figure 5.6: Model fit for individual awareness

Note: Direct causal relationship = \longrightarrow , Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \bigcirc e

The corresponding statistics for model fit for the individual awareness factor are shown in Table 5.14 below.

Table 5.14: Model fit indices for individual awareness

Fit Index	Obtained value	Prescribed threshold	Meeting criteria Yes/ No
Absolute fit indices			
Chi-Square (CMIN)	7.99		
Degree of freedom (df)	3		
Relative Chi-square (CMIN/DF)	2.66	<3 = Good <5 = Sometimes permissible	Yes
Root mean squared error of approximation (RMSEA)	0.076	≤ 0.08	Yes
Standardized root mean squared residual (SRMR)	0.019	≤ 0.08	Yes
PCLOSE	0.195	> 0.05	Yes
Relative/incremental fit indices			
Comparative fit index (CFI)	0.994	> 0.90	Yes
Tucker-Lewis index (TLI)	0.979	≥ 0.90	Yes

A summarised overview of the statistical fit analysis for the individual awareness model in Table 5.14 above was done using the following fit indices:

- The model had a CMIN value of 7.99 with 3 degrees of freedom, giving a CMIN/df of 2.66, which according to Hooper et al. (2008) is good and acceptable for model fit.
- A RMSEA value of 0.076 was obtained and this falls within the minimum acceptable fit of $RMSEA \leq 0.08$.
- A SRMR value of 0.019 was obtained, which is within the prescribed cut-off of ≤ 0.08 . This is within the satisfactory levels of goodness of fit.
- PCLOSE of 0.195, higher than the threshold value of $p > 0.05$, was obtained, which is a good and an acceptable fit.
- The value of CFI obtained was 0.994, which is above the threshold value of more than 0.90 and which is a satisfactory fit.

- The TLI of 0.979 is above the model fit requirement of ≥ 0.9 , which is acceptable.

The model satisfied all the fit indices tested for individual awareness, namely CMIN/df, RMSEA, SRMR, PCLOSE, CFI and TLI. This means that the model is deemed acceptable.

iv. Reporting on CFA for practice confidence

The other factor to load was practice confidence. This is presented in Figure 5.7 below, followed by the statistics for model fit in Table 5.15.

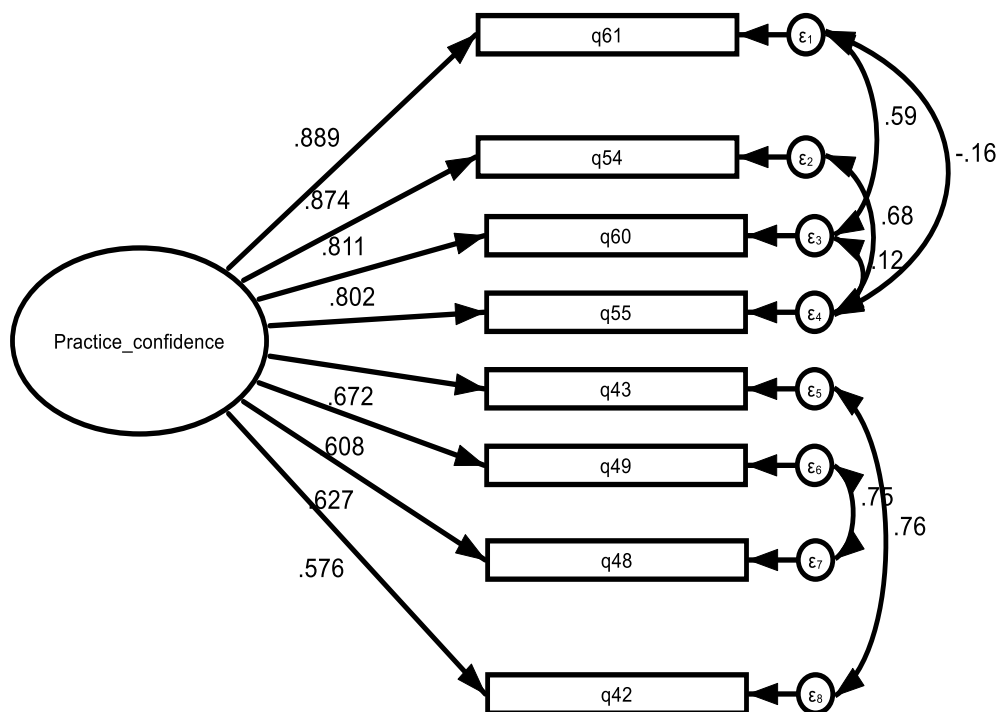


Figure 5.7 Model fit for practice confidence

Note: Direct causal relationship = \longrightarrow Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \textcircled{e}

The corresponding model fit statistics for the practice confidence factor are shown in Table 5.15 below.

Table 5.15: Model fit indices for practice confidence

Fit Index	Obtained value	Prescribed threshold	Meeting criteria Yes/ No
Absolute fit indices			
Chi-Square (CMIN)	114.22		
Degree of freedom (df)	13		
Relative Chi-square (CMIN/DF)	8.16	<3 = Good <5 = Sometimes permissible	No
Standardized root mean squared residual (SRMR)	0.052	≤ 0.08	Yes
Root mean squared error of approximation (RMSEA)	0.158	≤ 0.08	No
PCLOSE	0.000	> 0.05	No
Relative/incremental fit indices			
Comparative fit index (CFI)	0.957	> 0.90	Yes
Tucker-Lewis index (TLI)	0.913	≥ 0.90	Yes

A summarised overview of the statistical fit analysis for the practice confidence model in Table 5.15 above was done using the following fit indices:

- The model had a CMIN value of 114.22 with 13 degrees of freedom, giving a CMIN/df of 8.16, which according to Hooper et al. (2008) is not acceptable for model fit.
- A SRMR value of 0.052 was obtained, which is within the prescribed cut-off of ≤ 0.08. This is within the acceptable levels of goodness of fit.
- A RMSEA value of 0.158 was obtained and does not meet the minimum threshold of RMSEA ≤ 0.08, which is not acceptable.
- PCLOSE of 0.000, less than the threshold value of p > 0.05, was obtained. This is not good.
- The value of CFI obtained was 0.957, which was above the threshold value of > 0.90 and it is acceptable.
- The TLI of 0.913 is above the model fit requirement of ≥ 0.9 which is acceptable.

Although the CMIN/df, RMSEA and PCLOSE values were outside the acceptable threshold range, the practice confidence model was accepted based on the criteria proposed by Hair et al. (2014) and Hooper et al. (2008) for SRMR, CFI and TLI fit values.

v. *Reporting on CFA for correction expectation*

The other factor to load was correction expectation. This is presented in Figure 5.8 below, followed by the statistics for model fit in Table 5.16.

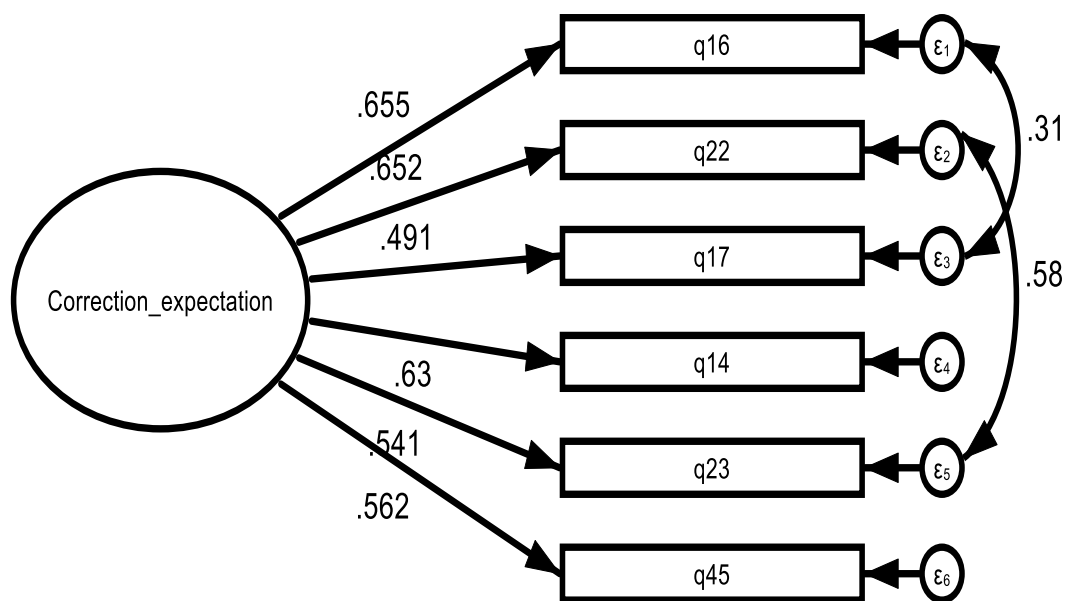


Figure 5.8 Model fit for correction expectation

Note: Direct causal relationship = \longrightarrow Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \textcircled{e}

The corresponding model fit statistics for the correction expectation factor are shown in Table 5.16 below.

Table 5.16: Model fit indices for correction expectation

Fit Index	Obtained value	Prescribed threshold	Acceptable fit Yes/ No
Absolute fit indices			
Chi-Square (CMIN)	13.40		
Degree of freedom (df)	7		
Relative Chi-square (CMIN/DF)	1.91	<3 = Good <5 = Sometimes permissible	Yes
Root mean squared error of approximation (RMSEA)	0.056	≤ 0.08	Yes
Standardized root mean squared residual (SRMR)	0.031	≤ 0.08	Yes
PCLOSE	0.354	> 0.05	Yes
Relative/incremental fit indices			
Comparative fit index (CFI)	0.988	> 0.90	Yes
Tucker-Lewis index (TLI)	0.974	≥ 0.90	Yes

A summarised overview of the statistical fit analysis for the correction expectation model in Table 5.16 above was done using the following fit indices:

- The model had a CMIN value of 13.40 with 7 degrees of freedom, giving a CMIN/df of 1.91, which according to Hooper et al. (2008) is good and acceptable for model fit.
- PCLOSE of 0.354, higher than the threshold value of $p > 0.05$, was obtained. This is a good and an acceptable fit.
- A RMSEA value of 0.056 was obtained and it meets the minimum acceptable fit of $RMSEA \leq 0.08$.
- A SRMR value of 0.031 was obtained, which is within the prescribed cut-off of ≤ 0.08 . This is within the acceptable levels of goodness of fit.
- The value of CFI obtained was 0.988, which is above the threshold value of more than 0.90 and it is a satisfactory fit.

- The TLI of 0.974 is above the model fit requirement of ≥ 0.9 , which is acceptable.

The model satisfied all the fit indices tested for correction expectation, namely CMIN/df, RMSEA, SRMR, PCLOSE, CFI and TLI. This means that the model is deemed acceptable.

vi. Reporting on external awareness

The external awareness factor is shown in Figure 5.9 below.

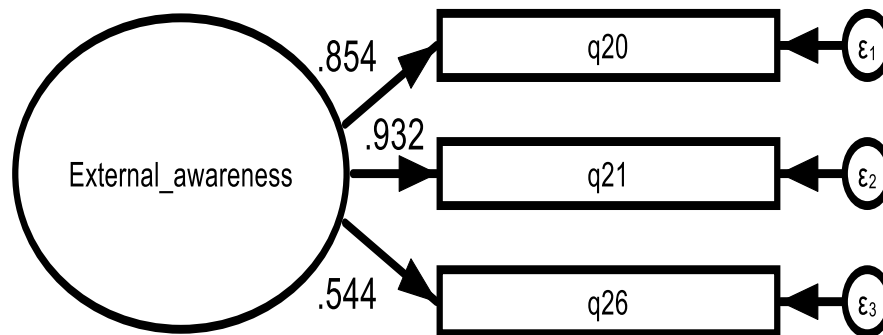


Figure 5.9 Model fit for external awareness

Note: Direct causal relationship = \longrightarrow , Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \textcircled{e}

There were too few degrees of freedom and the fit could not be estimated. Therefore, the model was not estimated. The relationships were further tested in SEM analysis.

vii. Reporting on privacy education

The last privacy education factor is shown in Figure 5.10 below.

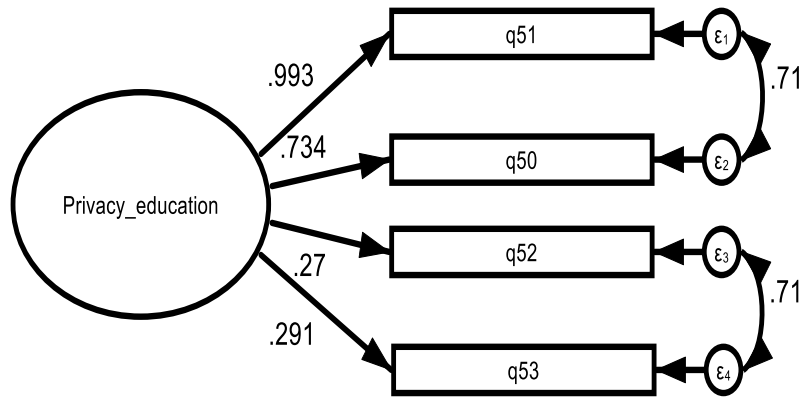


Figure 5.10: Model fit for privacy education

Note: Direct causal relationship = \longrightarrow Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \textcircled{e}

Just like the external awareness factor, there were also too few degrees of freedom and the fit could not be estimated; therefore, the model was also not estimated. There were also very low coefficients for q52 and q53. The relationships were further tested in SEM analysis.

The summarised information privacy perception model fit indices are presented in Table 5.17 below.

Table 5.17: Summary of information privacy perception model fit indices

Factor	Chi-square p>0.05	CFI >0.90	TLI ≥0.90	RMSEA <0.06	SRMR <0.08
University confidence	0.000	0.977	0.959	0.095	0.026
Privacy expectations	0.005	0.971	0.949	0.037	0.043
Individual awareness	0.046	0.994	0.979	0.076	0.019
External awareness	Too few degrees of freedom - model was not estimated				
Privacy Education	Too few degrees of freedom - model was not estimated				
Practice confidence	0.000	0.957	0.913	0.158	0.052
Correction expectation	0.063	0.988	0.974	0.056	0.031

In conducting the CFA, four of the seven factors (privacy expectations, university confidence, individual awareness and correction expectation) had fit indices that were acceptable. For practice confidence, the RMSEA was not within acceptable limits but the SRMR CFI and TLI were, rendering it acceptable. Unfortunately, there were not any modifications to the model which could improve the fit. For the other two factors without any fit indices (external awareness and privacy education), the degrees of freedom were too small to compute a fit index. The model can thus be estimated, but the fit cannot be determined. It was thus decided to continue with the model estimates, which are discussed in the following section.

5.4.2 Structural equation modelling (SEM)

The SEM confirmed the inclusion of three main concepts, namely expectations, awareness and confidence. Extracted factors from the factor analysis were also confirmed as privacy expectations, correction expectations, privacy education, individual awareness, external awareness, university confidence and practice confidence. The assumed relationships between the three main concepts and the various factors developed are shown in a model in Figure 5.11 below.

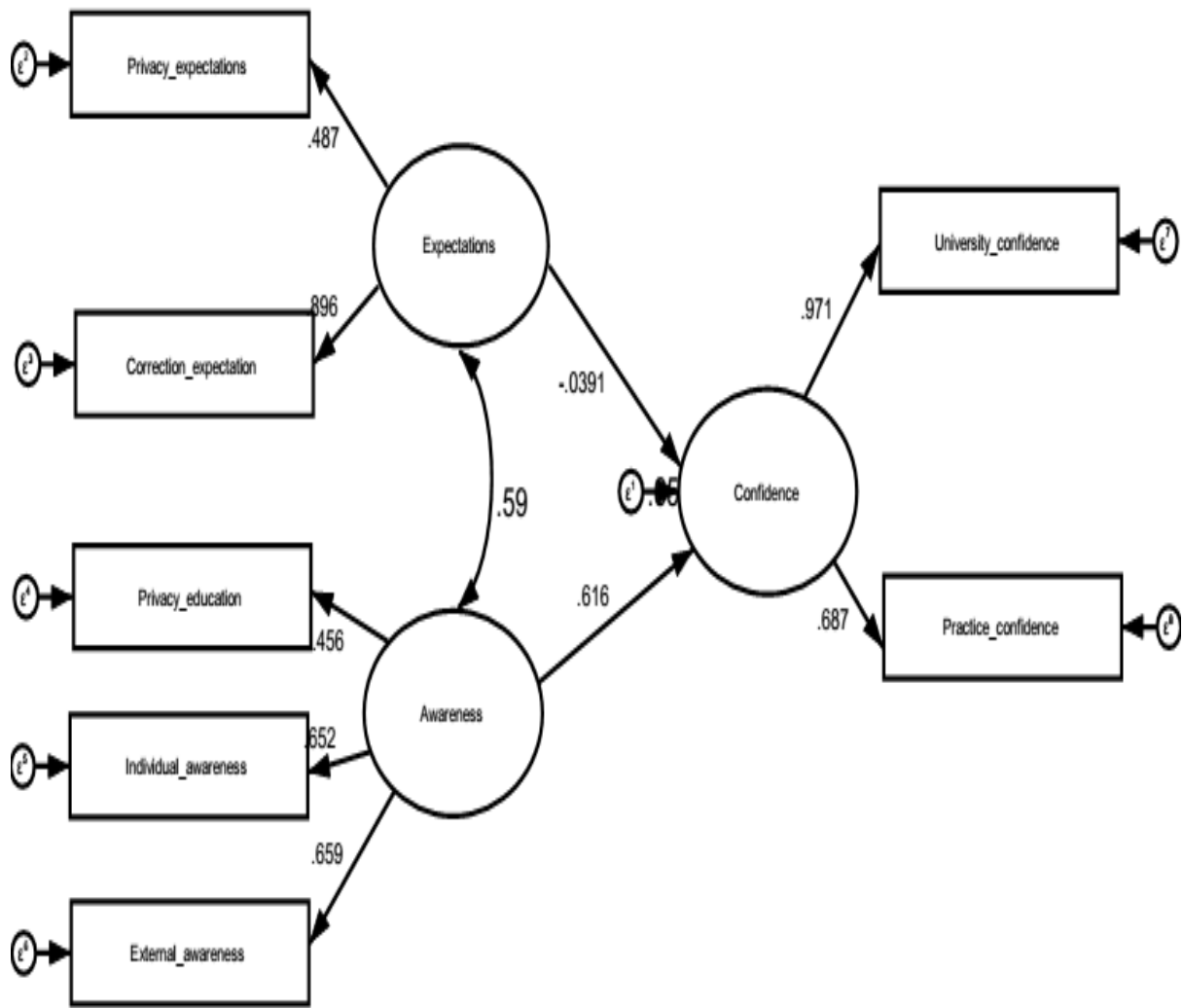


Figure 5.11: Model fit for information privacy perceptions

Note: Direct causal relationship = \longrightarrow , Correlations between variables = \longleftrightarrow
 Error between actual and predicted value = \textcircled{e}

From the model in Figure 5.11, various strong relationships exist. The first strong relationships that exists suggests that students' expectations influence privacy expectations (0.487) and correction expectation (0.896). This corroborates with the findings from other studies (Feri et al., 2016; Vail et al., 2008) that found that people (students) have expectations that the organisation (university) will handle their personal information fairly and will comply with the privacy policies in place.

It is also evident from the diagram that awareness strongly influences privacy awareness (0.456), individual awareness (0.652) and external awareness (0.659). Very strong relationships are shown to indicate that university confidence influences

privacy confidence (0.971) and practice confidence influences privacy confidence (0.687). The two main concepts, awareness and expectations also have a strong relationship (0.59) though no direction is specified. Awareness increases the confidence levels of students on privacy (0.616). Expectations do not have any influence on confidence as attested to by a very low score (0.0391).

The corresponding model fit statistics for the information privacy perceptions are shown in Table 5.18 below.

Table 5.18: Model fit for information privacy perceptions

Fit Index	Obtained value	Prescribed threshold	Acceptable fit Yes/ No
Absolute fit indices			
Chi-Square (CMIN)	351.64		
Degree of freedom	194		
Relative Chi-square (CMIN/DF)	1.81	<3 = Good <5 = Sometimes permissible	Yes
Root mean squared error of approximation (RMSEA)	0.059	≤ 0.08	Yes
Standardized root mean squared residual (SRMR)	0.041	≤ 0.08	Yes
PCLOSE	0.092	> 0.05	Yes
Relative/ incremental fit indices			
Comparative fit index (CFI)	0.937	> 0.90	Yes
Tucker-Lewis index (TLI)	0.921	≥ 0.90	Yes

In the summarised overview of the statistical fit analysis for the final information privacy perceptions model in Table 5.18 above, the following can be concluded based on the fit indices obtained:

- The model had a CMIN value of 351.64 with 194 degrees of freedom, giving a CMIN/df of 1.81, which according to Hooper et al. (2008) is good and acceptable for model fit.
- PCLOSE of 0.092, higher than the threshold value of $p > 0.05$, was obtained. This is a good and acceptable fit.
- A RMSEA value of 0.059 was obtained and falls within the minimum acceptable fit of $RMSEA \leq 0.08$.
- A SRMR value of 0.041 was obtained, which is within the prescribed cut-off of ≤ 0.08 . This is within the acceptable levels of goodness of fit.
- The value of CFI obtained was 0.937, which is above the threshold value of more than 0.90 and it is a satisfactory fit.
- The TLI of 0.921 is above the model fit requirement of ≥ 0.9 , which is acceptable.

The model satisfied all the fit indices tested for the final information privacy perceptions model i.e., CMIN/df, RMSEA, SRMR, PCLOSE, CFI and TLI, meaning that the privacy perception model is deemed acceptable and therefore validated. The model indicated an average overall good fit between the theoretically proposed privacy model and the empirically derived structural model as indicated in Figure 5.11. There was then a compelling desire to ascertain the relationships between concepts and dimensions in the model. This was done using the Pearson product moment correlation coefficient (PPMCC).

5.4.3 Pearson product moment correlation coefficient between variables

The Pearson product moment correlation coefficient (PPMCC), also called the Pearson correlation, represents the degree of relationships existing between the variables (Salkind, 2017). The PPMCC was used to validate hypothesis statement no 5 in section 4.12 that reads:

***H₀₅**: There are no relationships in the concepts and dimensions of the model.*

***H_{a5}**: There exist some relationships in the concepts and dimensions of the model.*

Correlations were useful in investigating the relationships existing between the variables in this study. According to Pallant (2011), for the Pearson correlation:

- coefficient of less than 0.10 is considered to have a small effect i.e., $r \leq 0.10$;
- coefficient of between 0.30 and 0.49 is considered to have a medium effect i.e., $0.3 < r \leq 0.49$, and
- coefficient above 0.50 is considered to have a large effect i.e., $r \geq 0.50$.

Pearson's correlation coefficient is considered to be the best way of measuring associations amongst variables (Saunders et al., 2016) because it uses the covariance method, the magnitude of association and the direction of the relationship. In this research, a cut-off value of $r > .30$ at $p < .05$ (medium effect) was chosen in determining the significance of the correlation coefficients. There were specific relationships which were derived from the seven extracted factors, namely university confidence (UC), privacy expectations (PE), individual awareness (IA), external awareness (EA), privacy education (PEd), practice confidence (PC) and correctness expectation (CE). These are shown in Table 5.19 (see Appendix H for full results on the correlation).





Table 5.19: Summary of practically significant factors using the Pearson correlation

Factor	Relationship to factor	r- score	p - score	Effect size
University confidence	Privacy expectations	.096	>.05	none
	Individual awareness	.376**	≤.05	medium
	External awareness	.381**	≤.05	medium
	Privacy education	.287**	≤.05	small
	Practice confidence	.667**	≤.05	large
	Correctness expectation	.294**	≤.05	small
Privacy expectations	University confidence	.096	>.05	none
	Individual awareness	.205**	≤.05	small
	External awareness	.182**	≤.05	small
	Privacy education	.185**	≤.05	small
	Practice confidence	.077	>.05	none

	Correctness expectation	.436**	≤.05	medium
Individual awareness	University confidence	.376**	≤.05	medium
	Privacy expectations	.205**	≤.05	small
	External awareness	.416**	≤.05	medium
	Privacy education	.331**	≤.05	medium
	Practice confidence	.283	≤.05	small
	Correctness expectation	.338**	≤.05	medium
External awareness	University confidence	.381**	≤.05	medium
	Privacy expectations	.182**	≤.05	small
	Individual awareness	.416**	≤.05	medium
	Privacy education	.295**	≤.05	small
	Practice confidence	.245**	≤.05	small
	Correctness expectation	.378**	≤.05	medium
Privacy education	University confidence	.257**	≤.05	small
	Privacy expectations	.185**	≤.05	small
	Individual awareness	.331**	≤.05	medium
	External awareness	.295**	≤.05	small
	Practice confidence	.223**	≤.05	small
	Correctness expectation	.194**	≤.05	small
Practice confidence	University confidence	.667**	≤.05	large
	Privacy expectations	0.077	>.05	none
	Individual awareness	.283**	≤.05	small
	External awareness	.245**	≤.05	small
	Privacy education	.223**	≤.05	small
	Correctness expectation	.180**	≤.05	small
Correctness expectation	University confidence	.294**	≤.05	small
	Privacy expectations	.436**	≤.05	medium
	Individual awareness	.338**	≤.05	medium
	External awareness	.378**	≤.05	medium
	Privacy education	.194**	≤.05	small
	Practice confidence	.180**	≤.05	small

Note: ** Indicates significant difference

Key:

large	
medium	
small	
none	

Based on Table 5.19, the following deductions can be made:

There is a strong (large) positive relationship between university confidence and practice confidence (0.667). There were also moderate (medium) relationships that existed between university confidence and individual awareness (0.376), university confidence and external awareness (0.381), individual awareness and external awareness (0.416), individual awareness and privacy education (0.331), privacy awareness and correctness expectation (0.436), individual awareness and correction expectation (0.338) and external awareness and correction expectation (0.378).

It is also evident from Table 5.19 above that small (weak) positive relationships exist between privacy expectation and individual awareness (0.205), university confidence and privacy education (0.257), privacy education and external awareness (0.295), individual awareness and practice confidence (0.283), external awareness and practice confidence (0.245), privacy education and practice confidence (0.223) as well as university confidence and correction expectation (0.294). Small relationships were also shown between privacy expectation and external awareness (0.182), privacy expectation and privacy education (0.185), privacy education and correctness expectation (0.194) as well as practice confidence and confidence expectation (0.180).

All the relationships, be they strong, medium or small were considered because correlation was deemed significant at 0.01 in a 2-tailed. Very weak relationships (negligible) relationships existed between university confidence and privacy expectation (0.096) and privacy expectation and practice confidence (0.077). These correlations were deemed insignificant as $p > 0.05$.

The following section discusses how group mean differences were tested.

5.4.4 Testing for group mean differences

This section addresses objective 7 in section 1.6.3 that reads: *To determine whether different biographical variables influence privacy awareness, expectations and also confidence of students.* Biographical variables in this research included age bands, gender, and mode of study and programme, which could lead to an answer to this research objective. This was addressed by using both t-tests and Analysis of variance (ANOVA). The t-tests were done for gender and the ANOVAs were done for age, learning mode and programme. ANOVA was used in this research to analyse how the five age bands (Generation Z, the Millennials, Generation X, Baby Boomers and the Silent Generation) perceived the concepts (awareness, expectations and confidence) differently. It was also used to test how conventional, parallel and block students from the three learning modes perceived the privacy of their personal information. Lastly, ANOVA tests were done for the various degree programmes at the university to ascertain if students pursuing different degree programmes had different perceptions regarding their expectations, awareness and confidence in the privacy of their personal information.

5.4.4.1 Gender

The results for the independent t-test indicated the absence of significant differences between males and females pertaining to the measured dimensions. The t-tests shown in Appendix I failed to report that there are statistically reliable differences on males and females with regards to practice confidence, university confidence, external awareness, privacy expectations, individual awareness, privacy education and correction expectations as all the p-values were larger than the pre-specified alpha level of 0.05.

5.4.4.2 Age

The ANOVAs were used to analyse the average scores and variation between scores. The ANOVAs were conducted for the three age groups, which are the 1996 - 2019, 1977 - 1995 and 1965 - 1976 to ascertain their perceptions on privacy with regards to expectations, awareness and confidence. However, the results also specify that there were no significant differences between age group and the independent variables.

This is a result of small F-values, resulting in values of $p > 0.05$. The results are shown in Appendix J.

5.4.4.3 Mode of study

ANOVA test was also conducted to ascertain if students engaging in various modes of study perceived information privacy differently. There were three groups for mode of study, namely conventional, parallel and block. However, the results also indicate the absence of noticeable significant differences amongst mode of study and the independent variables. For all groups, there were small F values, resulting in all values of $p > 0.05$. This meant that there were no significant differences between students from the various modes of study on their perceptions on privacy of their personal information. The corresponding inferential statistics on the ANOVA for modes of study are shown in Appendix K.

5.4.4.4 Programme of study

ANOVA tests were also conducted for the various degree programmes at the university to ascertain if students pursuing different degree programmes had different perceptions regarding their expectations, awareness and confidence in their personal information privacy. The degree programmes were grouped into BBM & IT, BAcc/BBM Finance, BBM Marketing, BA Development Studies, BA Dual Honours/DPhil and 6-month certificate. Statistically significant differences were recorded ($p < 0.05$) between participants' the *external awareness* ($F = 2.44$; $p = 0.048$), *practical confidence* ($F = 2.42$; $p = 0.049$) and *correction expectation factors* ($F = 2.49$; $p = 0.044$).

A Scheffe test for post hoc comparison was conducted to ascertain where precisely the differences amongst the groups lay. Although the three (external awareness, practical confidence and correction expectation) showed some marginal significance upon performing the post hoc tests, none of the pairing differences were significant. This signifies the absence of significant differences between the programmes on any of the scales that were measured, as evidenced by Table 5.20 below (more detail on the ANOVA test for programme of study are shown in Appendix M).

Table 5.20: ANOVAs and post hoc test for program of study

Variable		Sum of Squares	df	Mean Square	F	Sig.
University confidence	Between Groups	5.60	4	1.40	1.73	0.144
	Within Groups	209.92	259	0.81		
	Total	215.51	263			
Privacy expectations	Between Groups	1.32	4	0.33	2.05	0.088
	Within Groups	41.61	259	0.16		
	Total	42.92	263			
Individual awareness	Between Groups	5.34	4	1.33	2.32	0.058
	Within Groups	149.13	259	0.58		
	Total	154.47	263			
External awareness	Between Groups	5.96	4	1.49	2.44	*0.048
	Within Groups	158.28	259	0.61		
	Total	164.24	263			
Privacy education	Between Groups	0.87	4	0.22	0.40	0.809
	Within Groups	140.87	259	0.54		
	Total	141.74	263			
Practice confidence	Between Groups	7.43	4	1.86	2.42	*0.049
	Within Groups	199.09	259	0.77		
	Total	206.52	263			
Correction expectation	Between Groups	1.97	4	0.49	2.49	*0.044
	Within Groups	51.33	259	0.20		
	Total	53.30	263			
Expectations test	Between Groups	1.44	4	0.36	2.88	0.023
	Within Groups	32.27	259	0.12		
	Total	33.70	263			
Awareness test	Between Groups	2.87	4	0.72	2.26	0.063
	Within Groups	82.29	259	0.32		
	Total	85.16	263			
Confidence test	Between Groups	5.30	4	1.32	1.99	0.096
	Within Groups	172.39	259	0.67		
	Total	177.69	263			

Note: * Indicates significant difference

5.4.4.5 Year of study

There were too many groups for the conduct of ANOVA for the year of study; therefore, a non-parametric correlation was done instead, by using the Spearman correlation with a level of significance of $p < 0.05$ (Cohen et al., 2011). A total of six groups to choose from were selected, which are 1st year, 2nd year, 3rd year, 4th year, Doctorate and 6 months certificate. The years of study were treated as one variable, which goes from low to high. From the results, there was a small negative relationship between year of study and university confidence, with a correlation coefficient (r) of -0.181 , which was statistically significant at $p = 0.002$. A small negative relationship existed between year of study and external awareness, with a correlation coefficient of -0.128 , which was statistically significant at $p = 0.031$. The other factors were insubstantial and insignificant as $r < 0.1$ and $p > 0.05$.

The relationships between the three concepts (expectations, awareness and confidence) and year of study were run and the results showed a very weak negative correlations between awareness and year of study ($r = -0.120$; $p = 0.0042$) and very weak negative correlations between confidence and year of study ($r = -0.142$; $p = 0.0016$). In conclusion, there is a slight tendency for university confidence to be lower amongst respondents who have higher education. External awareness also decreases for students with higher qualifications. The non-parametric correlations using the Spearman rho are shown in Table 5.21 below (see Appendix L for more details on Spearman's rho for year of study).

Table 5.21: Spearman correlation for year of study

			6. Please indicate your year of study
Spearman's rho	6. Please indicate your year of study	Correlation Coefficient	1.000
		Sig. (2-tailed)	
	University confidence	Correlation Coefficient	-0.181
		Sig. (2-tailed)	0.002
	Privacy expectations	Correlation Coefficient	0.043
		Sig. (2-tailed)	0.469
	Individual awareness	Correlation Coefficient	-0.044
		Sig. (2-tailed)	0.459

External awareness	Correlation Coefficient	-0.128
	Sig. (2-tailed)	0.031
Privacy education	Correlation Coefficient	-0.036
	Sig. (2-tailed)	0.546
Practice confidence	Correlation Coefficient	-0.078
	Sig. (2-tailed)	0.190
Correction expectation	Correlation Coefficient	-0.014
	Sig. (2-tailed)	0.807
Expectations test	Correlation Coefficient	0.019
	Sig. (2-tailed)	0.753
Awareness test	Correlation Coefficient	-0.120
	Sig. (2-tailed)	0.042
Confidence test	Correlation Coefficient	-0.142
	Sig. (2-tailed)	0.016

NB: Values marked in blue indicate small/ weak relationships amongst the groups.

The results from this section (section 5.4.4) provided the researcher with supportive evidence for objective 8 and hypothesis H₀₆: *The different biographical variables do not influence privacy awareness, expectations and confidence of students.* In other words, the hypothesis is accepted.

5.5 CONCLUSION ON RESEARCH HYPOTHESES

The research hypotheses formulated in section 4.12 in the previous is now discussed and concluded on based on whether the hypothesis is accepted or rejected as supported by the empirical research findings.

Table 5.22: Summary of research hypotheses

Research aim	Research hypotheses		Hypothesis supported
Research aim 1: To develop and validate an instrument measuring privacy awareness,	H ₀₁	The nine-dimensional Information Privacy Perception Survey is not expected to measure the three privacy concepts (awareness, expectations	Rejected

expectations and confidence of students?		and confidence) based on the nine-privacy concepts.	
	Ha1	The nine-dimensional Information Privacy Perception Survey is expected to measure the three privacy concepts (awareness, expectations and confidence) based on the nine-privacy concepts.	Supported
Research aim 2: To determine the expectations of students when the university processes their personal information.	H02	Students do not expect privacy when the university processes their personal information.	Rejected
	Ha2	Students expect privacy when the university processes their personal information.	Supported
Research aim 3: To determine the privacy awareness levels of students when the university processes their personal information.	H03	Students are not aware of privacy when the university is processing their personal information.	Rejected
	Ha3	Students are aware of privacy when the university is processing their personal information.	Supported
Research aim 4: To determine the privacy confidence levels of students in the university observing the privacy of their personal information.	H04	Students do not have confidence in the university observing privacy of their personal information.	Rejected
	Ha4	Students have confidence in the university observing privacy of their personal information.	Supported

Research aim 5: To determine the relationship between the 3 concepts (expectations, awareness and confidence) using correlation analysis.	H ₀ 5	There are no relationships in the concepts and dimensions of the model.	Rejected
	H _a 5	There exist some relationships in the concepts and dimensions of the model.	Supported
Research aim 6: To determine whether different biographical variables influence privacy awareness, expectations and confidence of students.	H ₀ 6	The different biographical variables do not influence privacy awareness, expectations and confidence of students.	Supported
	H _a 6	The different biographical variables influence privacy awareness, expectations and confidence of students.	Rejected

Note: H₀: Null hypothesis and H_a: Alternative hypothesis

Source: Own compilation

Using the statistical output of this study, it can be established that the hypotheses from Ha1 to Ha5 were accepted and Ha6 was rejected because there are very weak and possibly insignificant relationships such that we can conclude that they do not have any influence.

5.6 CHAPTER SUMMARY

The chapter presented the statistical analysis of the results was done and the results were discussed. Biographical analysis was done using the survey response distribution, gender, nationality, mode of study and year of study. The research used both EFA and CFA for descriptive and inferential statistics. Descriptive statistics took the form of communalities, KMO and BTS values, factor analysis and Cronbach alpha coefficients, means and standard deviations. Inferential statistics were also reported using CFA and SEM and these were done for model fit, PPMC, Spearman rho, t-tests

and ANOVAs. The results enabled the researcher to interpret the empirical findings and align them with the theoretical literature review. In this chapter, the following empirical objectives were achieved:

- Research objective 2:** To validate the instrument using factor and item analysis.
- Research objective 3:** To determine the expectations of students when the university processes their personal information.
- Research objective 4:** To determine the privacy awareness levels of students when the university processes their personal information.
- Research objective 5:** To determine the privacy confidence levels of students in the university observing privacy of their personal information.
- Research objective 6:** To determine the relationship between the 3 concepts (expectations, awareness and confidence) using correlation analysis.
- Research objective 7:** To validate the model using structural equation modelling (SEM).
- Research objective 8:** To determine whether different biographical variables influence privacy awareness, expectations and confidence of students.

The following chapter gives a presentation of the study conclusions, limitations and recommendations.

CHAPTER SIX: CONCLUSION, LIMITATIONS AND RECOMMENDATIONS

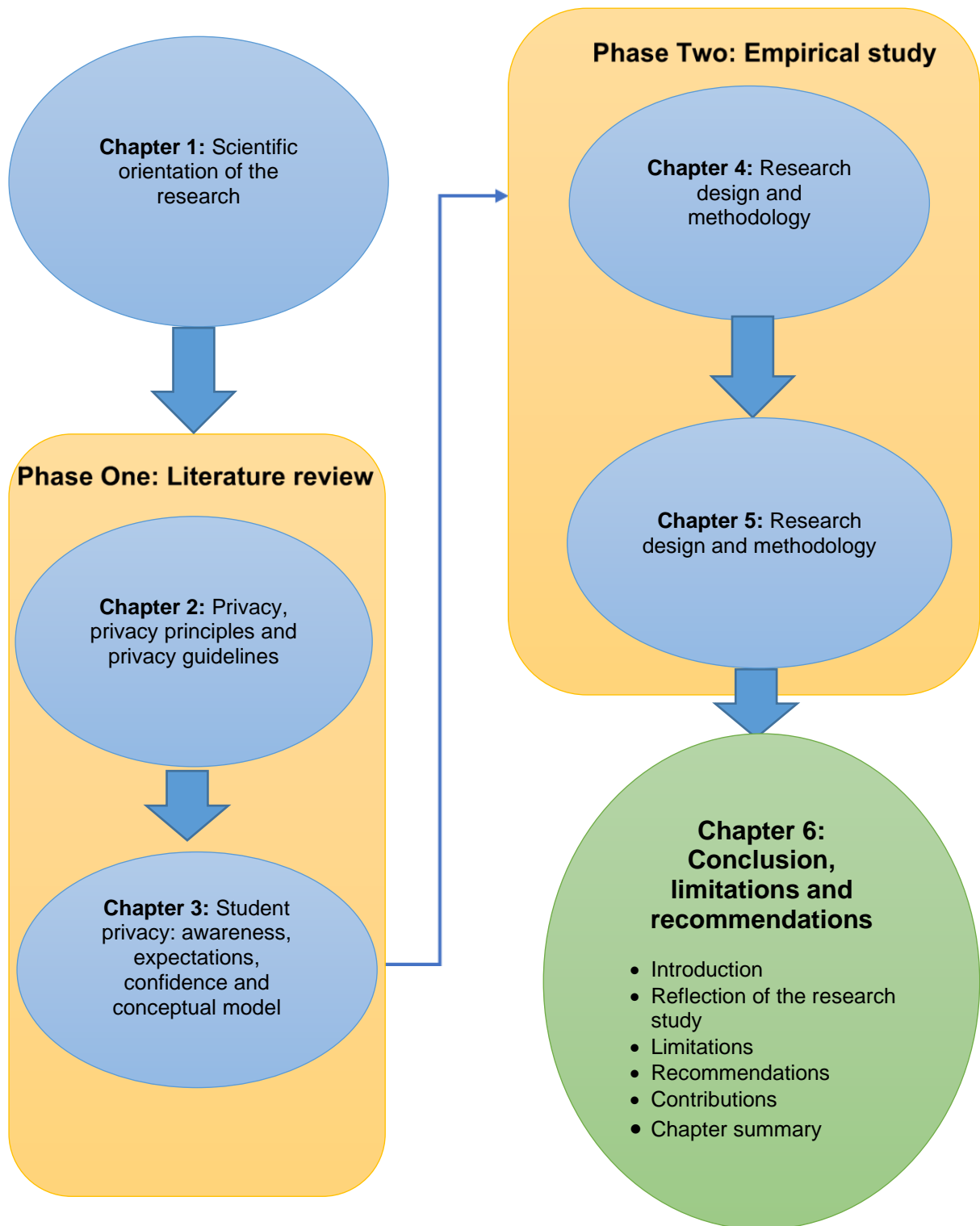


Figure 6.1: Chapter summary flowchart diagram
(Source: Author's own compilation)

6.1 INTRODUCTION

In this chapter, the empirical objective number 9, namely *to make recommendations to improve the information privacy perceptions on the basis of the findings in this research* is addressed. This was articulated in detail in section 6.4. Firstly, this chapter gives a reflection of the research by making conclusions based on literature, followed by conclusions based on the empirical study in the field of information privacy. Secondly, the limitations on both the empirical study and literature review are outlined. This is trailed by practical recommendations for universities based on the study findings and possible future research within the field of information privacy. This also includes a proposed model for the student privacy perceptions. Lastly, the research gives the theoretical, empirical as well as practical value of the research, which are the contributions of this research. The chapter ends with the conclusion of the study.

6.2 REFLECTION OF THE STUDY

In this research, the primary objective was to develop and validate a model and diagnostic instrument to aid universities comprehend the privacy concerns of students and expectations in protecting the privacy of their personal information and aid in affording effect to privacy as their constitutional right. This research was executed in two phases as explained below.

The first phase was the development of the student personal information privacy perception (SPIPP) conceptual model for a university. The structural equation modelling (SEM) was used to validate the empirical model in the second phase. In pursuing the primary aim, there were literature and empirical aims as outlined in sections 1.5.2 and 1.5.3 respectively. Conclusions were drawn on each of these.

6.2.1 Discussion of research aims relating to literature review:

The focus of this section is mainly on literature review conclusions, with respect to the objectives formulated in section 1.5.2 of chapter 1.

6.2.1.1 To conceptualise privacy awareness of students from a theoretical perspective.

This first objective was realised in section 3.4.1 of chapter 3. In achieving this objective, the following information came to light:

- Awareness can be raised through privacy notices, which are amongst the FIPPs fundamental principles for information privacy (Vail et al., 2008). As part of best practice, awareness must not be a once off event as it must be done continuously so that individuals and organisations are educated on what is expected of them on privacy (Botha et al., 2015). The university should remind students continually about privacy issues through privacy education. This can take the form of privacy newsletters, magazines or any form of notices. The university should also conduct privacy training for students so as to increase awareness of privacy.
- The users (students) need to know the importance of being aware of their privacy rights as well as company (university) privacy policies particularly when electronic means are used (Kyobe, 2010b). That is why the university must be compelled to publish privacy notices like the privacy policy on the university websites or the privacy terms and conditions. Lack of awareness signifies that will not be privy to the fine details that are needed for compliance, which might cause non-compliance on privacy related matters, even by the student (Botha et al., 2015).
- Awareness is also an ingredient for a knowledgeable atmosphere on privacy related issues, leading to participation on all university related activities by the students where personal information is needed (Fink, 2012). The university must limit the collection of personal information. Information about the religion, political party affiliation, health status, tribe amongst others is not necessary for academic purposes and therefore, there is no need for its collection.
- Universities are expected to nurture privacy awareness and permit students to practice their consent right when personal information is to be handled. Lack of awareness is a threat to the students' privacy (Isabwe & Reichert, 2013). The university needs to have a reasonable justification for collecting and processing student personal information. The processing will only be justified by the student's consent, a contract or if it is a legal requirement.

- Besides the fact that awareness can increase if students are informed periodically using awareness campaigns about the risks to their privacy, students need to be educated about how best they can control their own personal information collected by the university (Lawler & Molluzzo, 2011; Malandrino, Scarano & Spinelli, 2013). Students must be aware of their right to opt in for (i.e., allow) or opt out for (i.e., disallow) the use of their personal information for some other purposes like marketing, newsletters, job or product advertisements.
- Universities need to conduct themselves in a transparent manner so that students feel empowered, which will make it easy to create a sense of trust (Dwyer & Marsh, 2016). Consequently, it will be easy for students to collaborate in giving out more information.
- According to Nasir, Arshah and Ab Hamid (2017) and Pensa and Di Blasi (2017), if awareness is made a primary concern for an institution, privacy risks and the extent of privacy exposure tend to be under control and minimal.

6.2.1.2 To conceptualise privacy expectations of students from a theoretical perspective.

This objective was achieved in section 3.4.2 of chapter 3. In achieving this objective, the following information came to light:

- Universities need to meet the privacy expectations of students in line with the privacy policies, privacy principles and privacy regulations. Since students' expectations on privacy are sometimes regulated, failure to comply will result in the emergence of lawsuits due to misuse of students' personal information. (Smit et al., 2009). This is so because students expect their personal information not to be disclosed, made available or used, unless it is in line with the law. If not, they will seek justice legally through lawsuits.
- If the university meets the expectations of students on privacy, it increases their promptness in disclosing the required personal information details (Krzych & Ratajczyk, 2013; Schumacher & Ifenthaler, 2018). This can be achieved if the university limits the personal information collection, especially information that is not critical and necessary for purposes in academia like religion, political party affiliation, health status, tribe amongst others. Students also expect the

university to take reasonable steps to ensure that their personal information processed by them is correct in terms of being accurate, up to date, complete and relevant to the purpose of collection.

- Students expect clearly stated privacy rules and policies within universities (Degroot & Vik, 2017). Therefore, the university's privacy notices are expected to be easily understood. It is an expectation of students that the university must have a process whereby the students can request whatever personal information the university has collected about them. This process must also allow the students to request copies of the records of their personal information from the university.
- In cases where there is a necessity for the university to collect and process personal information, some substantial amount of expectations are assumed on privacy that there will be minimal collection and rational expectations on getting information from the individual is relevant (Braun et al., 2018; Mo, 2014). Therefore, students expect the university to collect information lawfully, fairly, to be minimal and to be only for the specified purpose. The university also has to provide students with a method for reviewing their personal information that has been collected to ensure that it is accurate, up to date, complete and relevant for the purpose of collection.

6.2.1.3 To conceptualise student confidence in academic institutions from a theoretical perspective.

This objective was achieved in section 3.4.3 of chapter 3. In achieving this objective, the following information came to light:

- Students have some level of confidence in their universities such that in some instances, they do not bother asking the accessibility of privacy related documents (Stange, 2011). This is a form of trust that students attach to their universities that they will use their personal information to the best of their (students') interests. It becomes the duty of the data controller (the university) to create and maintain such positive environment where students would trust their institution on privacy.
- The presence of some privacy restrictive measures by universities when handling personal information increases trust and confidence to students

(Kafali et al., 2017). This is indicated by the students' confidence that the university has a privacy policy which will guide and restrict how personal information is used. At the same time, too much monitoring and collection of students' personal information can demotivate and dent their confidence in the university (Schumacher & Ifenthaler, 2018). Therefore, the university must give reasonable justification for the collection and processing of student personal information. The justification might be through student consent, a contract or legal requirement. The purpose must be specified no later than the point of personal information collection.

- When customers (students) are given more control over their personal information, their confidence tends to be boosted (Chang et al., 2018; Dwyer & Marsh, 2016; Rao et al., 2014). The best way of doing this is through training so that they are cognisant of information privacy, which reduces the risk of privacy breaches. The university must also have a privacy policy that must be easy to understand for students to have confidence in the institution. The university can also provide students with a method for reviewing their personal information that will have been collected to ensure that it is correct, accurate, up to date, complete and relevant.

6.2.1.4 To develop a conceptual model of privacy awareness, expectations and confidence of students from a theoretical perspective.

This objective was achieved in section 3.7 of chapter 3. The literature review in chapters 2 and 3 and the social contract theory formulated the theoretical foundation for the proposed conceptual model. The student personal information privacy perceptions (SPIPP) conceptual model was proposed in Figure 3.4 of section 3.7.

The following conclusions were drawn from the proposed conceptual model for personal information privacy perceptions for a university:

- The privacy concepts and components were formulated from the FIPPs, the OECD Protection of Privacy and Transborder Flows of Personal Data document, the GDPR and the ZDPA bill. The model's scope was grounded on the privacy of personal information from both the student and university perspective. The components are notice/openness, purpose specification,

information quality, use limitation, collection minimisation, individual participation, privacy education, privacy policy and consent. These aid the understanding of the information privacy perceptions in terms of the awareness, the expectations and the confidence on the university, which were regarded the key concepts of the study.

- Privacy has to be implemented within a university environment where students' details are collected for processing. Students have expectations on privacy and privacy awareness levels, which contribute to the growth of confidence in the university by the student, especially when the university meets their privacy expectations (Alnatheer, Chan & Nelson, 2012). The privacy awareness, expectations and confidence in the university by the students formulate the concepts as perceived in this study.

6.2.2 Discussion of research aims relating to empirical study:

The research findings reflect crucial information on the development and discussion of the three concepts of the empirical model. The study resulted in the design of a diagnostic tool that would aid universities in comprehending and understanding the student's privacy concerns and their expectations on the protection of personal information, privacy and assist in giving effect to their privacy constitutional right.

6.2.2.1 Research objective 1: To develop a privacy perception instrument measuring privacy awareness, expectations and confidence of students

In this research, steps were taken to develop the instrument based on the conceptual model and the questions were phrased from each of the three concepts, namely awareness, confidence and expectations to develop a quantitative survey instrument called the Information Privacy Perception Survey (IPPS). This was used to collect primary data (Kumar, 2011) from student respondents. A self-administered closed ended instrument (Kazi & Khalid, 2012) that used the 5-point Likert scale was developed and distributed over email.

In the instrument design process, the first step was to draft questions that answered the formulated research questions (Saunders et al., 2016). As posited by Greenfield and Greener (2016), it is imperative that the questions be supported by literature.

Expert review analysis and piloting were done (as stated in section 4.10.5) to increase content validity. The result was the final html survey which was distributed to students using the printed hard copies and the link provided to students online.

6.2.2.2 Research objective 2: To validate the instrument using factor and item analysis.

The second objective was to validate the instrument using factor and item analysis as described in sections 5.3.3 and 5.3.5 of chapter 5. The instrument was deployed in an academic institution in Zimbabwe and registered students from various departments within the institution completed the instrument. After data collection, the instrument was subjected to statistical analysis for validation. Both EFA and CFA were deployed in the study. The 54 items were tested for suitability of factor extraction. This was confirmed by the BTS and KMO measures of sample adequacy; therefore, factor analysis was doable. The scree plot explained a cumulative percentage of variance of 60.750% of the total variance. This was perceived to be acceptable as it was above the 60% threshold (Hair et al., 2014). Factor analysis resulted in eight new factors of which factor 6 was excluded based on very low loadings, which were < 0.7 and cross loadings < 0.20 (Hair et al., 2014). The remaining seven factors were named university confidence (UC), privacy expectations (PE), individual awareness (IA), external awareness (EA), privacy awareness (PA), practice confidence (PC) and correctness expectations (CE). The average Cronbach alpha value for the seven factors for reliability was 0.83 and > 0.7 , which is permissible.

6.2.2.3 Research objective 3: To determine the expectations of students when the university processes their personal information.

The third objective was to determine the expectations of students when the university processed their personal information. This objective was realised in chapter 5. The empirical results provided supportive evidence for hypothesis H_{a3} (students expect privacy when the university processes their personal information). Based on the students' responses, and using the newly adopted factors, the mean values for *privacy expectations* and *correction expectation* were 4.56 and 4.53 respectively. These mean values gave a testimony to the fact that students had high expectations on the university upholding the privacy of their personal information.

As the empirical results show, students have high privacy expectations that include the university having reasonable justification for processing their personal information (through consent, contracts, legal requirements for instance). Students expect the university to remind them continually of privacy issues through privacy education and this can be done using privacy newsletters, magazines and notices. Students are also of the view that their personal information should not be disclosed unless if it is in line with the law, which is in line with the results of a study by Pelteret and Ophoff (2016) which found that information must be used in accordance to the individuals' wishes and not be disclosed to third parties without consent from the data subject. The university cannot collect students' personal information without specifying the reasons for such collection and this purpose ought to be specified not later than the point of collection. When the information has been collected, students still feel that they have the privacy right of reviewing what will have been collected to ascertain if its accurate, up to date, complete and relevant.

6.2.2.4 Research objective 4: To determine the privacy awareness levels of students when the university processes their personal information.

The fourth objective was to determine the privacy awareness levels of students when the university processed their personal information. This objective was realised through analysis in chapter 5. The empirical results provided supportive evidence for hypothesis H_{a4} (students are aware of privacy when the university is processing their personal information). Based on the students' responses on the newly adopted factors, awareness levels were recorded on *individual awareness* and *external awareness*, with mean values of 4.10 and 4.14 respectively. This is an indication that students were aware of privacy when the university handles their personal information.

As concluded in the empirical study, students are aware of the fact that the university should take reasonable steps to ensure that their personal information being processed by the university is correct, accurate, up to date, complete and relevant for the purpose of collection. Students are further aware of their privacy right to consent for personal information processing, the right to opt in for personal information use for other purposes like marketing, job or product advertisements and have the same right to opt-out in case they no longer feel comfortable. In addition, students are also aware

of the fact that the university must have a privacy policy, and that the university must uphold best practices through the conduct of privacy training and privacy education for students. This is in line with Fink's (2012) conclusion that awareness by using privacy policies is key in mitigating privacy issues. Kyobe (2010) also argues that it is the duty of institutions to make students aware of their expectations when personal information is being shared.

6.2.2.5 Research objective 5: To determine the privacy confidence levels of students in the university observing privacy of their personal information.

The fifth objective was to determine the privacy confidence levels of students in the university observing the privacy of their personal information. This objective was also realised through analysis in chapter 5. Based on students' responses to the newly adopted factors, confidence levels were recorded on *university confidence* and *practice confidence*, with mean values of 3.57 and 3.41 respectively. The empirical results indicated that students had low confidence levels in the university when using and handling student personal information. The empirical results provided supportive evidence for hypothesis H₀₅ (students do not have confidence in the university observing privacy of their personal information).

Students indicated that they were not confident that the university conducted privacy training for students. Students were also not confident that the university reminded them continually of privacy issues through privacy education using media such as privacy newsletters, magazines and notices. Although the instrument designed by Da Veiga (2018b) was for measuring consumer (student) privacy expectations and confidence, the results were similar to this study in that it reported lack of confidence of consumers (students) in organisations aligning with privacy principles and regulations in the processing of their personal information.

6.2.2.6 Research objective 6: To determine the relationship between the 3 concepts (expectations, awareness and confidence) using correlation analysis.

The sixth objective was to determine the relationship between the 3 concepts (expectations, awareness and confidence) using Pearson correlation analysis.

In achieving this objective, the following was determined:

- The empirical results provided supportive evidence for hypothesis H_{a5} (there exist some relationships in the concepts and dimensions of the model).
- This resulted in different forms of relationships which were also discussed in section 5.4.3. Small, medium and large positive relationships were noticed amongst the variables.
- Positive significant relationships were observed between university confidence and practice confidence, university confidence and individual awareness, university confidence and external awareness, individual awareness and external awareness, individual awareness and privacy education, privacy awareness and correctness expectation, individual awareness and correction expectation and external awareness and correction expectation. These results resonate with Ortiz, Chih and Tsai's (2018) findings, that indicate a direct relationship in ascertaining the relationship between security awareness with concern for information privacy, which are relevant in confirming the significance and relationship between information privacy and information security.
- Small (weak) positive relationships existed between privacy expectation and individual awareness, university confidence and privacy education, privacy education and external awareness, individual awareness and practice confidence, external awareness and practice confidence, privacy education and practice confidence, university confidence and correction expectation, privacy expectation and external awareness, privacy expectation and privacy education, privacy education and correctness expectation as well as practice confidence and confidence expectation. These gave an indication that the relationship could exist but with minimal influence on each other. To the best knowledge of the researcher, there has not been any research on the relationships between the three concepts (expectations, awareness and confidence). However, research by Kurkovsky and Syta (2011) suggests that if students are aware about privacy, they tend to develop trust in the university and this removes their privacy concerns and other negative perceptions.

6.2.2.7 *Research objective 7: To validate the model using structural equation modelling (SEM).*

The seventh objective was to validate the model using structural equation modelling (SEM). This objective was achieved in section 5.4.2 of chapter 5. In achieving this objective, the following information was concluded:

- In conducting SEM, the following indices were used for the model fit: the chi-square (CMIN) of 351.64, degree of freedom 194, relative chi-square (CMIN/DF) 1.81, root mean squared error of approximation (RMSEA) of 0.059, standardized root mean squared residual (SRMR) of 0.041, PCLOSE of 0.092, comparative fit index (CFI) of 0.937 and Tucker-Lewis index (TLI) of 0.921, as shown in Table 5.17.
- In conducting confirmatory factor analysis (CFA) for the newly developed individual factors, five of the seven factors (university confidence, privacy expectations, individual awareness, practice confidence and correction expectation) had fit indices that were acceptable (see Table 5.16). For the other two factors (external awareness and privacy education), the degrees of freedom were too small to compute any fit index and therefore their model fit indices (for external awareness and privacy education) could not be determined.
- The final SEM was conducted for the student personal information privacy perception (SPIPP) model (see Figure 5.12) and the model fit indices (see Table 5.17) were noted. As shown in Table 5.17, the model showed absolute and incremental good fit indices. SEM also confirmed some direct casual relationships as well as correlations between the variables, indicating that university confidence and practice confidence were the main indicators of *confidence*; privacy awareness, individual awareness and external awareness were the main indicators for instilling *awareness* within a university and privacy expectations and correction expectation being the indicators of students' *privacy expectations* within universities.

A student personal information privacy perception (SPIPP) conceptual model was designed in section 3.7, which was based on the literature review. A statistically defined model fit for privacy perceptions was also done in Figure 5.12. Based on the

model, privacy expectations and correction expectation are meaningful factors that are pivotal to the development of a student personal information privacy model for a university, resulting in students developing confidence in the university for upholding the privacy of their personal information. This indicates the fact that students expect the university to maintain the privacy of their personal information as suggested by Henkoğlu and Uçak (2016). Once students are aware of their privacy obligations and the university meets their privacy expectations, trust will evolve and ultimately confidence in the institution (Alnatheer et al., 2012).

Using the statistically designed model fit in Figure 5.12 in section 5.4.2, a SPIPP model was designed using the empirical findings and from the literature review. The three main concepts (expectations, awareness and confidence) and their relationships to the new factors, were indicated in ascertaining student privacy perceptions. This is indicated in Figure 6.2 below.

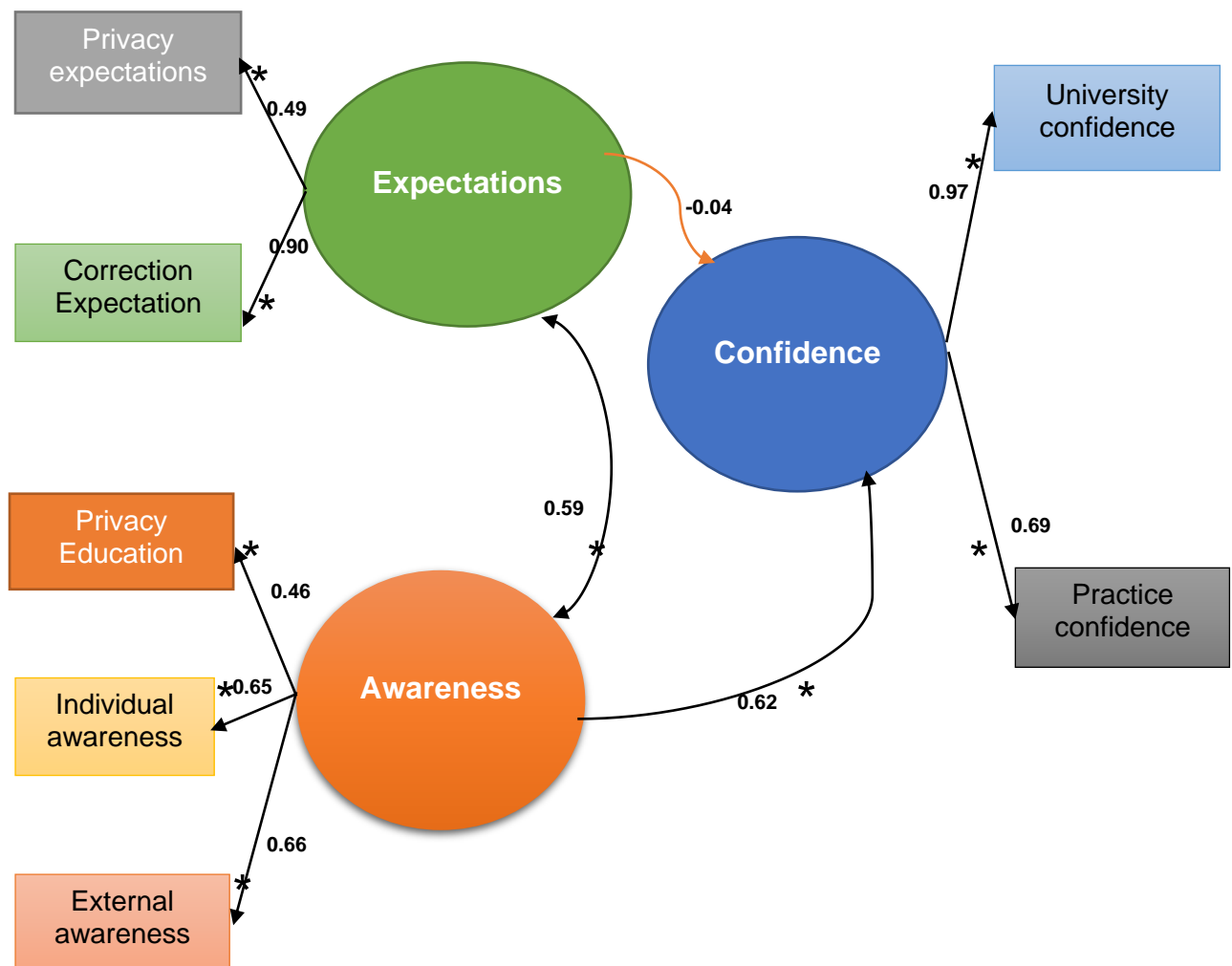
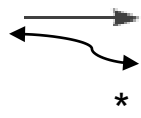


Figure 6.2: Final validated information privacy model
(Source: Author's own compilation)

Key



Indicates a direct relationship between concept and factor.

Indicates a bi-directional relationship amongst concepts.

*

Indicates the significance of the factor

The items being measured and the student feedback on the statements were used in designing the above validated model, and the following conclusions are also made:

- Privacy expectations

Students have a certain level of expectations in terms of how the university processes their personal information (as indicated by a mean value of 4.56). The students were of the opinion that the university has to justify the purpose of collection and this must be done at the point of collection. This collection must be done in a fair and lawful manner. Student personal information must not be disclosed or made available unless if it is in line with the law. Besides the fact that a university must have a privacy policy and do privacy notices, these must also be simple to understand and comprehend. More so, students expect to have the right to opt-in for the usage of their personal information by the university and unreservedly, and opt-out in case they no longer want to share their personal information.

- Correction expectation

The correction expectation factor scored a 4.53 mean value. Students expect the university to come up with methods of ensuring that their personal information is correct, accurate, up-to-date and complete. They also expect the university administrator to specify the purpose for collecting their personal information, on or before the point of collection. Once collected, the university must also ensure that there is a method of checking the collected personal information. This will allow the students to correct and update the information accordingly.

- Individual awareness

At personal level, students have levels of awareness as depicted by a mean value of

4.08. These include appreciation of their right to opt-in in case the university requests them to participate in information sharing and the right to opt-out in case they no longer want to share their personal information. Students are also aware that the university must not disclose or share their personal information in any way without their consent. More so, when they want to have access to their collected personal information, they are aware that there is a due process or method that they have to follow.

- Privacy education

Besides awareness at personal level, the institution must also be aware that they need to specify the purpose for collecting student personal information. This is reflected by a 4.13 mean value. This purpose has to be specified not later than the point of collection. In the process, the university has to justify the purpose of collection to the satisfaction of the subjects (students).

- External awareness

Privacy education is essential as it increases awareness. A mean value of 4.14 was obtained for the external awareness factor. Students will need to be continuously reminded of privacy issues so that their awareness levels are increased. This can be done through newsletters, notices and magazines. In addition, awareness can be increased through conducting of privacy training, which must be fundamentally prioritised in institutions.

- University confidence

University confidence factor had a mean value of 3.57 (which is below the 4.0 threshold value) according to Castro and Martins (2010). Therefore, this indicates an area for university improvement. For students to have confidence in the university, they need to first seek consent from the students so that they can process their personal information. Before collection, the students can have confidence in the process if the motive for collection is specified before collection. Students also have confidence in an institution that does not share or disclose their personal information, except for legal purposes. Publication of privacy policies tends to increase confidence amongst the students on privacy related issues.

- Practice confidence

A mean value of 3.42 was obtained for the practice confidence factor. This is another area in dire need of improvement by the university. The way the university presents itself in handling and using student personal information instils confidence or kills the confidence. When students are given the right to opt-in or opt-out, they will perceive the university of being privacy compliant. The conduct of privacy training by the university is a practice that instils confidence. Another privacy practice that instils confidence is continuous reminders on privacy related issues. In addition to reminding students on privacy related issues, having a privacy policy and a privacy notice are privacy practices that increase student confidence in the institution. A privacy practice like affording students to adhere to a method or follow a due process for checking their collected information tend to also increase student confidence in the university. In conclusion, the SEM results indicated an average overall good fit between the proposed SPIPP conceptual model and the empirically derived SPIPP model.

6.2.2.8 Research objective 8: To determine whether different biographical variables influence privacy awareness, expectations and confidence of students.

The eighth objective was to determine whether different biographical variables influenced privacy awareness, expectations and confidence of students. This was achieved using the t-tests and the ANOVA techniques. Significant differences were obtained for gender, age bands, mode of study, year of study and programmes studied. This is further discussed below:

- Gender

The results of the t-tests that were conducted indicated that there were no significant differences between males and females with regards to university confidence, privacy expectations, individual awareness, external awareness, privacy education, practice confidence and correction expectations because $p > 0.05$ (see Appendix I). Both males and females had the same perceptions on the privacy of their personal information. The research results give a possibility that the concept of privacy is navigated the same by all students, that is, they have the same views. Similarly, in

ascertaining the willingness on information disclosure of personal data on user profiles, Walrave, Vanwesenbeeck and Heirman (2012) also discovered that there were no significant differences on gender.

- Age bands

To ascertain students' perceptions on privacy with regards to expectations, awareness and confidence, ANOVAs were conducted for three age groups (1996 - 2019, 1977 - 1995 and 1965 - 1976). Based on the results obtained (see Appendix J), there were no significant differences between age group and the independent variables. This means that all age groups had the same perceptions on privacy. In a different study assessing the attitude of students on privacy, no significant differences were found on age (Mohamud et al., 2016). Research by Lee, Fan, Oh and Chang (2019) reports some significant differences of age on privacy in that women had higher information privacy concerns on personal information. In resemblance, Walrave, Vanwesenbeeck and Heirman (2012) also discovered that age had significance influence on information disclosure, with the elderly less willing to disclose as compared to young adults.

- Mode of study

To ascertain if students engaging in various modes of study perceived information privacy differently, ANOVAs were conducted. The modes of study included conventional, parallel and block. Using the results in Appendix K, there were no noticeable significant differences amongst mode of study and the independent variables. In this study, the mode of study did not influence the perceptions of students on the privacy of their personal information. All the students within the university shared the same perceptions on privacy.

- Year of study

A non-parametric correlation was done using the Spearman correlation. With six groups selected (1st year, 2nd year, 3rd year, 4th year, Doctorate and 6 months certificate), results (see Appendix L) showed a small negative relationship between year of study and university confidence and year of study and external awareness.

The relationships between the three concepts (expectations, awareness and confidence) with year of study were conducted and there were very weak negative correlations between awareness and year of study and between confidence and year of study.

Confidence in the university was lower amongst respondents who were doing post graduate qualifications and for external awareness seemingly high for students doing undergraduate qualifications. The probable reason is that the post graduate students had obtained other university qualifications at the lower level and were therefore more familiar with university processes. Consequently, they could have seen university shortcomings on privacy, resulting in lower confidence. Significant differences were noted also in other studies on the perceptions of students on information privacy according to various levels of study (Mohamud et al., 2016).

- Programmes under study

ANOVA tests were also conducted for the degree programmes to ascertain if students pursuing different degree programmes had different perceptions regarding their expectations, awareness and confidence in the privacy of their personal information (see Appendix M). In conclusion, there was no significant differences between the programmes on any of the scales that were measured. The programme being pursued by the student did not in any way influence the perceptions of the students. This is similar to the findings by Lawler, Molluzzo and Doshi (2012) where there were no significant differences in understanding privacy dangers online by undergraduate students who were doing different computing courses.

6.2.2.9 Research objective 9: To make recommendations to improve the information privacy perceptions on the basis of the findings of this research.

The ninth objective was to give recommendations to improve the information privacy perceptions on the basis of the findings of this research. A discussion of the recommendations was done in this chapter in section 6.4.

The implications of the findings are perceived to be of paramount importance in guiding how universities will process student personal information. The

recommendations, if implemented, will assist the university in aligning personal information usage with national and international privacy principles and regulations, in the process reducing privacy lawsuits and helping in instilling students' confidence, which is anticipated to reduce student attrition rate.

6.2.3 Conclusions regarding the hypotheses

The conclusions pertaining to hypotheses are presented in this section.

Hypothesis 1: The nine-dimensional Information Privacy Perception Survey was expected to measure the three privacy concepts (awareness, expectations and confidence) based on the nine-privacy concepts. The hypothesis H_{a1} was however rejected in the empirical research. The seven new factors that were used to measure the privacy perceptions of the students were university confidence, privacy expectations, individual awareness, external awareness, privacy education, practice confidence and correctness expectations as discussed in sections 5.3.3 and 5.3.4 and summarised in section 6.2.2.1.

Hypothesis 2: Students expect privacy when the university processes their personal information. This hypothesis was supported as discussed in sections 5.3.1 and 5.3.2. A mean value of 4.55 was obtained for student expectations of the university regarding the processing of their personal information.

Hypothesis 3: Students are aware of privacy when the students are processing their personal information. This hypothesis was supported as discussed in sections 5.3.1 and 5.3.2. A mean value of 4.11 was obtained for student awareness of privacy related issues.

Hypothesis 4: Students have confidence in the university observing the privacy of their personal information. This hypothesis was also supported as discussed in sections 5.3.1 and 5.3.2 (although the confidence level is low). A 3.55 mean value was obtained for student confidence.

Hypothesis 5: There exist some relationships in the concepts and dimensions of the model. The hypothesis was accepted. Small, medium and strong relationships were

identified amongst the concepts and the hypothesis was supported and discussed in section 5.4.3 as well as summarised in section 6.2.2.6.

Hypothesis 6: The different biographical variables influence privacy awareness, expectations and confidence of students. This hypothesis was rejected and discussed in various sections. There were no statistically significant differences on gender with regards to the various factors (section 5.4.4.1), no significant differences between the age groups and the independent variables (section 5.4.4.2), no noticeable significant differences amongst mode of study and the independent variables (5.4.4.3), minor marginal significance on programmes on any of the scales that were measured (section 5.4.4.4). This was also summarised in section 6.2.2.8. Weaker relationships, which were insignificant, were also noticed for the year of study on the variables being measured.

6.3 LIMITATIONS

The limitations in this study are discussed in two steps: the literature review limitations and the empirical study limitations.

6.3.1 Literature review limitations

The limitations of the literature research include:

- The ZDPA bill is yet to be pronounced and promulgated into a law. This means that there is no data governance authority or custodian as yet, which is fundamental in the proposed privacy model for Zimbabwe. Nonetheless, the FIPPs and OECD privacy design guidelines and principles were a good reference point in the design of the model and measuring instrument for privacy within universities.
- In the absence of the law, organisations such as universities are not compelled by law to implement the privacy requirements of the ZDPA bill. The implication therefore is that the results of this survey might be different if the act was in effect because it would have been enforceable, with consequences for every action clearly defined. Thus, we are measuring perception of something that is not yet applicable to this country (Zimbabwe). However, the study is still

applicable because some students and university administrators are now aware of the existence of the bill and there is a high chance that their perceptions are from an informed position.

- Databases used in the literature review were limited to ACM, IEEE Xplore, Sage Research, ScienceDirect, Scopus, Google Scholar and Web of Science. This could have limited some search results that have the potential to enhance this research.

6.3.2 Empirical study limitations

The limitations of the empirical research include:

- Firstly, an increase in the sample size produces a decrease in sampling error and a more representation of the views and perceptions of the population (Visser et al., 2013). A larger sample size could produce a more representative sample result with a small error sampling margin. In addition, the results shown in Table 5.6 reflect a low response rate to the survey, especially if the whole university population is to be considered. Thus, the sample that participated in the study can be argued not to be a true representation of student perceptions on privacy within universities. With a student compliment of more than 5000, it is a challenge to generalise the views of 287 students to represent the views of the university as a whole.
- Secondly, the study was conducted only in one private institution in Zimbabwe. A research argument could be made that these findings were specific to one institution that was used in the study. A wider sample that includes other universities in Zimbabwe could give the researcher a more informed position to generalise the results. This would have been a true reflection of privacy perceptions of Zimbabwean students.
- Whilst still on sampling, the researcher used convenience sampling as students were recruited to participate based on their availability. As pointed out by Hallam and Zanella (2017), the representativeness of convenience sampling is unknown and this could have issues with external validity. To mitigate this, there is need for further research on the same phenomenon in a bid to ravel and generalise student behaviour.
- The fourth empirical issue in this research was based on the limitations of

surveys as in-depth information could not be obtained. According to Jackson (2009), a survey does not support the explanations to questions which might need clarity; before responding to the survey, respondents can be misled by the wording as they might fail to interpret them and surveys suffer from response bias. Interviews were not conducted to obtain in-depth data (Jackson, 2009).

- The fifth limitation is associated with the use of the 5-point Likert scale. Although it can be easily comprehended by the respondents and with consistent possible answers, it is not flexible in offering a wider range of options. Cohen et al. (2011) suggests that the respondent will not be afforded the chance to freely express themselves, rendering the criteria not fully representative of their exact opinions.
- Lastly, the other limitation is that the privacy paradox is more of a trait for the young students as compared to other ages (Kokolakis, 2017). It is the view of the researcher that students might have responded by suggesting that they perceive privacy in a certain way, which could be different from their actual behaviour in reality. Kokolakis (2017) also points out that self-reports especially on privacy behaviour (as requested in this survey) tend to be unreliable, which might be reduced by relying on actual behaviour evidence as opposed to self-reports.

The recommendations are presented next.

6.4 RECOMMENDATIONS

Using the research findings, conclusions and limitations, recommendations for the university as well as for future research are presented in this section.

6.4.1 Recommendations for universities

The recommendations for the university include:

- Results in Table 5.10 indicate that the main areas for improvement are university confidence and practice confidence. Practice confidence is one area requiring improvement, specifically in terms of how to lever consent, individual

participation, privacy education and privacy policy.

- The university's privacy practices in creating an environment that fosters the upholding of privacy of personal information needs to improve. The university has to improve and create an environment that instils student confidence regarding privacy. The descriptive statistics indicated that the university should make sure that they define privacy policies that are easily understood, specify the reason of collection (with consent) and it should minimise as much as possible, the amount of information it collects. Above all, there is need to keep student personal information accurate and up to date. These factors are important because they assist the university in knowing how to uphold privacy within a university environment.
- The results on the biographical groups reported that there is a difference in the undergraduate and postgraduate students' perceptions on privacy. Based on these results, the university can use this to focus on increasing awareness to the less aware undergraduate group. This can be done by using newsletters, privacy notices and magazines.
- The university needs to focus on ascertaining students' expectations towards privacy and understanding their awareness towards their privacy rights. Awareness and expectations, if met and well addressed, have an adverse positive effect on the confidence levels the students have on the university administrator(s) concerning their personal information. To reduce doubt and privacy concerns while increasing student confidence in the privacy practices of the university, student engagement on privacy related issues is envisaged as a practice that must remain ongoing. This is achieved when the university continuously reminds students of privacy issues through privacy education and using privacy newsletters, magazines and notices. This will make students feel comfortable in sharing their personal information, giving them an indirect obligation of upholding privacy.
- There is need for continuous engagement between universities and the data controller. This is done to ensure that compliance is prioritised by the university as the data handler. Undoubtedly, this will instil confidence to students and they will want to be associated with processes that are transparent.
- Based on the correlations and SEM results in Figure 5.12, it can be recommended that privacy awareness influences the confidence levels of students on the university upholding the privacy of their personal information.

Therefore, it is imperative that the university focuses on embarking on awareness enriching privacy education and training. The university must only use the collected personal information for the specified reasons, limiting personal information collection and use, seeking consent for personal information collection and use as well as allowing the students to participate in how their personal information will be used. These are fundamental in increasing the confidence levels of students with the university, as well as having confidence in university privacy practices.

- Based on the feedback from the students, it is the researcher's view that if privacy is to be appreciated and comprehended as an emerging concept in a techno-reliance environment in institutions of higher learning, there is need for a pedagogical approach to it. Privacy and privacy concepts can be imbedded into the current curricula, so as to increase awareness, which is considered fundamental in privacy compliance (Botha et al., 2015; Kyobe, 2010b).

6.4.2 Recommendations for future research

The following are issues suggested for further investigation:

- This study was conducted using one institution as a sample study. In future research, it will be prudent to conduct, validate and even standardise an instrument that is applicable to students in both private and public universities in Zimbabwe as discussed in section 6.3.2. The results would give a model that represents all students from the broader spectrum and it will be highly implementable. This would entail having a larger sample size, representing many students' perceptions on privacy. The bigger the sample size, the more accurate, reliable and valid it becomes (Creswell & Creswell, 2018; Gerber & Hall, 2017). Further to this, a comparison among public and private institutions would aid in knowing which type of institutions (private or public), would need more privacy awareness. Better still, a comparative analysis of student privacy perceptions on privacy on an international scale could also be explored. This might result in an international model that can be implementable anywhere in the world.
- The current study can be repeated using the same concepts and components, but for perceptions in other domains like consumer (student) perceptions on

privacy. Because the provisions of the ZDPA bill are broad, the awareness, expectations and confidence perceptions of consumers (students) also need to be measured so that corrective action is prescribed.

- Since the ZDPA bill is yet to be implemented, the study can be repeated to identify the privacy perceptions once the bill is enacted. This could be done to see if there are subsequent changes on the awareness, expectations and confidence levels of students.
- This research was quantitative in nature. The study can be extended to qualitative research as it is renowned for its comprehensive clarity on facts based on its exploration and efforts to understand how individuals or groups feel about phenomena, for example by using interviews (Creswell & Creswell, 2018). One can also obtain in-depth data by adopting a mixed method approach in which interviews are also used to address the limitation of surveys (Jackson, 2009). Understanding privacy and its related concepts requires an inquiry that will give affirmation to all stakeholders concerned.

6.5 CONTRIBUTIONS

The primary objective of the study was to develop and validate a model and diagnostic instrument to aid universities in comprehending and understanding the student privacy concerns, their expectations in the protection of personal information, privacy and help in achieving their privacy constitutional right. The diagnostic instrument was designed using design principles based on the FIPPs as guidelines and supported by the OECD Protection of Privacy and Transborder Flows of Personal Data document, GDPR and the ZDPA bill. The information gathered in this study was aimed at giving answers to the research questions and this led to the theoretical, empirical and practical contributions as discussed in the sections that follow.

6.5.1 Theoretical level contribution

The theoretical contributions of the research include:

- Literature gave new insight on the conceptualisation of awareness, expectations and confidence of students' perceptions on privacy. The literature further gave insight into the various privacy principles and guidelines with

reference to the nine principles of notice/openness to information usage, information quality, use limitation, purpose specification, collection limitation, individual participation, privacy education, privacy policy and consent. This knowledge led to the development of the conceptual model in section 3.7. The developed conceptual model could thus be used as a model for aiding understanding of the information privacy perceptions of students in terms of awareness, expectations and confidence in the university. Furthermore, future researchers in the field of privacy and its related concepts can make reference to theoretical findings of this research and enhance their searches.

- Earlier studies emphasised privacy related issues like compliance, privacy concerns, privacy online, privacy breaches, privacy awareness, privacy culture for instance, as clearly described in section 1.4. This study focuses on the university-student context with much emphasis on awareness, expectations and confidence. The research results aid in giving an overview of privacy related issues in a university environment, which is critical in comprehending privacy where students are involved.
- The research proposed a model that integrated awareness, expectations and confidence concepts. More so, the study was a result of the integration of the OECD design principles, FIPPs privacy guidelines, the GDPR directive and the ZDPA bill privacy regulation. This makes its adoption easy in Zimbabwe to be easy as well as in other countries.

6.5.2 Empirical contribution

The empirical contributions of the research include the following:

- The research made a stern contribution of constructing a valid and reliable diagnostic instrument for student personal information privacy perceptions in Zimbabwe. The IPPS instrument was developed following the instrument design principles (Jain et al., 2016; Kazi & Khalid, 2012; Kothari, 2012) and all the conceptual and methodological issues raised in literature were addressed and adopted in the development of the IPPS. This valid and reliable instrument can be used for student privacy perceptions measurement within universities. The instrument was validated using factor and item analysis.
- Another important contribution of this study is the construction of an empirically

tested and validated model for privacy perceptions. This validated model should aid universities in gaining a deeper understanding of student privacy perceptions when the universities are collecting and processing their information.

- University administrators could use this validated instrument with a better level of confidence to gather more reliable and valid information about the privacy perceptions that students have when their personal information is handled by the university.
- The university can use the validated model as a guideline to increase privacy awareness so that students have more confidence in the university in upholding the privacy of their personal information.
- The study contributes to the existing knowledge on privacy awareness, privacy expectations and privacy confidence within universities.

6.5.3 Practical contribution

The following are the practical contributions of this study to university, students, the industry, government and other researchers:

- One of the major contributions of this research was the development of a diagnostic instrument that measures privacy awareness, expectations and confidence of students. This instrument can be used by other universities to ascertain privacy perceptions of students based on the three constructs. The instrument developed can be used by universities internationally to ascertain the perceptions of students on privacy. This is useful if the university uses the outcome to identify various action plans like inculcating privacy education and awareness through training, newsletters, privacy notices and magazines and this will be in line with the developmental constructs identified. The instrument can also be customised for the industry to ascertain privacy perceptions of their employees on privacy related issues. For all these reasons, the instrument can be used as a measure of ascertaining privacy perceptions of individuals. Universities can use the instrument to identify how to further improve student awareness of privacy, in line with their expectations. This will ultimately aid in better protection of student personal information and addressing concerns for information privacy amongst students. Assuredly, the instrument will aid in

creating a privacy culture within the university.

- A model for information privacy perceptions was designed based on the model fit privacy perceptions in section 5.4.2 and Figure 7.2 in section 6.4.1. This is a novel privacy perceptions model in a university environment, not only customised for Zimbabwe only but also for application internationally.
- The findings from this research can be used to positively uphold privacy of students' personal information within universities. It is the duty of the university to make students aware of their privacy rights and to align their processing of personal information with legal requirements. To do this, they need to grasp the students' privacy expectations. The model was designed using the Data Protection Bill of Zimbabwe as a piece of available legislature in Zimbabwe. It also derived from some well noted international privacy principles like the FIPPs privacy principle, the OECD design principles and the GDPR and these were aligned to and complimented the Data Protection Bill in Zimbabwe.
- The study contributes to the improvement in the protection of personal information of students processed by universities. The results will aid university management and information regulators to implement measures to create a culture of privacy and to protect student data in line with regulatory and best practice.
- An analysis of the ZDPA bill, the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data privacy guidelines and the GDPR was done. Together with the research results, this could potentially contribute to the body of knowledge concerning privacy awareness, expectations and confidence of students on privacy in institutions of higher learning, primarily in Zimbabwe but also beyond.

6.6 CHAPTER SUMMARY

The chapter gave an overview of the conclusions of this research in the field of information privacy based on the literature and the empirical results. The SPIPP model was proposed in this chapter. The limitations to this research (both literature and empirical) were clearly highlighted, and these were followed by the recommendations. The chapter concluded by explaining the contribution of this research from the theoretical, the empirical and the practical perspectives. In conclusion, the study developed and validated a model and diagnostic tool to aid universities in

comprehending and understanding the privacy concerns of students and their expectations in the protection of their personal information, privacy and help in achieving their privacy constitutional right.

REFERENCE LIST

- Ackerman, M. S., & Mainwaring, S. D. (2005). Privacy Issues and Human-Computer Interaction. *O'Reilly & Associates*, 27(5), 1–19.
- Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Events Study. *Fifth Workshop on the Economics of Information Security*, 1--20. <https://doi.org/10.1.1.73.2942>
- Adelola, T., Dawson, R., & Batmaz, F. (2014). Privacy and data protection in E-commerce: The effectiveness of a government regulation approach in developing nations, using Nigeria as a case. *9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*, 234–239. <https://doi.org/10.1109/ICITST.2014.7038812>
- Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2013). How Privacy Flaws Affect Consumer Perception. *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, 10–17. <https://doi.org/10.1109/STAST.2013.13>
- Aghasian, E., Garg, S., Gao, L., Yu, S., & Montgomery, J. (2017). Scoring Users' Privacy Disclosure Across Multiple Online Social Networks. *IEEE Access*, 5, 13118–13130. <https://doi.org/10.1109/ACCESS.2017.2720187>
- Aghasian, E., Garg, S., & Montgomery, J. (2020). An automated model to score the privacy of unstructured information — Social media case. *Computers & Security*, 92, 1–10. <https://doi.org/10.1016/j.cose.2020.101778>
- Akalu, R. (2018). Privacy, consent and vehicular ad hoc networks (VANETs). *Computer Law and Security Review*, 34(1), 175–179. <https://doi.org/10.1016/j.clsr.2017.06.006>
- Akpojivi, U., & Bevan-Dye, A. (2014). Mobile advertisements and information privacy perception amongst South African Generation Y students. *Telematics and Informatics*, 32(1), 1–10. <https://doi.org/10.1016/j.tele.2014.08.001>
- Allen & Overy LLP. (2017). *The EU General Data Protection Regulation : a new data protection landscape*. pp. 1–12. <https://doi.org/10.1007/978-3-319-57959-7>
- Almadhoun, N. M., Dominic, P. D. D., & Woon, F. L. (2011). Perceived Security , Privacy, and Trust concerns within Social Networking Sites. *IEEE International Conference on Control System, Computing and Engineering*, 426–431. <https://doi.org/10.1109/ICCSCE.2011.6190564>
- Almatarneh, A. (2011). *Privacy protection in the information and communications technology (ICT): a comparative analysis of the laws of the United States , European Union and Jordan* (University of Wollongong). Retrieved from

<http://ro.uow.edu.au/theses/3470>

- Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding And Measuring Information Security Culture. *Pacific Asia Conference on Information Systems (PACIS)*, 144(12), 1–15. Retrieved from <http://aisel.aisnet.org/pacis2012/144>
- Anjum, A., Malik, S. ur R., Choo, K. K. R., Khan, A., Haroon, A., Khan, S., ... Raza, B. (2018). An efficient privacy mechanism for electronic health records. *Computers and Security*, 72, 196–211. <https://doi.org/10.1016/j.cose.2017.09.014>
- Arksey, H., & Malley, L. O. (2005). Scoping Studies: Towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19–32.
- Arnold, K. E., & Sclater, N. (2017). Student perceptions of their privacy in leaning analytics applications. *Proceedings of the Seventh International Learning Analytics & Knowledge Conference on - LAK '17*, 66–69. <https://doi.org/10.1145/3027385.3027392>
- Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, 45, 93–98. <https://doi.org/10.1016/j.chb.2014.11.075>
- Ayyagari, R., & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education: Innovations in Practice*, 11, 85–96. <https://doi.org/10.28945/1569>
- Azemović, J. (2012). Privacy aware eLearning environments based on hippocratic database principles. *Proceedings of the Fifth Balkan Conference in Informatics on - BCI '12*, 142. <https://doi.org/10.1145/2371316.2371344>
- Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, 52, 101947. <https://doi.org/10.1016/j.jretconser.2019.101947>
- Banerjee, S. (2015). Development and Validation of a Conceptual Framework for IT Offshoring Engagement Success (University of Bedfordshire). Retrieved from <http://hdl.handle.net/10547/583209>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management*, 53(1), 1–21. <https://doi.org/10.1016/j.im.2015.08.001>
- 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>
- Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55–69.
<https://doi.org/10.1016/j.tele.2019.03.003>
- Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). *International Differences in Information Privacy Concerns: A Global Survey of Consumers*.
<https://doi.org/10.1080/01972240490507956>
- Bhattacharjee, A. (2012). Introduction to Research, Social Science Research: Principles, Methods, and Practices (2nd ed.). Florida, USA: Global Text Project
- Boell, S. K., & Cecez-Kecmanovic, D. (2015). What is an information system? , *Proceedings of the Annual Hawaii International Conference on System Sciences § (2015)*.
- Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, 15(4), 267–293.
<https://doi.org/10.1016/j.infoandorg.2005.03.001>
- Botha, J. G., Eloff, M. M., & Swart, I. (2015). The effects of the PoPI Act on small and medium enterprises in South Africa. *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*.
<https://doi.org/10.1109/ISSA.2015.7335054>
- Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). *Security and privacy challenges in smart cities*. 39, 499–507.
- Burdon, M. (2011). The conceptual and operational compatibility of data breach notification and information privacy laws (Queensland University of Technology) Retrieved from <https://eprints.qut.edu.au/47512/>
- Burdon, M., Lane, B., & Von Nessen, P. (2012). Data breach notification law in the EU and Australia - Where to now? *Computer Law and Security Review*, 28(3), 296–307. <https://doi.org/10.1016/j.clsr.2012.03.007>
- Burmeister, F., Drews, P., & Schirmer, I. (2019). A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, pp. 1–10. doi: 10125/60040.
- Bush, D. (2016). How data breaches lead to fraud. *Network Security*, 2016(7), 11–

13. [https://doi.org/10.1016/S1353-4858\(16\)30069-1](https://doi.org/10.1016/S1353-4858(16)30069-1)
- Callanan, C., Jerman-Blažič, B., & Blažič, A. J. (2016). User awareness and tolerance of privacy abuse on mobile Internet: An exploratory study. *Telematics and Informatics*, 33(1), 109–128. <https://doi.org/10.1016/j.tele.2015.04.009>
- Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards and Interfaces*, 42, 24–31. <https://doi.org/10.1016/j.csi.2015.04.001>
- Casman, B. S. (2011). *The Right to Privacy in Light of the Patriot Act and Social Contract Theory*. University of Nevada, Las Vegas.
- Castro, M. L., & Martins, N. (2010). The relationship between organisational climate and employee satisfaction in a South African information and technology organisation. *South African Journal of Industrial Psychology*, 36(1), 1–3.
- Cate, F. H. (2006). The Failure of Fair Information Practice Principles. In *Conference on Consumer protection in the age of the `information economy*. Retrieved from <https://ssrn.com/abstract=1156972>
- Cavoukian, A. (2009). Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices. *Information and Privacy Commissioner of Ontario, Canada*, 5. <https://doi.org/10.1007/s12394-010-0062-y>
- Chamroonsawasdi, K., Chottanapund, S., Tunyasitthisundhorn, P., Nawaphan, P., Ruksujarit, T., & Phasuksathaporn, P. (2017). *Development and Validation of a Questionnaire to Assess Knowledge , Threat and Coping Appraisal , and Intention to Practice Healthy Behaviors Related to Non-Communicable Diseases in the Thai Population*, 1–10. <https://doi.org/10.3390/bs7020020>
- Chandramouli, R., Grance, T., Kuhn, R., & Landau, S. (2006). Managing Information Privacy - Developing a Context for Security and Privacy Standards Convergence. *IEEE Security & Privacy*, 4(4), 92–95. <https://doi.org/10.1109/MSP.2006.98>
- Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 35(3), 445-459. <https://doi.org/10.1016/j.giq.2018.04.002>
- Chen, H., Ping, S., & Chen, G. (2015). Computers in Human Behavior Far from reach but near at hand : The role of social media for cross-national mobilization. *Computers in Human Behavior*, 53, 443–451. <https://doi.org/10.1016/j.chb.2015.05.052>

- Chen, L. F., & Ismail, R. (2013). Information Technology program students' awareness and perceptions towards personal data protection and privacy. *International Conference on Research and Innovation in Information Systems (ICRIIS)*. <https://doi.org/10.1109/ICRIIS.2013.6716749>
- Chen, L., Yang, J., Wang, Q., & Niu, Y. (2012). A framework for privacy-preserving healthcare data sharing. *14th International Conference on E-Health Networking, Applications and Services (Healthcom)*, 341–346. <https://doi.org/10.1109/HealthCom.2012.6379433>
- Chetty, P. (2013). Presentation On Zimbabwe Data Protection Bill. In *Harmonization of the ICT Policies in Sub-Sahara Africa*. Retrieved from [https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/In-country support documents/Zimbabwe_Overview of Data Protection Bill_Zimbabwe July 2013 Version 1.pdf](https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/In-country%20support%20documents/Zimbabwe_Overview%20of%20Data%20Protection%20Bill_Zimbabwe%20July%202013%20Version%201.pdf)
- Chilisa, B., & Kawulich, B. (2012). Selecting a Research Approach: Paradigm, Methodology, and Methods. In C. Wagner, B. Kawulich, M. Garner (Eds.), *Doing Social Research A Global Context* (pp. 51–61). McGraw-Hill Higher Education, London.
- Choi, H. S., Lee, W. S., & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modeling. *Computers and Security*, 67, 244–253. <https://doi.org/10.1016/j.cose.2017.03.007>
- Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. <https://doi.org/10.1016/j.tele.2017.01.008>
- Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, 161(September), 120299. <https://doi.org/10.1016/j.techfore.2020.120299>
- Cohen, L., Manion, L., & Morrison, K. (2011). *Research Methods in Education* (7th Editio). London: Routledge.
- Coleman, L., & Purcell, B. M. (2015). Data Breaches in Higher Education. *Journal of Business Cases and Applications*, 15(15), 1–7. Retrieved from <http://www.aabri.com/copyright.html>
- Colquhoun, H. L., Levac, D., O'Brien, K. K., Straus, S., Tricco, A. C., Perrier, L., ... Moher, D. (2014). Scoping reviews: Time for clarity in definition, methods, and reporting. *Journal of Clinical Epidemiology*, 67(12), 1291–1294.

- <https://doi.org/10.1016/j.jclinepi.2014.03.013>
- Cornock, M. (2018). General Data Protection Regulation (GDPR) and implications for research. *Maturitas*, 111, 20–21.
- <https://doi.org/10.1016/j.maturitas.2018.01.017>
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed methods Approaches*. (4th ed.). Los Angeles, USA: SAGE Publications.
- Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (5th ed.). Los Angeles, USA: SAGE Publications.
- Curran, M. (2010). *Introduction to Data Analysis with R for Forensic Scientists* (1st ed.). Boca Raton: CRC Press
- Custers, B., Dechesne, F., Sears, A. ., Tani, T., & van der Hof, S. (2017). A Comparison of Data Protection Legislation and Policies Across the EU. *Computer Law & Security Review*, 1–10.
- <https://doi.org/10.1016/j.clsr.2017.09.001>
- Da Veiga A., Ophoff J. (2020) Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa. In: Clarke N., Furnell S. (eds) *Human Aspects of Information Security and Assurance. HAISA 2020. IFIP Advances in Information and Communication Technology*, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_2
- Da Veiga, Adele. (2008). *Cultivating and Assessing Information Security Culture* (University of Pretoria). Retrieved from <http://hdl.handle.net/2263/24117>
- Da Veiga, Adele. (2017). An Information Privacy Culture Index Framework and Instrument to Measure Privacy Perceptions across Nations : Results of an Empirical Study. *Conference: Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 196–209. Retrieved from <http://hdl.handle.net/10500/23566>
- Da Veiga, Adele. (2018a). An online information privacy culture: A framework and validated instrument to measure consumer expectations and confidence. *2018 Conference on Information Communications Technology and Society (ICTAS)*, 26(2), 1–6. <https://doi.org/10.1109/ICTAS.2018.8368759>
- Da Veiga, Adéle. (2018b). An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information & Computer Security*, 26(3), 338–364.
- Da Veiga, Adele, & Martins, N. (2014). Information Security Culture : A Comparative

- Analysis of Four Assessments. *European Conference on Information Management and Evaluation*, 8, 49–57. <https://doi.org/10.13140/2.1.3221.8885>
- Da Veiga, Adéle, & Martins, N. (2015). Information security culture and information protection culture : A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243–256. <https://doi.org/10.1016/j.clsr.2015.01.005>
- Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law and Security Review*, 34(3), 477–495. <https://doi.org/10.1016/j.clsr.2018.01.005>
- Danezis, G., Domingo-Ferrer, J., Hoepman, J.-H., & Schiffner, S. (2014). Privacy and Data Protection by Design – from policy to engineering. *European Union Agency for Network and Information Security (ENISA)*. <https://doi.org/10.2824/38623>
- Davidson, R. M. (2004). Research Methodology. *City University of Hong Kong*, 1–20. <https://doi.org/10.1016/B978-0-12-802927-5/00003-4>
- Davis, K., Drey, N., & Gould, D. (2009). What are scoping studies? A review of the nursing literature. *International Journal of Nursing Studies*, 46, 1386–1400. <https://doi.org/10.1016/j.ijnurstu.2009.02.010>
- De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, 28, 130–142. <https://doi.org/10.1016/j.clsr.2012.01.011>
- Decoster, J. (1998). *Overview of Factor Analysis*. Retrieved from <http://www.stat-help.com/notes.html>
- Degroot, J. M., & Vik, T. A. (2017). “We were not prepared to tell people yet”: Confidentiality breaches and boundary turbulence on Facebook. *Computers in Human Behavior*, 70, 351-359. <https://doi.org/10.1016/j.chb.2017.01.016>
- Dijkers, M. (2015). What is a Scoping Review ? *Knowledge Translation for Disability and Rehabilitation Research*, 4(1), 1–5. Retrieved from <http://ktdrr.org/products/update/v4n1>
- Djatzmiko, M. (2014). *Trust and Data Privacy in Collaborative and Distributed Environments* (University of New South Wales). Retrieved from <http://unsworks.unsw.edu.au/fapi/datastream/unsworks:11992/SOURCE02?view=true>
- DLA Piper. (2017). Data protection laws of the world. Retrieved from Attorney Advertising website: <https://www.dlapiperdataprotection.com/index.html>

- DLA Piper. (2018). DLA Piper Global Data Protection Laws of the World - World Map. <https://doi.org/10.1017/CBO9781139173254.002>
- Dwyer, N., & Marsh, S. (2016). How students regard trust in an elearning context. *14th Annual Conference on Privacy, Security and Trust (PST)*, 682–685. <https://doi.org/10.1109/PST.2016.7906956>
- Eastlick, M. A., Lotz, S., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. <https://doi.org/10.1016/j.jbusres.2006.02.006>
- El-sheikh, M. M. (2013). *Developing a Libyan information privacy framework* (Queensland University of Technology). Retrieved from [http://eprints.qut.edu.au/65866/1/Mahmoud Mohamed Omar_El-Sheikh_Thesis.pdf](http://eprints.qut.edu.au/65866/1/Mahmoud%20Mohamed%20Omar_El-Sheikh_Thesis.pdf)
- Elder, S. (2009). *Sampling methodology*. Geneva: International Labour Office.
- Ellis, J. L. (2017). *Factor analysis and item analysis*. Retrieved from https://www.applyingstatisticsinbehaviouralresearch.com/documenten/factor_analysis_and_item_analysis_version_11_.pdf
- European Union. (2016a). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88. https://doi.org/10.1007/978-3-319-21719-1_1
- European Union. (2016b). Regulation 2016/679 of the European parliament and the Council of the European Union. *Official Journal of the European Communities*, 2014, 1–88. https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf
- Evergreen, S., Gullickson, A., Mann, C., & Welch, W. (2011). *Developing & Validating Survey Instruments Instrument Validation Steps*. 5895. Retrieved from <http://www.colorado.edu/ibs/decaproject/pubs/instrument-design-webinar-handout.pdf>
- Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2016). A taxonomy of perceived information security and privacy threats among IT security students. *10th International Conference for Internet Technology and Secured Transactions*, 280–286. <https://doi.org/10.1109/ICITST.2015.7412106>
- Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., & Yasin, A. (2019). Sharing

- information online rationally : An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, 48, 102351. <https://doi.org/10.1016/j.jisa.2019.06.007>
- Feri, F., Giannetti, C., & Jentsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior and Organization*, 123, 138–148. <https://doi.org/10.1016/j.jebo.2015.12.001>
- Field, A. (2009). *Discovering Statistics Using SPSS*. Los Angeles, CA: SAGE Publications.
- Field, A. (2012). Effect sizes. *BMJ (Online)*, 345(7882), 1–9. <https://doi.org/10.1136/bmj.e7370>
- Fink, C. (2012). Privacy and Confidentiality in the Virtual Classroom : Instructor Perceptions , Knowledge and Strategies. (University of Victoria). Retrieved from <http://hdl.handle.net/1828/4176>
- Flinders University. (2016). *Flinders University Privacy Policy Framework*. Retrieved from <https://www.flinders.edu.au/content/dam/documents/staff/policies/facilities-info-management/privacy-policy.pdf>
- Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour : Towards an integrated model &. *European Research on Management and Business Economics*, 22(3), 167–176. <https://doi.org/10.1016/j.iedeen.2016.04.002>
- Gajanayake, R., Iannella, R., & Sahama, T. (2011). Privacy by information accountability for e-health systems. *6th International Conference on Industrial and Information Systems*, 49–53. <https://doi.org/10.1109/ICIINFS.2011.6038039>
- Gambanga, N. (2016). Here's a copy of Zimbabwe's draft Data Protection Bill, the law meant to protect you from data theft. *TechZim*. Retrieved from <https://www.techzim.co.zw/2016/08/heres-copy-zimbabwes-draft-data-protection-bill-law-meant-protect-data-theft/>
- Ge, J., Peng, J., & Chen, Z. (2014). Your privacy information are leaking when you surfing on the social networks: A survey of the degree of online self-disclosure (DOSD). *13th International Conference on Cognitive Informatics and Cognitive Computing*, 329–336. <https://doi.org/10.1109/ICCI-CC.2014.6921479>
- Gellman, R. (2017). Fair Information Practices: A Basic History - Version 2.19. *SSRN Electronic Journal*, 1–46. <https://doi.org/10.2139/ssrn.2415020>
- Gerber, H., & Hall, R. (2017). *Quantitative Research Design*. Pretoria: HR Statistics.
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A

- systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, 77, 226–261.
<https://doi.org/10.1016/j.cose.2018.04.002>
- Gie, A., & Pearce, S. (2012). *A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis* (Vol. 9). <https://doi.org/10.20982/tqmp.09.2.p079>
- Gilliland, S. (2014). Towards a Framework for Managing Enterprise Architecture Acceptance (North West University). Retrieved from <http://hdl.handle.net/10394/14776>
- Govani and Pashley. (2005). Student Awareness of the Privacy Implications When Using Facebook. *Education and the Law*, 17(3), 105–110.
<https://doi.org/10.1080/09539960500334087>
- Govender, I. (2015). Mapping “Security Safeguard” Requirements in a data privacy legislation to an international privacy framework: A compliance methodology. *Information Security for South Africa*, 1–8.
<https://doi.org/10.1109/ISSA.2015.7335062>
- Grant, C., & Osanloo, A. (2014). Understanding, selecting and integrating theoretical framework in dissertation research: Creating the blueprint for your house,. *Administrative Issues Journal: Connecting Education, Practice and Research*, 4(2), 12–26. <https://doi.org/10.5929/2014.4.2.9>
- Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher*, 21(6), 34–38.
<https://doi.org/10.7748/nr.21.6.34.e1252>
- Greene, G., & Arcy, J. D. (2010). *Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance*. 1–8. Retrieved from <https://www.albany.edu/iasymposium/proceedings/2010/14-Greene&D'Arcy.pdf>
- Greener, S. (2008). *Business Research Methods*. London, Ventus Publishing ApS
- Greenfield, T., & Greener, S. (2016). *Research Methods for Postgraduates* (3rd ed.). Chichester, UK: John Wiley & Sons Inc
- Guerin, D. & Dohr, J. (2005). Part III: Research Methods (p. 1-9). In D, Guerin & J. Dohr, *Research 101: An Introduction to Research*. University of Minnesota: Informe Design.
- Guffin, P. (2017). FIPPs and PIA. State of the Judicial Branch. Retrieved from https://www.courts.maine.gov/maine_courts/committees/tap/FIPPs-and-PIA-email.pdf

- Haddad, G. El, & Aïmeur, E. (2018). Understanding Trust , Privacy and Financial Fears in Online Payment. *IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, 28–36.
<https://doi.org/10.1109/TrustCom/BigDataSE.2018.00015>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Univariate Data Analysis*. (7th ed.). Essex, England : Pearson New International Edition.
- Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217–227.
<https://doi.org/10.1016/j.chb.2016.11.033>
- Harber, J. G. (2011). *Generations in the workplace: similarities and differences* (East Tennessee State University). Retrieved from
<https://dc.etsu.edu/cgi/viewcontent.cgi?article=2446&context=etd>
- Harborth, D., & Pape, S. (2020). How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor. *ACM SIGMIS Database*, 51(1), 51–69.
<https://doi.org/10.1145/3380799.3380805>
- Hasbullah, N. A., Abdul, W., Wan, R., & Isa, M. (2013). Towards T-Government in Malaysia : Investigation of Citizen ' s Willingness to Participate in Democratic Services and Information Privacy Concern. *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 366–369.
<https://doi.org/10.1109/ICRIIS.2013.6716737>
- Heath, J. (2013). A Privacy Framework for Secondary Use of Medical Data. (University of Wollongong). Retrieved from
<https://doi.org/10.1109/ISTAS.2013.6613116>
- Henkoğlu, A., & Uçak, N. (2016). Information Security and the Protection of Personal Data in Universities. *International Journal of Business and Management Invention*, 5(11), 30–43.
- Hina, S., & Oxley, A. (2014). Participation/collaboration pattern: Perspectives of trust and security risks. *2014 International Conference on Computer and Information Sciences - ICCOINS*, 1–6. <https://doi.org/10.1109/ICCOINS.2014.6868430>
- Homeland Security. (2008). Privacy Policy Guidance Memorandum. U.S. Dept. of Homeland Security. Retrieved from
https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-02_0.pdf

- Hooda, M., & Yadav, B. (2017). Perceptions of Millennials Towards Social Media Privacy Issues : A Survey. *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, 1154–1158. <https://doi.org/10.1109/CTCEEC.2017.8455161>
- Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural Equation Modelling : Guidelines for Determining Model Fit. *Electronic Journal on Business Research Methods*, 6(1), 53–60.
- Hossain, A. A., & Zhang, W. (2015). Privacy and security concern of online social networks from user perspective. *1st International Conference on Information Systems Security and Privacy - ICISSP*, 246–253. Angers, France: IEEE.
- Hox, J. J., & Bechger, T. M. (1998). An Introduction to Structural Equation Modeling. *Family Science Review*, 11, 354–373. Retrieved from <https://www.semanticscholar.org/paper/An-introduction-to-structural-equation-modeling-Hox-Bechger/df2e4362884f74c1d814ab002852368bf4300c4e>
- Huang, H., & Bashir, M. (2016). Privacy by Region: Evaluation Online Users ' Privacy Perceptions by Geographical Region. *2016 Future Technologies Conference (FTC)*, 968–977. <https://doi.org/10.1109/FTC.2016.7821721>
- Hughes, R. L. D. (2015). Two concepts of privacy. *Computer Law & Security Review*, 31(4), 527–537. <https://doi.org/10.1016/j.clsr.2015.05.010>
- Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends® in Human-Computer Interaction*, 1(1), 1–137. <https://doi.org/10.1561/11000000004>
- International Digital Education Group. (2016). Personal Data Protection Competency Framework for School Students. Retrieved from <http://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf>
- Irwin, L. (2020). 54% of universities reported a data breach in the past year. Retrieved from <https://www.itgovernance.co.uk/blog/54-of-universities-reported-a-data-breach-in-the-past-year>
- Isabwe, G. M. N., & Reichert, F. (2013). Revisiting students' privacy in computer supported learning systems. *International Conference on Information Society (i-Society)*, 256–262. Toronto, ON, Canada.
- Islam, M. B., Watson, J., Iannella, R., & Geva, S. (2017). A greater understanding of social networks privacy requirements: The user perspective. *Journal of Information Security and Applications*, 33, 30–44.

- <https://doi.org/10.1016/j.jisa.2017.01.004>
- Israel, M., & Hay, I. (2006). *Research Ethics for Social Scientists*. London, UK: SAGE Publications.
- Ivanova, M., Grosseck, G., & Holotescu, C. (2015). Researching Data Privacy in eLearning. *2015 International Conference on Information Technology Based Higher Education and Training (ITHET)*, 1–6.
<https://doi.org/10.1109/ITHET.2015.7218033>
- Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, 8(4), 49–62.
<https://doi.org/10.1177/160940690900800406>
- Jackson, S. L. (2009). *Research Methods and Statistics: A Critical Thinking Approach* (3rd ed.). Belmont, USA: Wadsworth Cengage Learning.
- Jain, S., Dubey, S., & Jain, S. (2016). Designing and validation of questionnaire. *International Dental & Medical Journal of Advanced Research*, 2(1), 1–3.
<https://doi.org/10.15713/ins.idmjar.39>
- Johnston, A., & Wilson, S. (2012). Privacy compliance risks for Facebook. *IEEE Technology and Society Magazine*, 31(2), 59–64.
<https://doi.org/10.1109/MTS.2012.2185731>
- Jordaan, Y., & Van Heerden, G. (2016). Online privacy-related predictors of Facebook usage intensity. *Computers in Human Behavior*, 70(5), 90–96.
<https://doi.org/10.1016/j.chb.2016.12.048>
- Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications*, 171, 1–32.
<https://doi.org/10.1016/j.jnca.2020.102807>
- Kafali, O., Jones, J., Petruso, M., Williams, L., & Singh, M. P. (2017). How Good Is a Security Policy against Real Breaches? A HIPAA Case Study. *017 IEEE/ACM 39th International Conference on Software Engineering - ICSE*, 530–540.
<https://doi.org/10.1109/ICSE.2017.55>
- Kaneen, C. K., & Petrakis, E. G. M. (2020). Towards evaluating GDPR compliance in IoT applications. *24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems*, 176, 2989–2998.
<https://doi.org/10.1016/j.procs.2020.09.204>
- Katell, M. A., Mishra, S. R., & Scaff, L. (2016). A fair exchange: exploring how online privacy is valued. *49th Hawaii International Conference on System Sciences*,

- 2016-March, 1881–1891. <https://doi.org/10.1109/HICSS.2016.239>
- Katurura, M., & Cilliers, L. (2016). The extent to which the POPI act makes provision for patient privacy in mobile personal health record systems. *2016 IST-Africa Week Conference*, 1–8. <https://doi.org/10.1109/ISTAFRICA.2016.7530595>
- Kazi, A. M., & Khalid, W. (2012). Questionnaire designing and validation. *Journal of the Pakistan Medical Association*, 62(5), 514–516.
- Kim, D., Park, K., Park, Y., & Ahn, J. (2019). Willingness to provide personal information : Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273–281. <https://doi.org/10.1016/j.chb.2018.11.022>
- King, N. J., & Forder, J. (2016). Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data. *Computer Law and Security Review*, 32(5), 696–714. <https://doi.org/10.1016/j.clsr.2016.05.002>
- Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, 6(5), 26. <https://doi.org/10.5430/ijhe.v6n5p26>
- Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling*. New York: The Guilford Press.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers in Human Behavior*, 34(1), 1–24. <https://doi.org/10.1016/j.chb.2018.01.028>
- Kothari, C. (2012). *Research Methods: Methods and Techniques*. (3rd ed.). New Delhi: New Age International (Pvt) Ltd Publishers.
- Krempel, E., & Beyerer, J. (2018). The EU General Data Protection Regulation and its Effects on Designing Assistive Environments. *Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference*, 327–330. <https://doi.org/10.1145/3197768.3201567>
- Krishnan, P., & Vorobyov, K. (2015). Enforcement of privacy requirements. *Computers & Security*, 52, 164–177. <https://doi.org/10.1016/j.cose.2015.03.004>
- Kruikemeier, S., Boerman, S. C., & Bol, N. (2020). Breaching the contract ? Using social contract theory to explain individuals ' online behavior to safeguard privacy. *Media Psychology*, 23(2), 269–292. <https://doi.org/10.1080/15213269.2019.1598434>
- Krzych, Ł. J., & Ratajczyk, D. (2013). Awareness of the patients' rights by subjects on admission to a tertiary university hospital in Poland. *Journal of Forensic and*

- Legal Medicine*, 20(7), 902–905. <https://doi.org/10.1016/j.jflm.2013.06.006>
- Kumar, R. (2011). *Research Methodology: a step-by-step guide for beginners* (3rd ed.). London: Sage Publications.
- Kumaraguru, P., & Cranor, L. (2005). Privacy indexes: A survey of Westin's studies. *Institute for Software Research International (ISRI)*, 1–22. Retrieved from <http://www.casos.cs.cmu.edu/publications/papers/CMU-ISRI-05-138.pdf><http://repository.cmu.edu/isr/856/>
- Kurkovsky, S., & Syta, E. (2011). Monitoring of electronic communications at universities: Policies and perceptions of privacy. *Proceedings of the 44th Annual Hawaii International Conference on System Sciences*, 1–10. <https://doi.org/10.1109/HICSS.2011.312>
- Kyobe, M. (2010a). Knowledge Management Using Information Technology : Ethical and Legal Issues in a University. *2010 International Conference on Information Society*, 592–597. <https://doi.org/10.1109/i-Society16502.2010.6018783>
- Kyobe, M. (2010b). Towards a framework to guide compliance with IS security policies and regulations in a university. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*, 1–6. <https://doi.org/10.1109/ISSA.2010.5588651>
- Lancelot, C., & Smith, H. J. (2019). Information & Management Falsifying and withholding : exploring individuals ' contextual privacy- related decision-making. *Information & Management*, 56(5), 696–717. <https://doi.org/10.1016/j.im.2018.11.004>
- Landesberg, M. K., Levin, T. M., Curtin, C. G., & Lev, O. (1998). Fair Information Practice Principles. Retrieved from Privacy online: A Report to Congress website: [http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Fair Information Practice Principles](http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Fair%20Information%20Practice%20Principles)
- Larrucea, X., Asaf, S., & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Computer Standards & Interfaces*, 69, 1–7. <https://doi.org/10.1016/j.csi.2019.103408>
- Lawler, J., & Molluzzo, J. C. (2011). A survey of first-year college student perceptions of privacy in social networking. *Journal of Computing Sciences in Colleges*, 26(3), 36–41.
- Lawler, J. P., Molluzzo, J. C., & Doshi, V. (2012). An Expanded Study of Net Generation Perceptions on Privacy and Security on Social Networking Sites (SNS). *Information Systems Education Journal (ISEDJ)*, 10(1), 21–36.

- Lehman, A., O'Rourke, N., Hatcher, L., & Stepanski, E. J. (2005). *JMP for Basic Univariate and Multivariate Statistics: A Step-by-step Guide* (1st ed.). Cary, NC: SAS Institute.
- Li, C., & Palanisamy, B. (2019). Privacy in Internet of Things : From Principles to Technologies. *IEEE Internet of Things Journal*, 6(1), 488–505.
<https://doi.org/10.1109/JIOT.2018.2864168>
- Li, H., Luo, X. (Robert), Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information and Management*, 54(8), 1012–1022.
<https://doi.org/10.1016/j.im.2017.02.005>
- Lumpur, K. (2010). Sensitivity to Online Privacy in Social Networking Sites. *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, 21–26.
<https://doi.org/10.1109/ICT4M.2010.5971890>
- Ma, C., & Shek, D. T. (2018). Structural Equation Modeling. In *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation* (pp. 1625–1629). <https://doi.org/http://dx.doi.org/10.4135/9781506326139>
- Mai, J. (2016). Big data privacy : The datafication of personal information. *The Information Society*, 32(3), 192–199.
<https://doi.org/10.1080/01972243.2016.1153010>
- Malandrino, D., Scarano, V., & Spinelli, R. (2013). How increased awareness can impact attitudes and behaviors toward online privacy protection. *2013 International Conference on Social Computing*, 57–62.
<https://doi.org/10.1109/SocialCom.2013.15>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users ' Information Privacy Concerns (IUIPC): The Construct , the Scal ... *Information Systems Research*, 15(4), 336–355.
- Mamonov, S., & Benbunan-fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32–44. <https://doi.org/10.1016/j.chb.2018.01.028>
- Mamonov, S., & Benbunan-Fich, R. (2015). An empirical investigation of privacy breach perceptions among smartphone application users. *Computers in Human Behavior*, 49, 427–436. <https://doi.org/10.1016/j.chb.2015.03.019>
- Manworren, N., Letwat, J., & Daily, O. (2017). Why you should care about the Target data breach. *Business Horizons*, 59(3), 257–266.

- <https://doi.org/10.1016/j.bushor.2016.01.002>
- Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. M. (2015). An Analysis of Personal Information Privacy Concerns using Q-Methodology. *Proceedings of the 26th Australasian Conference on Information Systems*, 1–10. Retrieved from <https://arxiv.org/abs/1606.03547>
- Martin, K. (2015). Privacy Notices as Tabula Rasa : An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing* ., 34(2), 1–47. <https://doi.org/10.1509/jppm.14.139>
- Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, 82, 103–116. <https://doi.org/10.1016/j.jbusres.2017.08.034>
- Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. *Business Ethics Quarterly*, 30(1), 65–96. <https://doi.org/10.1017/beq.2019.24>
- Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., ... Weaven, S. K. (2020). Data Privacy in Retail. *Journal of Retailing*, 96(4), 474–489. <https://doi.org/10.1016/j.jretai.2020.08.003>
- Martin, K. E. (2015). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 137(3), 551–569. <https://doi.org/10.1007/s10551-015-2565-9>
- Martins, N., & Veiga, A. Da. (2015). An Information Security Culture Model Validated with Structural Equation Modelling. *Nineth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 11–21. Retrieved from <http://hdl.handle.net/10500/19061>
- Mathers, N., Fox, N., & Hunn, A. (2009). Surveys and Questionnaires. The NIHR RDS for the East Midlands / Yorkshire & the Humber. Retrieved from https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/12_Surveys_and_Questionnaires_Revision_2009.pdf
- Maydeu-Olivares, A., & Garcia-Forero, C. (2010). Goodness-of-Fit Testing. In *International Encyclopedia of Education*, 7, pp. 190–196. <https://doi.org/10.1016/B978-0-08-044894-7.01333-6>
- Mays, N., Roberts, E., & Popay, J. (2001). Synthesising research evidence. In N. Fulop, P. Allen, A. Clarke, & N. Black (Eds.) *Studying the organisation and delivery of health services* (pp. 188–219). London: Routledge.

- McKnight, H., Carter, M., & Clay, P. (2009). Trust in Technology: Development of a Set of Constructs and Measures. DIGIT 2009 Proceedings - Diffusion Interest Group in Information Technology, 10. <http://aisel.aisnet.org/digit2009>.
- McKnight, H. D., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems*, 11(3), 297–323. [https://doi.org/10.1016/S0963-8687\(02\)00020-3](https://doi.org/10.1016/S0963-8687(02)00020-3)
- Mehta, R. S. (2013). Conceptual and theoretical framework. Retrieved from Technology, Health & Medicine website: <https://www.slideshare.net/rsmehta/conceptual-and-theoretical-framework>
- Mello, S. (2018). *Data Breaches in Higher Education Institutions* (University of New Hampshire). Retrieved from <https://scholars.unh.edu/honors/400>
- Merwe, M. D. Van Der, & Staden, W. J. C. Van. (2015). Unsolicited Short Message Service Marketing : A Preliminary Investigation into Individual Acceptance , Perceptions of Content , and Privacy Concerns. *2015 Information Security for South Africa (ISSA)*, 1–7. <https://doi.org/10.1109/ISSA.2015.7335072>
- Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking & Finance*, 88, 192–207. <https://doi.org/10.1016/j.jbankfin.2017.12.002>
- Miltgen, C. L. (2009). Online consumer privacy concerns and willingness to provide personal data on the internet. *International Journal of Networking and Virtual Organisations*, 6(6), 574. <https://doi.org/10.1504/IJNVO.2009.027790>
- Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information and Management*, 52(6), 741–759. <https://doi.org/10.1016/j.im.2015.06.006>
- Mo, J. Y. C. (2014). Are data protection laws sufficient for privacy intrusions? the case in Hong Kong. *Computer Law and Security Review*, 30(4), 429–438. <https://doi.org/10.1016/j.clsr.2014.05.006>
- Mohammed, Z. A., & Tejay, G. P. (2017). Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. *Computers and Security*, 67, 254–265. <https://doi.org/10.1016/j.cose.2017.03.001>
- Mohamud, I. K., Zeki, A. M., & Saidin, A. Z. (2016). Attitude towards Information Privacy Issues among Students of IIUM. *Proceedings - 2015 4th International Conference on Advanced Computer Science Applications and Technologies*,

- ACSAT 2015, 171–175. <https://doi.org/10.1109/ACSAT.2015.53>
- Mohamud, Ibrahim K., Saidin, A. Z., & Zeki, A. M. (2017). Attitude towards information property rights among students: The case of International Islamic University Malaysia. *Proceedings - 2016 4th International Conference on User Science and Engineering, i-USer 2016*, 145–148. <https://doi.org/10.1109/IUSER.2016.7857950>
- Molenberghs, G. (2010). *Survey Methods and Sampling Techniques*. Brussel: Springer
- Monash University. (2020). Data Protection and Privacy. Retrieved from Strategic Marketing and Communications website: <https://www.monash.edu/privacy-monash/privacy-collection-statements>
- Mudzingwa, F. (2018). HIT Hacked Again? More Than 3 500 Student Account Credentials Leaked. Retrieved August 17, 2018, from TechZim website: <https://www.techzim.co.zw/2018/05/hit-hacked-again-more-than-3-500-student-account-credentials-leaked/>
- Muller, H. (2014). *Quantitative Research : Important issues pertaining to research methodology & analysis strategy*. Retrieved from <https://pdf4pro.com/cdn/quantitative-research-important-issues-pertaining-to-419747.pdf>
- Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture. *Proceedings of the 2017 International Conference on Information System and Data Mining - ICISDM '17*, 56–60. <https://doi.org/10.1145/3077584.3077593>
- NCSS. (2019). Item Analysis. In *Thai Medicine Education Database*. Retrieved from [http://teachingresources.psu.ac.th/files/articles/9_Item Analysis.pdf](http://teachingresources.psu.ac.th/files/articles/9_Item%20Analysis.pdf)
- Ncube, C. B. (2016). Data Protection in Zimbabwe. *African Data Privacy Laws. Law, Governance and Technology Series*, 33, 99–116. https://doi.org/https://doi.org/10.1007/978-3-319-47317-8_5
- Neuman, L. W. (2014). *Social Research Methods: qualitative and quantitative approaches*. Essex, England: Pearson Education Limited.
- Newsom, J. T. (2015). Some Clarifications and Recommendations on Fit Indices. In *Structural Equation Modeling*. Retrieved from <http://www.sci epub.com/reference/209681>
- Nielsen, J., & Landauer, T. K. (1993). A mathematical model of the finding of

- usability problems. *Conference on Human Factors in Computing Systems*, 206–213. <https://doi.org/10.1145/169059.169166>
- Nwaeze, A. C., Zavarsky, P., & Ruhl, R. (2018). Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011. *2017 Twelfth International Conference on Digital Information Management (ICDIM)*, 98–102. <https://doi.org/10.1109/ICDIM.2017.8244644>
- O'Rourke, N., & Hatcher, A. (2013). *A step-by-step approach to using SAS for Factor Analysis and Structural Equation Modelling* (2nd ed.). Cary, NC.: SAS Institute.
- OAIC. (2015). Privacy management framework : Retrieved May 23, 2019, from Office of the Australian Information Commissioner Privacy website: <https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-plan-template-for-organisations/>
- Oats, L. (2012). *Taxation: A Fieldwork Research Handbook* (1st ed.). London, UK: Routledge
- OECD. (2013a). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). *The OECD Privacy Framework*, Retrieved from <http://www.huntonprivacyblog.com/wp-content/files/2013/09/2013-oecd-privacy-guidelines.pdf>
- OECD. (2013b). The OECD Privacy Guidelines. *The OECD Privacy Framework*. Retrieved from <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>
- Okazaki, S., Eisend, M., Plangger, K., Ruyter, K. De, & Grewal, D. (2020). Understanding the Strategic Consequences of Customer Privacy Concerns : A Meta-Analytic Review. *Journal of Retailing*, 96(4), 458–473. <https://doi.org/10.1016/j.jretai.2020.05.007>
- OpenNet Africa. (2016). *State of Internet Freedom in Zimbabwe 2016: Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights*. Retrieved from https://cipesa.org/?wpfb_dl=231
- Ortiz, J., Chih, W. H., & Tsai, F. S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior*, 80, 143–157. <https://doi.org/10.1016/j.chb.2017.11.005>
- Ouma, S. (2013). *M-health user experience framework for the public healthcare sector* (Nelson Mandela Metropolitan University). Retrieved from

<https://core.ac.uk/download/pdf/145050351.pdf>

- Ozdemir, Z. D., Benamati, J. H., & Smith, H. J. (2016). A Cross-Cultural Comparison of Information Privacy Concerns in Singapore , Sweden and the United States. *Proceedings of the 18th Annual International Conference on Electronic Commerce: E-Commerce in Smart Connected World*, 1–5.
<https://doi.org/https://doi.org/10.1145/2971603.2971607>
- Pallant, J. (2011). *SPSS Survival manual: A step by step guide to data analysis using the SPSS* (4th ed.). Berkshire: Allen & Unwin.
- Patsakis, C., Charemis, A., Papageorgiou, A., Mermigas, D., & Pirounias, S. (2018). The market's response toward privacy and mass surveillance: The Snowden aftermath. *Computers and Security*, 73, 194–206.
<https://doi.org/10.1016/j.cose.2017.11.002>
- Pelteret, M., & Ophoff, J. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. *Informing Science: The International Journal of an Emerging Transdiscipline*, 19, 277–301. Retrieved from <http://www.informingscience.org/Publications/3573%0AA>
- Penfield, R. D. (2013). Item analysis. In K. F. Geisinger, B. A. Bracken, J. F. Carlson, J.-I. C. Hansen, N. R. Kuncel, S. P. Reise, & M. C. Rodriguez (Eds.), *APA handbooks in psychology®. APA handbook of testing and assessment in psychology, Vol. 1. Test theory and testing and assessment in industrial and organizational psychology* (p. 121–138). American Psychological Association.
<https://doi.org/10.1037/14047-007>
- Pensa, R. G., & Di Blasi, G. (2017). A privacy self-assessment framework for online social networks. *Expert Systems with Applications*, 86, 18–31.
<https://doi.org/10.1016/j.eswa.2017.05.054>
- Peters, M. D. J., Godfrey, C. M., Khalil, H., McInerney, P., Parker, D., & Soares, C. B. (2015). Guidance for conducting systematic scoping reviews. *International Journal of Evidence-Based Healthcare*, 13(3), 141–146.
<https://doi.org/10.1097/XEB.0000000000000050>
- Peterson, J., Pearce, P. F., Ferguson, L. A., & Langford, C. A. (2017). Understanding scoping reviews: Definition, purpose, and process. *Journal of the American Association of Nurse Practitioners*, 29(1), 12–16. <https://doi.org/10.1002/2327-6924.12380>
- Pham, M. T., Rajić, A., Greig, J. D., Sargeant, J. M., Papadopoulos, A., & McEwen, S. A. (2014). A scoping review of scoping reviews: Advancing the approach and

- enhancing the consistency. *Research Synthesis Methods*, 5(4), 371–385.
<https://doi.org/10.1002/jrsm.1123>
- Pindula News. (2017, June 22). HIT and Nust websites hacked: Retrieved 4 May, 2021, from Pindula News Web site:
<http://www.pindula.co.zw/news/2017/06/22/hit-nust-websites-hacked/#.WVoCkVFLfIU>
- Plessis, M. D. U. (2018). *Constructing and validating a measuring instrument for coping with occupational stress* (University of South Africa). Retrieved from
<http://hdl.handle.net/10500/25387>
- Pouillet, Y. (2018). Is the general data protection regulation the solution ? *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34(4), 773–778. <https://doi.org/10.1016/j.clsr.2018.05.021>
- Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2016). Data protection compliance regulations and implications for smart factories of the future. *Proceedings - 12th International Conference on Intelligent Environments, IE 2016*, 40–47.
<https://doi.org/10.1109/IE.2016.15>
- Privacy Rights Clearinghouse. (2019). Data Breaches. Retrieved from
<https://privacyrights.org/data-breaches>
- Rao, A. A., Chen, L. F., & Dhillon, J. S. (2014). A Preliminary Study on Online Data Privacy Frameworks. *6th International Conference on Information Technology and Multimedia*, 15–20. <https://doi.org/10.1109/ICIMU.2014.7066596>.
- Rasmussen, C., & Dara, R. (2014). Recommender Systems for Privacy Management : A Framework. *IEEE 15th International Symposium on High-Assurance Systems Engineering Recommender*, 243–244.
<https://doi.org/10.1109/HASE.2014.43>
- Raykov, T., & Marcoulides, G. A. (2006). *A First Course in Structural Equation Modeling* (2nd ed.). Retrieved from <https://www.routledge.com/A-First-Course-in-Structural-Equation-Modeling-Raykov-Marcoulides/p/book/9780805855883>
- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers and Security*, 27(7), 241–253.
<https://doi.org/10.1016/j.cose.2008.07.008>
- Riley-Tillman, T. C., & Reinke, W. (2011). Commentary on “Building Local Capacity for Training and Coaching Data-Based Problem Solving With Positive Behavior Intervention and Support Teams.” *Journal of Applied School Psychology*, 27(3), 246–251. <https://doi.org/10.1080/15377903.2011.590782>

- Rossiter, D. G. (2017). *Technical Note : An example of statistical data analysis using the R environment for statistical computing*. Retrieved from https://library.wur.nl/isric/fulltext/isricu_i33970_001.pdf
- Sabbagha, S. M. F. de. (2016). A model for employee motivation and job satisfaction for staff retention practices within a South African foreign exchange banking organisation (University of South Africa). Retrieved from <http://hdl.handle.net/10500/23278>
- Salkind, N. J. (2017). *Exploring research* (9th ed.). Essex, England: Pearson Education Limited
- Salleh, N., Hussein, R., Mohamed, N., & Aditiawarman, U. (2013). An Empirical Study of the Factors Influencing Information Disclosure Behaviour in Social Networking Sites. *2013 International Conference on Advanced Computer Science Applications and Technologies*, 181–185. <https://doi.org/10.1109/ACSAT.2013.43>
- Samani, A., Ghenniwa, H. H., & Wahaishi, A. (2015). Privacy in Internet of Things : A Model and Protection Framework. *Procedia Computer Science*, 52, 606–613. <https://doi.org/10.1016/j.procs.2015.05.046>
- Santanen, E. (2018). The value of protecting privacy. *Business Horizons*, 62(1), 5–14. <https://doi.org/10.1016/j.bushor.2018.04.004>
- Sargsyan, T. (2016). The privacy role of information intermediaries through self-regulation. *Internet Policy Review Journal on Internet Regulation*, 5(4), 1–17. <https://doi.org/10.14763/2016.4.438>
- Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed.). Essex, England: Pearson.
- Scantron. (2018). Survey Tracker Plus. Retrieved November 25, 2019, from https://www.scantron.com/wp-content/uploads/2018/08/SurveyTracker_Plus_Network.pdf
- Schermelleh-engel, K., & Moosbrugger, H. (2014). Evaluating the Fit of Structural Equation Models : Tests of Significance and Descriptive Goodness-of-fit measures. *Methods of Psychological Research*, 8(2), 23–74.
- Schofield, C. B. P., & Joinson, A. N. (2008). Privacy, trust, and disclosure online. *Psychological Aspects of Cyberspace: Theory, Research, Applications*, 13–31. <https://doi.org/10.1017/CBO9780511813740.003>
- Schumacher, C., & Ifenthaler, D. (2018). Features students really expect from learning analytics. *Computers in Human Behavior*, 78, 397–407.

<https://doi.org/10.1016/j.chb.2017.06.030>

- Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management*, 50(1), 1–12. <https://doi.org/10.1016/j.im.2012.11.002>
- Schwaig, S. K., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices : How are the Fortune 500 handling online privacy disclosures? *Information & Management*, 43(7), 805–820. <https://doi.org/10.1016/j.im.2006.07.003>
- Schwarz J. (2014). Research methodology: item analysis, scale analysis and factor Analysis. *Lucerne University of Applied Sciences and Arts*. Retrieved from http://www.schwarzpartners.ch/Applied_Data_Analysis/Lecture_02_EN_2014_Item_Analysis_Scale_Analysis_Factor_Analysis.pdf
- Shen, N., Bernier, T., Sequeira, L., Strauss, J., & Pannor, M. (2019). Understanding the patient privacy perspective on health information exchange : A systematic review. *International Journal of Medical Informatics*, 125, 1–12. <https://doi.org/10.1016/j.ijmedinf.2019.01.014>
- Smit, M., Lyons, K., McAllister, M., & Slonim, J. (2009). Detecting privacy infractions in applications: A framework and methodology. *6th International Conference on Mobile Adhoc and Sensor Systems, MASS '09*, 694–701. <https://doi.org/10.1109/MOBHOC.2009.5336935>
- Sodiya, A. S., & Adegbuyi, B. (2016). *A Framework for Protecting Users' Privacy in Cloud*. 10(4), 33–43. <https://doi.org/10.4018/IJISP.2016100102>
- Stakeholder Review. (2016). *The Right to Privacy in Zimbabwe*. Retrieved from https://hrp.law.harvard.edu/wp-content/uploads/2016/04/zimbabwe_upr2016.pdf
- Stange, C. (2011). Privacy Concern and Student Engagement in the Virtual Classroom (University of Victoria). Retrieved from <https://docplayer.net/13882757-Privacy-concern-and-student-engagement-in-the-virtual-classroom.html>
- Sung, W., & Kang, S. (2017). An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness. *ACM*, 10, 10. <https://doi.org/10.1145/3085228.3085242>
- Swartz, P., & Da Veiga, A. (2016). PoPI Act - Opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment. *2016 Information Security for South Africa - Proceedings of the 2016 ISSA Conference*, 9–17. <https://doi.org/10.1109/ISSA.2016.7802923>

- Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29(3), 821–826.
<https://doi.org/10.1016/j.chb.2012.11.022>
- Talib, S., Ismail, N. A., Olowolayemo, A., Syed Naser, S. A., Haron, S. Z., & Mohammad Yusof, A. H. (2014). Social networks privacy policy awareness among undergraduate students: The case of Twitter. *2014 the 5th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2014*. <https://doi.org/10.1109/ICT4M.2014.7020674>
- Tan, A. Z. Y., Wen Yong Chua, & Chang, K. T. T. (2014). Location Based Services and Information Privacy Concerns among Literate and Semi-literate Users. *47th Hawaii International Conference on System Sciences*, 3198–3206.
<https://doi.org/10.1109/HICSS.2014.394>
- Tankard, C. (2016). What the GDPR means for businesses. *Network Security 2016*, 6, 5–8. [https://doi.org/10.1016/S1353-4858\(16\)30056-3](https://doi.org/10.1016/S1353-4858(16)30056-3)
- Taylor-Powell, E., & Hermann, C. (2000). *Collecting Evaluation Data: Surveys*. Retrieved from <http://learningstore.uwex.edu/Collecting-Evaluation-Data-Surveys-P1027C0.aspx>
- Teijlingen, E. R., & Hundley, V. (2002). Social research update: The importance of pilot studies. *The Social Research Update*, 16(40), 33–36.
<https://doi.org/10.7748/ns2002.06.16.40.33.c3214>
- Teufel, H. (2008). *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*. Retrieved from <https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf>
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 34(1), 134–153.
<https://doi.org/10.1016/j.clsr.2017.05.015>
- Tom, J. (2018). Assessing and Improving Compliance to Privacy Regulations in Business Processes. *CEUR-WS*, 2114, 55–63. Retrieved from <http://ceur-ws.org/Vol-2114/paper7.pdf>
- Tracy, S. J. (2013). *Qualitative Research Methods: collecting evidence, crafting analysis, communicating impact*. (1st ed.). Chichester, United Kingdom: Wiley-Blackwell.
- Tricco, A. C., Soobiah, C., Antony, J., Cogo, E., Macdonald, H., Lillie, E., ... Kastner,

- M. (2016). A scoping review identifies multiple emerging knowledge synthesis methods, but few studies operationalize the method. *Journal of Clinical Epidemiology*, 73, 19–28. <https://doi.org/10.1016/j.jclinepi.2015.08.030>
- Tricco, A. C., Tetzlaff, J., & Moher, D. (2011). The art and science of knowledge synthesis. *Journal of Clinical Epidemiology*, 64(1), 11–20. <https://doi.org/10.1016/j.jclinepi.2009.11.007>
- Ullah, I. (2017). *Privacy-Preserving Mechanisms for Targeted Mobile Advertising* (University of New South Wales). Retrieved from <http://unsworks.unsw.edu.au/fapi/datastream/unsworks:43376/SOURCE02?view=true>
- University of Canterbury. (2019). *Student Declaration Use of Personal Information*. Retrieved from <https://www.canterbury.ac.nz/privacy/student-declaration/use-of-information/>
- University of Plymouth. (2019). University of Plymouth privacy framework.pdf. Retrieved June 17, 2019, from <https://www.plymouth.ac.uk/students-and-family/governance/general-data-protection-regulation-gdpr>
- US Department of Homeland Security & Homeland Security. (2017). Privacy Policy Guidance Memorandum. *U. S. Dept. of Homeland Security*, pp. 1–4.
- Vail, M. W., Earp, J. B., & Antón, A. L. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management*, 55(3), 442–454. <https://doi.org/10.1109/TEM.2008.922634>
- Victor, N., Lopez, D., & Abawajy, J. H. (2016). Privacy models for big data : a survey. *Big Data Intelligence*, 3(1), 61–75. <https://doi.org/10.1504/IJBID.2016.073904>
- Visser, P. S., Krosnick, J. A., & Lavrakas, P. J. (2013). Survey research. In *Handbook of Research Methods in Social and Personality Psychology* (pp. 1–30). Retrieved from https://web.stanford.edu/dept/communication/faculty/krosnick/Survey_Research.pdf
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the ‘privacy paradox.’ *Current Opinion in Psychology*, 31, 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- Walliman, N. (2014). Research Methods: The Basics. In *Research Methods: The Basics* (1st ed.). London: Routledge.
- Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting?

- Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 6(1). <https://doi.org/10.5817/CP2012-1-3>
- Warren, A. M., Sulaiman, A., & Jaafar, N. I. (2014). Social media effects on fostering online civic engagement and building citizen trust and trust in institutions. *Government Information Quarterly*, 31(2), 291–301. <https://doi.org/10.1016/j.giq.2013.11.007>
- Weiers, R. M. (2011). *Introductory Business Statistics* (7th ed.). South-Western: Cengage Learning.
- Weston, R. (2018). A Brief Guide to Structural Equation Modeling. *The Counseling Psychologist*, 34(5), 719–751. <https://doi.org/10.1177/0011000006286345>
- Westwick, C. R. (1976). Item analysis. *The Journal of Nursing Education*, 15(1), 27–32. Retrieved from <http://www.mendeley.com>
- Wheatley, S., Hofmann, A., & Sornette, D. (2019). Data breaches in the catastrophe framework & beyond. *ArXiv Preprint*. Retrieved from <http://arxiv.org/abs/1901.00699>
- Wiley J.F. & Pace L.A. (2015) Chapter 8: Descriptive Statistics and Exploratory Data Analysis. In: *Beginning R: An Introduction to Statistical Programming*. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-0373-6_8
- Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A Contextual Approach to Information Privacy Research. *Journal of the Association for Information Science and Technology*, 71(1), 1–6. <https://doi.org/10.1002/asi.24232>
- Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *Thirty Third International Conference on Information Systems*, 1–16. <https://doi.org/10.1037/t44647-000>
- Yang, F., & Wang, S. (2014). Students' perception toward personal information and privacy disclosure in e-learning. *Turkish Online Journal of Educational Technology*, 13(1), 207–216.
- Young, A., & Quan-Haase, A. (2008). Privacy protection strategies on Facebook. *Information Communication and Society*, 16(4), 479–500. <https://doi.org/10.1080/1369118X.2013.777757>
- Zimbabwe Data Protection Act Bill, D. (2013). *The Zimbabwe Data Protection Act Bill* (pp. 1–47). pp. 1–47. Retrieved from <https://www.dataguidance.com/legal-research/constitution-zimbabwe-amendment-no-20-2013>
- Zimbabwe Data Protection Act draft bill, Z. (2013). Data Protection Bill [Lords].

Retrieved from

https://www.dlapipeperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=ZW

ZIMSTAT. (2017). *Inter-Censal Demographic Survey report*. Retrieved from

http://www.zimstat.co.zw/sites/default/files/img/ICDS_2017.pdf

Zorica, M. B., Biskupic, I. O., Ivanjko, T., & Spiranec, S. (2011). Students and privacy in the networked environment. *34th International Convention MIPRO*, 1090–

1094. Retrieved from <https://ieeexplore.ieee.org/document/5967217>

INDEX OF APPENDICES

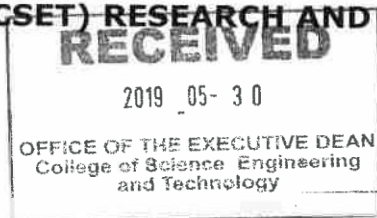
Appendix A: Ethical clearance approval

A1: Humans Ethical Clearance



UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) RESEARCH AND ETHICS COMMITTEE

30 May 2019



Ref #: 030/KM/2019/CSET_SOC

Name: Mr Kudakwashe Maguraushe

Staff #:

Student #: 61945218

Dear Mr Kudakwashe Maguraushe

**Decision: Ethics Approval for 5 years
(Humans involved)**

Researchers: Mr Kudakwashe Maguraushe, 16079 Nkulumane 12, Bulawayo, Zimbabwe, 61945218@mvlife.unisa.ac.za, +263 77 337 6222

Project Leader(s): Dr Adele da Veiga, dveiga@unisa.ac.za, +27 11 670 9175
Prof Nico Martins, martinsn@mweb.co.za, +27 83 266 6372

Working Title of Research:

Framework and assessment instrument for student information privacy culture in a Zimbabwe University

Qualification: PhD Information Systems

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee for the above mentioned research. Ethics approval is granted for a period of five years, from 30 May 2019 to 30 May 2024.

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee. An amended application could be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants.

The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.

3. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
4. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
5. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
6. No field work activities may continue after the expiry date 30 May 2024. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.
7. The Confidentiality Agreement for Research 3rd Parties form for the statistician, must be signed by the statistician before any empirical work is analyzed or received.

Note:

The reference number 030/KM/2019/CSET_SOC should be clearly indicated on all forms of communication with the intended research participants, as well as with the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee.

Yours sincerely




Dr. B Chimbo

Chair: Ethics Sub-Committee SoC, College of Science, Engineering and Technology (CSET)



Prof I. Osunmakinde

Director: School of Computing, CSET



Prof B. Mamba

Executive Dean: CSET

**UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S
(CSET) RESEARCH AND ETHICS COMMITTEE**

28 September 2018

Ref #: 057/KM/2018/CSET_SOC
Name: Mr Kudakwashe Maguraushe
Student #: 61945218
Staff #:

Dear Mr Kudakwashe Maguraushe

**Decision: Ethics Approval for 5 years
(No Humans involved)**

RECEIVED

2018-10-02

OFFICE OF THE CHIEF ETHICS OFFICER
UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY

Researchers: Mr Kudakwashe Maguraushe, 16079 Nkulumane 12, Bulawayo, Zimbabwe,
61945218@mylife.unisa.ac.za, kmaguraushe@gmail.com, +263 77 337 6222

Project Leader(s): Dr A da Veiga, dveiga@unisa.ac.za, +27 11 670 9175
Prof N Martins, martinsn@mweb.co.za

Working title of Research:

A Framework and Assessment Instrument for Student Information Privacy Culture in
Zimbabwe Universities

Qualification: PhD in Information Systems

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee for the above mentioned research. Ethics approval is granted for a period of five years, from 28 September 2018 to 28 September 2023.

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee. An amended application could



Open Rubric

- be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
 4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
 5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
 6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
 7. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number 057/KM/2018/CSSET_SOC should be clearly indicated on all forms of communication with the intended research participants, as well as with the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee.

Yours sincerely



Dr. B Chimbo

Chair: Ethics Sub-Committee SoC, College of Science, Engineering and Technology (CSET)



Prof I. Osunmakinde

Director: School of Computing, CSET



Prof B Mamba

Executive Dean: CSET



Approved - decision template – updated Aug 2016

University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix B: Approval letter for research

NB: Letterhead removed for anonymity

Date: 17 April 2019

Request to conduct research Form (Ref: RBC/KM/042019)

I, **Kudakwashe Maguraushe**, a student at the **University of South Africa (UNISA)**, am doing research titled:

“A framework and assessment instrument for student information privacy culture in Zimbabwean universities”.

The purpose of the research is to carry out a study on the key components that constitute a framework and assessment instrument for personal information privacy perceptions in the Zimbabwean university context and to develop and validate a framework and diagnostic tool to aid universities in comprehending student information privacy concerns and their expectations in the protection of personal information, privacy and assist in achieving the privacy constitutional right. The proposed framework & diagnostic instrument will assist universities as a guideline to understand student perceptions towards privacy and how they perceive the university in meeting privacy requirements. This will be achieved when the university use the outcome to identify action plans in line with the developmental constructs identified. The study will also make some suggestions and recommendations which are useful within the university domain in improving their privacy related matters and to aid in giving effect to the constitutional right to privacy.

The research will be conducted by making prior arrangements with the heads of departments for a presentation in the Department of Business Management and Information Technology (BBM&IT) under the Faculty of Commerce. This is done to orient students on the objectives of the research, what is expected in case someone decides to respond and stressing that participation is voluntary i.e. one can opt out in case they are no longer interested. A total of 270 students will be asked for their consent to participate. They will respond to the questionnaire by answering the survey questions which will be distributed online using SurveyTracker.

I shall undertake to uphold the integrity of the **XXXX** University and respect its ethos and values and will not intentionally seek to undermine its integrity in any way. I also undertake to provide a copy of the completed report to the **XXXX** University Library at the time that I submit my final research findings to my institution.

Signed:



Kudakwashe Maguraushe (researcher)

Cell: +263 773 376 222

Email: 61945218@unisa.ac.za



Approved by the Research Board Chair:

Cell: |

Email:

N.B. A copy of the signed declaration will be kept with the **Research Board Ethics Committee**.

Appendix C: Participation information sheet:

C1: Expert panel participation information sheet

Ethics clearance reference number: 030/KM/2019/CSET_SOC

Date: 19-06-2019

Title: A model and assessment instrument for student information privacy perceptions in a Zimbabwean university

Dear Prospective Participant

My name is Kudakwashe Maguraushe and I am doing research with Dr. A. Da Veiga, Senior Lecturer in the School of Computing and Prof N. Martins, Research Professor in the Department of Industrial and Organisational Psychology, towards a PhD Information Systems at the University of South Africa. We are inviting you to participate in a study entitled "A model and assessment instrument for student information privacy perceptions in a Zimbabwean university".

WHAT IS THE PURPOSE OF THE STUDY?

The research is to investigate the key components that constitute a model and assessment instrument for personal information privacy perceptions in the Zimbabwean university context and secondly to develop and validate a model and diagnostic tool to aid universities in comprehending the student privacy concerns and their expectations in the protection of the privacy of their personal information and assist in achieving their privacy constitutional right.

WHY AM I BEING INVITED TO PARTICIPATE?

You are invited to participate in the evaluation of the questionnaire as an expert panel member. For this expert panel group, we envisage 5-6 people to participate. I have invited the expert panel members to participate in this study because of their expertise in the field of privacy and the protection of personal information. The expert panel review will assist in undertaking a review of the questionnaire questions and are

requested to make recommendations where required. They are made up of people from various disciplines like academics, industry or former students.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a survey whereby the participants, which will be students, will complete a questionnaire. Biographical, general awareness and privacy perception type of questions are included in the questionnaire. The expert panel is invited to review the questionnaire questions prior to the phase whereby the pilot group survey and the final survey are sent out to students.

The expected review time for the expert panel is 1-2 weeks. During this time the expert panel will be given an opportunity to review the questionnaire and to give input.

Participation to review the questionnaire questions will not take up no more than 20 minutes of the expert panel member's time.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey will use a pseudonym for the expert panel members in order to protect their confidentiality and to preserve their privacy.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the privacy of student personal information in the participating university from a research perspective. It is projected that the information gained from this survey will assist us to develop a comprehensive university privacy model and a diagnostic instrument for student personal information. The proposed model & diagnostic instrument will assist universities as a guideline to understand student perceptions towards privacy and how they perceive the university in meeting privacy requirements.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not anticipate that you will encounter any negative experience by completing the research survey. The survey is anonymous, no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

A pseudonym will be recorded and used for the expert panel members. Your feedback will be given a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings. No individual participants will be identifiable in any publications.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at the student's premises and/or Unisa for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Hard copies will be shredded and data will be permanently deleted from the survey application database files and hard drive of the computer through a relevant software application once the purpose has been achieved.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the protection of student personal information in Zimbabwean universities from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Kudakwashe Maguraushe on +263(0)773376222 or email: 61945218@mylife.unisa.ac.za. The findings are accessible for a period of at least 5 years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Kudakwashe Maguraushe on +263(0)773376222 or email: 61945218@mylife.unisa.ac.za.

Should you have concerns about the way in which the research has been conducted, you may contact Dr A. [Da Veiga](mailto:dveiga@unisa.ac.za) on 0116709175 or dveiga@unisa.ac.za. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee, Dr Bester Chimbo, on (011) 670 9105 or chimbb@unisa.ac.za.

Thank you for taking time to read this information sheet and for participating in this study.

Thank you.



Mr. Kudakwashe Maguraushe

C2: Pilot group participation information sheet

Ethics clearance reference number: 030/KM/2019/CSET_SOC

Date: 08-08-2019

Title: A model and assessment instrument for student information privacy perceptions in a Zimbabwean university

Dear Prospective Participant

My name is Kudakwashe Maguraushe and I am doing research with Dr. A. Da Veiga, Senior Lecturer in the School of Computing and Prof N. Martins, Research Professor in the Department of Industrial and Organisational Psychology, towards a PhD Information Systems at the University of South Africa. We are inviting you to participate in a study entitled "A model and assessment instrument for student information privacy perceptions in a Zimbabwean university".

WHAT IS THE PURPOSE OF THE STUDY?

The research is to investigate the key components that constitute a model and assessment instrument for personal information privacy perceptions in the Zimbabwean university context and secondly to develop and validate a model and diagnostic tool to aid universities in comprehending the student privacy concerns and their expectations in the protection of the privacy of their personal information and assist in achieving their privacy constitutional right.

WHY AM I BEING INVITED TO PARTICIPATE?

Students in the participating institution will take part in the pilot study and are invited based on their interaction and use of systems in the organisations whereby personal information is processed. A group of about 10-15 students will participate in the pilot study.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a survey whereby the participants, which will be students, will complete a questionnaire. Biographical, general awareness and privacy perception type of questions are included in the questionnaire. The pilot group will review the questions before the final survey instrument is sent out to students.

The expected timeframe for the pilot group to complete the questionnaire is 15 - 20 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey is designed to be anonymous, therefore there is no way of linking the information provided to you personally.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the privacy of student personal information in the participating university from a research perspective. It is assumed that the information gained from this research survey will help us to develop a comprehensive university privacy model and a diagnostic instrument for student personal information. The proposed model & diagnostic instrument will assist universities as a guideline to understand student perceptions towards privacy and how they perceive the university in meeting privacy requirements.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not anticipate that you will encounter any negative experience by completing the research survey. The survey is anonymous, no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

A pseudonym will be recorded and used for the panel group members. Your feedback will be given a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings. No individual participants will be identifiable in any publications.

By completing this survey, the anonymous information you give may be used for research purposes, that include the dissemination through conference proceedings. And peer-reviewed publications. A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at the student's premises and/or Unisa for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Hard copies will be shredded and data will be permanently deleted from the survey application database files and hard drive of the computer using a relevant software application once the purpose has been achieved.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the protection of student personal information in Zimbabwean universities from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Kudakwashe Maguraushe on +263(0)773376222 or email: 61945218@mylife.unisa.ac.za. The findings are accessible for a period of at least 5 years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Kudakwashe Maguraushe on +263(0)773376222 or email: 61945218@mylife.unisa.ac.za.

Should you have concerns about the way in which the research has been conducted, you may contact Dr A. [Da Veiga](mailto:dveiga@unisa.ac.za) on 0116709175 or dveiga@unisa.ac.za. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee, Dr Bester Chimbo, on (011) 670 9105 or chimbb@unisa.ac.za.

Thank you for taking time to read this information sheet and for participating in this study.

Thank you.



Kudakwashe Maguraushe

Appendix D: Consent to participate form

D1: Expert panel consent form

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the processing of my feedback for the review of the questionnaire as part of the expert panel.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature..... Date.....

Researcher's Name & Surname: **Magoraushe Kudakwashe**

Researcher's signature..... ..... Date: 29-05-2019

CONSENT TO PARTICIPATE IN THIS STUDY

PILOT GROUP

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.


I agree to the processing of my answers in completing the questionnaire for the pilot group.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature.....Date.....

Researcher's Name & Surname: **Maguraushe Kudakwashe**

Researcher's signature..........Date: **29-05-2019**

Appendix E: Questionnaires

E1: Expert review information privacy perceptions questionnaire

Please make sure that you have read the participation information sheet and signed the consent form prior to completing the questionnaire

Information and definition section

It is fully acknowledged that you receive many requests to participate in surveys as a professional in your field. Therefore, your participation in this very important survey is sincerely appreciated.

The questionnaires consist of two sections, namely section one where information about the expert panel is requested and section two with the awareness, expectations and confidence questions. We require the expert panel to indicate for each question whether they believe the item is essential to include or not and whether it is clear or not.

Below some definitions.

Definition 1: Privacy - the ability of an individual to control the terms under which their personal information is acquired and used (Ackerman & Mainwaring, 2005; Schwaig, Kane & Storey, 2006).

Definition 2: Personal information – “any data or information relating to an identified or identifiable individual” (OECD, 2013, p. 13).

The questionnaire comprises of nine components from three dimensions as follows:

A - Notice/ Openness - 2 statements each asked about component A and from an awareness, expectations and confidence perspective.

B - Information quality - 2 statements each asked about component B and from an awareness, expectations and confidence perspective.

C - Purpose specification - 2 statements each asked about component C and from an awareness, expectations and confidence perspective.

D - Use limitation - 2 statements each asked about component D and from an awareness, expectations and confidence perspective.

E - Collection limitation - 2 statements each asked about component E and from an awareness, expectations and confidence perspective.

F - Individual participation - 2 statements each asked about component F and from an awareness, expectations and confidence perspective.

G - Privacy policy - 2 statements each asked about component G and from an awareness, expectations and confidence perspective.

H - Privacy education - 2 statements each asked about component H and from an awareness, expectations and confidence perspective.

I – Consent - 2 statements each asked about component I and from an awareness, expectations and confidence perspective.

On the next page please find the questionnaire. Completion is expected to take no more than 20 minutes.

Section 1: Expert panel information

We require some background information about the experts involved in reviewing the questionnaire and would appreciate if you can please complete the questions below.

- i. What is your field of expertise (e.g. IT technician, legal, academic, privacy consultant)?

- ii. What experience do you have in information privacy?

- iii. How many years' experience do you have in information privacy?

- iv. What experience do you have in information privacy frameworks and policy formulation?

- v. How many years' experience do you have in services/work relating to information privacy frameworks and policy formulation?

- vi. What is your highest qualification?

The survey is conducted to determine the perceptions of students (awareness, expectations and confidence in universities) on the privacy of their personal information.

Instructions

Please provide one response to each item in the questionnaire, starting on the next page.

Indicate with a tick (✓) as to whether you believe the item is essential to include or not and whether it is clear or not.

Section 3 – Personal Information Privacy Culture - Awareness, Expectations and Confidence questions

A - Notice/Openness						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
1. I am aware of the university's privacy notices.									
2. I am aware that institutions can publish a notice for privacy.									
Expectations									
3. I expect to be made aware of privacy through notices.									
4. I expect the university to publish a notice for privacy.									
Confidence									
5. I am confident of privacy through privacy notices									
6. I am confident that the university should publish notices for privacy									
B - Information Quality						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
7. I am aware that the university should ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection									
8. I am aware that the university should protect my personal information									

Expectations									
9. I expect the university to ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection.									
10. I expect the university to protect my personal information.									
Confidence									
11. I am confident that the university should ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection.									
12. I am confident that the university will protect my personal information.									
C - Purpose Specification						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
13. I am aware that the university should specify the purpose when collecting my personal information at the point of collection.									
14. I am aware that the university will inform me about the purpose of collecting my personal information at the point of collection.									
Expectations									
15. I expect the university to specify the purpose when collecting my personal information at the point of collection.									
16. I expect the university to inform me about the purpose of collecting my personal information at the point of collection.									
Confidence									

17. I am confident that the university will specify the purpose when collecting my personal information at the point of collection.									
18. I am confident that the university will inform me about the purpose for collecting my personal information at the point of collection.									
D - Use limitation						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
19. I am aware that my personal information should not be disclosed, made available or used unless if it is by the authority of the law.									
20. I expect my personal information not to be disclosed, made available or used without my consent by the university.									
Expectations									
21. I expect my personal information not to be disclosed, made available or used without my consent by the university.									
22. I expect my personal information not to be disclosed, made available or used unless if it is by the authority of the law.									
Confidence									
23. I am confident that my personal information has not be disclosed, made available or used without my consent by the university.									
24. I am confident that my personal information has not be disclosed, made available or used unless if it is by the authority of the law.									
E - Collection limitation						Expert panel select 1 answer here			

	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
25. I am aware that the university should collect information lawfully, fairly and only for the specified purposes.									
26. I am aware that the university should limit collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.									
Expectations									
27. I expect the university to collect information lawfully, fairly and only for the specified purposes.									
28. I expect the university to limit collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.									
Confidence									
29. I am confident that the university should collect information lawfully, fairly and only for the specified purposes.									
30. I am confident that the university will limit the collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.									
F - Individual participation						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
31. I am aware that i can request from the university, a confirmation on what personal data the university has collected about myself.									

32. I am aware that the university should have a process when requesting personal information that has been collected by the university about myself.									
Expectations									
33. I expect to be able to request from the university, a confirmation on what personal data the university has collected about myself.									
34. I expect the university to have a process when requesting personal information about myself.									
Confidence									
35. I am confident of requesting from the university, a confirmation on what personal data the university has collected about myself.									
36. I am confident that the university has a process to follow when requesting personal information about myself.									
G - Privacy policy	Expert panel select 1 answer here								
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
37. I am aware that the university should have a privacy policy.									
38. I am aware that the privacy policy should be easily understandable.									
Expectations									
39. I expect the university to have a privacy policy.									
40. I expect the privacy policy to be easily understandable.									
Confidence									
41. I am confident that the university has a privacy policy.									

42. I am confident that the privacy policy is easily understandable.									
H - Privacy education						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
43. I am aware that the university should have existing privacy education for students (e.g. on the safe keeping of students' financial details, on the protection of their personal devices, on impersonation issues when on social media platforms, about monitoring of unauthorised access to their emails, on their examination results etc.).									
44. I am aware that the university should remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).									
Expectations									
45. I expect the university to have existing privacy education for students (for example on the safe keeping of their laptops, on the protection of their personal information, when online using social media platforms, on their examination results etc.).									
46. I expect the university to remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).									
Confidence									
47. I am confident that the university has existing privacy education for students (for example on the safe keeping of their laptops, on the protection of their personal information, when online using									

social media platforms, on their examination results etc.).									
48. I am confident that the university reminds me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).									
I - Consent						Expert panel select 1 answer here			
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree	Not essential	Essential	Item is clear	Item is unclear
Awareness									
49. I am aware that i have the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements etc.).									
50. I am aware that i have the right to opt out for the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements etc.).									
Expectations									
51. I expect to have the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements etc.).									
52. I expect to have the right to opt out for the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements etc.).									
Confidence									
53. I am confident that the university gives me the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements etc.).									
54. I am confident that the university gives me the right to opt out for the use of my personal information for other purposes if I am no longer									

interested (like marketing, newsletters, job or product advertisements etc.)									
--	--	--	--	--	--	--	--	--	--

Thank you for completing the document!

E2: Pilot study information privacy perceptions questionnaire

Please make sure that you have read the participation information sheet and signed the consent form prior to completing the questionnaire

Information and definition section

It is fully acknowledged that you might have received many requests to participate in surveys as a university student in your field. Therefore, your participation in this very important survey is sincerely appreciated.

The questionnaire consists of two sections, namely section one where biographical information is requested and section two with the student personal information privacy culture perception questions.

Below some definitions.

Definition 1: Privacy - the ability of an individual to control the terms under which their personal information is acquired and used (Ackerman & Mainwaring, 2005; Schwaig, Kane & Storey, 2006).

Definition 2: Personal information – “any data or information relating to an identified or identifiable individual” (OECD, 2013, p. 13). For example, name, address, phone number, sex, identity number, email address, ethnicity, political/ religious beliefs, marital status, sexual orientation etc.

Definition 3: Personal information processing - “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as obtaining, recording or holding the data or carrying out any operation or set of operations on data, including (a) organization, adaptation or alteration of the data; (b) retrieval, consultation or use of the data; or (c) alignment, combination, blocking, erasure or destruction of the data” (Zimbabwe Data Protection Act bill, 2013).

On the next page please find the questionnaire. Completion is expected to take no more than 20 minutes.

Section 2 – Personal Information Privacy Culture - Awareness, Expectations and Confidence questions

A - Notice/Openness					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
1. I am aware of the university's privacy notices.					
2. I am aware that institutions can publish a notice for privacy.					
Expectations					
3. I expect to be made aware of privacy through notices.					
4. I expect the university to publish a notice for privacy.					
Confidence					
5. I am confident of privacy through privacy notices.					
6. I am confident that the university should publish notices for privacy.					
B - Information Quality					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
7. I am aware that the university should ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection					
8. I am aware that the university should protect my personal information					
Expectations					

9. I expect the university to ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection.					
10. I expect the university to protect my personal information.					
Confidence					
11. I am confident that the university will ensure that my personal information is accurate, up to date, complete and relevant for the purpose of collection.					
12. I am confident that the university protects my personal information.					
C - Purpose Specification					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
13. I am aware that the university should specify the purpose when collecting my personal information at the point of collection.					
14. I am aware that the university will inform me about the purpose of collecting my personal information at the point of collection.					
Expectations					
15. I expect the university to specify the purpose when collecting my personal information at the point of collection.					
16. I expect the university to inform me about the purpose of collecting my personal information at the point of collection.					
Confidence					
17. I am confident that the university will specify the purpose when collecting my personal information at the point of collection.					
18. I am confident that the university informs me about the purpose for collecting my personal information at the point of collection.					
D - Use limitation					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree

Awareness					
19. I am aware that my personal information should not be disclosed, made available or used unless if it is by the authority of the law.					
20. I expect my personal information not to be disclosed, made available or used without my consent by the university.					
Expectations					
21. I expect my personal information not to be disclosed, made available or used without my consent by the university.					
22. I expect my personal information not to be disclosed, made available or used unless if it is by the authority of the law.					
Confidence					
23. I am confident that my personal information has not be disclosed, made available or used without my consent by the university.					
24. I am confident that my personal information has not be disclosed, made available or used unless if it is by the authority of the law.					
E - Collection limitation					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
25. I am aware that the university should collect information lawfully, fairly and only for the specified purposes.					
26. I am aware that the university should limit collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.					
Expectations					
27. I expect the university to collect information lawfully, fairly and only for the specified purposes.					
28. I expect the university to limit collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.					
Confidence					

29. I am confident that the university collects information lawfully, fairly and only for the specified purposes.					
30. I am confident that the university will limit the collection of personal information (like religion, political party affiliation, tribe etc.) which is not necessary for academic purposes.					
F - Individual participation					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
31. I am aware that i can request from the university, a confirmation on what personal data the university has collected about myself.					
32. I am aware that the university should have a process when requesting personal information that has been collected by the university about myself.					
Expectations					
33. I expect to be able to request from the university, a confirmation on what personal data the university has collected about myself.					
34. I expect the university to have a process when requesting personal information about myself.					
Confidence					
35. I am confident of requesting from the university, a confirmation on what personal data the university has collected about myself.					
36. I am confident that the university has a process to follow when requesting personal information about myself.					
G - Privacy policy					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
37. I am aware that the university should have a privacy policy.					
38. I am aware that the privacy policy should be easily understandable.					

Expectations					
39. I expect the university to have a privacy policy.					
40. I expect the privacy policy to be easily understandable.					
Confidence					
41. I am confident that the university has a privacy policy.					
42. I am confident that the privacy policy is easily understandable.					
H - Privacy education					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
43. I am aware that the university should have existing privacy education for students (e.g. on the safe keeping of students' financial details, on the protection of their personal devices, on impersonation issues when on social media platforms, about monitoring of unauthorised access to their emails, on their examination results etc.).					
44. I am aware that the university should remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).					
Expectations					
45. I expect the university to have existing privacy education for students (for example on the safe keeping of their laptops, on the protection of their personal information, when online using social media platforms, on their examination results etc.).					
46. I expect the university to remind me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc.).					
Confidence					
47. I am confident that the university has existing privacy education for students (for example on the safe keeping of their laptops, on the protection of their personal information, when online using social media platforms, on their examination results etc.).					

48. I am confident that the university reminds me continuously on privacy issues through privacy education (for example by having privacy newsletters, magazines, notices etc).					
I - Consent					
	Strongly Agree	Agree	Do not agree or disagree	Disagree	Strongly Disagree
Awareness					
49. I am aware that i have the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements etc.).					
50. I am aware that i have the right to opt out for the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements etc.).					
Expectations					
51. I expect to have the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements etc.).					
52. I expect to have the right to opt out for the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements etc.).					
Confidence					
53. I am confident that the university gives me the right to opt in for the use of my personal information for other purposes (like marketing, newsletters, job or product advertisements etc.)					
54. I am confident that the university gives me the right to opt out for the use of my personal information for other purposes if I am no longer interested (like marketing, newsletters, job or product advertisements etc.)					

Thank you for completing the survey!

E3: Final questionnaire for the survey (HTML format)

Information Privacy Perception Survey
September - October 2019

INFORMATION PRIVACY PERCEPTION SURVEY

September - October 2019



Scroll to the bottom of the screen and click on NEXT

Ethical clearance #: 030/KM/2019/CSET_SOC

Participant Information

Title: A framework and assessment instrument for student information privacy perception in a Zimbabwean university

Dear Participant,

You are invited to participate in a survey conducted by Kudakwashe Maguraushe under the supervision of Prof. Adéle Da Veiga, Professor in the School of Computing and Prof Nico Martins, Research Professor in the Department of Industrial and Organisational Psychology, towards a PhD Information Systems at the University of South Africa.

The survey you have received has been designed to investigate the personal information privacy in the Zimbabwean university context and secondly, to validate the questionnaire. It is envisaged that the questionnaire could be used to aid universities in comprehending student concerns on privacy and their expectations on privacy in the protection of their personal information privacy and assist in achieving their privacy constitutional right.

You were selected to participate in this survey based on your interaction and use of systems in the institution whereby personal information is processed. You will not be eligible to complete the survey if you are younger than 18 years. By completing this research survey, you are agreeing that the information provided may be used for other research purposes, including the dissemination through conference proceedings and peer-reviewed publications.

It is assumed that the information gained from this research survey will help us to design a framework and questionnaire that will give a guideline and make recommendations to universities for improving student personal information privacy in universities. However, you are under no compulsion to complete the research survey and you can pull out from the study before submitting the survey. The survey was designed to be anonymous, which means that we do not have a way of linking the information that you give to you personally. Consequently, you won't be able to pull out from the study once you have clicked the *submit* button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the protection of student personal information in Zimbabwean universities from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

We do not foresee that you will experience any negative consequences by completing the online survey. The online survey is anonymous and no personal identifiable information will be collected. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be permanently destroyed. Hard copies will be shredded and electronic versions will be permanently deleted from the hard drive of the computer.

Information Privacy Perception Survey
September - October 2019

Participant Information continued

The research was reviewed and ethically approved by the Research Ethics Review Committee of the School of Computing, UNISA (approval number: 030/KM/2019/CSET_SOC). The primary researcher, Kudakwashe Maguraushe, can be contacted during office hours at :263773376222 or email:

61945218@mylife.unisa.ac.za. The study leader, Prof Adéle Da Veiga can be contacted during office hours at +27116709175 or dveiga@unisa.ac.za. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee, Dr Bester Chimbo, on +27116709105 or chimbb@unisa.ac.za. Alternatively, you can report any serious unethical behaviour at the University's Toll Free Hotline 080086 96 93.

You are making a decision whether or not to participate by continuing to the next page. You are free to withdraw from the study at any time prior to clicking the send button.

Thank you for participating in this study.

Kudakwashe Maguraushe

Information Privacy Perception Survey
September - October 2019

To proceed with the questionnaire, please answer the following question:

I provide consent by completing this questionnaire.

Yes

No

Consent note:

If you select '**Yes**' in the question above, the questionnaire will skip to *General Information* followed by *Instructions for Online Completion*.

If you select '**No**' in the question above, the questionnaire will skip to the last screen where you can click on SUBMIT without responding to any further questions.

Information Privacy Perception Survey
September - October 2019

General Information

We acknowledge that you might have received many requests to participate in surveys as a university student in your field. Therefore, your participation in this very important survey is sincerely appreciated.

The questionnaire consists of two sections. Section 1 requires you to provide your biographical information and section 2 contains the student personal information privacy questions.

Definitions

Definition 1: Privacy - "the ability of an individual to control the terms under which their personal information is acquired and used"(Ackerman & Mainwaring 2005; Schwaig, Kane & Storey 2006).

Definition 2: Personal information - "any data or information relating to an identified or identifiable individual" (OECD 2013). Examples are name, address, phone number, gender, identity number, e-mail address, ethnicity, political/religious beliefs affiliations, marital status and sexual orientation.

Definition 3: Personal information processing - "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as obtaining, recording or holding the data or carrying out any operation or set of operations on data, including (a) organisation, adaptation or alteration of data; (b) retrieval, consultation or use of the data; or (c) alignment, combination, blocking, erasure or destruction of data" (Zimbabwe. Data Protection Act bill 2013).

Information Privacy Perception Survey
September - October 2019

On the next page, please find the questionnaire. We estimate that it will take you around 15 minutes to complete it.

Please complete the survey in one session. Due to anonymity of the survey it cannot be book marked or saved and returned to later.

Thank you for your co-operation!

TECHNICAL DIFFICULTIES

For any **technical difficulties** please contact Ellen +27 00000 0000 or send an e-mail to: xxxxx@iafrica.com

Section 1: Biographical Information

We require some background information and would appreciate it if you would answer the following questions.

Instructions

Please provide one response to each item in the questionnaire.

Indicate your selection with a click in the circle.

Make sure a bullet appears in the circle that you select.

Section 1 - Biographical Information

1. Please indicate your age band

- 1996 - Date
- 1977 - 1995
- 1965 - 1976
- 1946 - 1964
- Born 1945 or earlier

2. Please indicate your Gender

- Male
- Female
- Other

3. Please indicate your Nationality

- Zimbabwean
- Another African Country
- European
- American
- Australian
- Asian
- Other

Information Privacy Perception Survey
September - October 2019

4. Please indicate your learning mode

- Conventional
- Parallel
- Block
- Other

5. Please indicate your year of study

- 1st year
- 2nd year
- 3rd year
- 4th year
- Master's
- Doctorate
- 6-month certificate

6. Please specify your programme

- BBM&IT
- BAcc
- BBM Finance
- BBM Marketing
- BA Dev Studies
- BA Dual Honours
- BA Theology
- MBA
- DPhil
- 6-month certificate
- Other

Section 2 - Personal information privacy: awareness, expectations and confidence questions

There are nine (9) components of the Student Personal Information Privacy Perception (SPIPP) questionnaire. Each will be measured in terms of the three dimensions, i.e. awareness, expectations and confidence.

To what extent do you agree or disagree with the following:

A - Notice/Openness

Awareness

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 7. I am aware that the university should publish a privacy notice (e.g. the privacy policy on the university website or privacy terms and conditions). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8. I am aware that the university's privacy notice should be easy to understand. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Expectations

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 9. I expect the university to publish a privacy notice. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10. I expect the university's privacy notice to be easily understood. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Information Privacy Perception Survey
September - October 2019

Confidence

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 11. I am confident that the university publishes a privacy notice. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 12. I am confident that the university's privacy notice is easy to understand. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

B - Information quality

Awareness

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 13. I am aware that the university should take reasonable steps to ensure that my personal information processed by them is correct (e.g. accurate, up to date, complete and relevant) for the purpose of collection. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 14. I am aware that the university should have a method whereby I can review my personal information to ensure that it is correct (e.g. accurate, up to date, complete and relevant). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Information Privacy Perception Survey
September - October 2019

Expectations

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 15. I expect the university to take reasonable steps to ensure that my personal information processed by them is correct (e.g. accurate, up to date, complete and relevant) for the purpose of collection. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 16. I expect the university to provide me with a method whereby I can review my personal information that they have collected to ensure that it is correct (e.g. accurate, up to date, complete and relevant). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Confidence

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 17. I am confident that the university takes reasonable steps to ensure that my personal information processed by them is correct (e.g. accurate, up to date, complete and relevant) for the purpose of collection. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 18. I am confident that the university provides me with a method whereby I can review my personal information that they have collected to ensure that it is correct (e.g. accurate, up to date, complete and relevant). | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

C - Purpose specification

Awareness

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 19. I am aware that the university should specify the purpose of collecting my personal information. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 20. I am aware that the purpose should be specified no later than at the point of collection. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Expectations

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 21. I expect the university to specify the purpose of collecting my personal information. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 22. I expect the purpose to be specified no later than at the point of collection. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Confidence

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 23. I am confident that the university specifies the purpose of collecting my personal information. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 24. I am confident that the purpose is specified no later than at the point of collection. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

D - Use limitation

Awareness

25. I am aware that the university should have reasonable justification (e.g. consent, a contract, legal requirement) for processing my personal information.

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

26. I am aware that my personal information should not be disclosed, made available or used, unless it is in line with the requirements of the law.

	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

27. I expect the university to have reasonable justification (e.g. consent, a contract, legal requirement) for processing my personal information.

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

28. I expect my personal information not to be disclosed, made available or used, unless it is in line with the law.

	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Confidence

29. I am confident that the university has reasonable justification (e.g. consent, a contract, legal requirement) for processing my personal information.

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

30. I am confident that my personal information has not been disclosed, made available or used, unless it is in line with the law.

	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

E - Collection limitation

Awareness

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
31. I am aware that the university should collect information lawfully, fairly and only for the specified purposes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
32. I am aware that the university should limit the collection of personal information (about religion, political party affiliation, health status, tribe, etc.) that is not necessary for academic purposes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Expectations

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
33. I expect the university to collect information lawfully, fairly and only for the specified purposes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
34. I expect the university to limit the collection of personal information (about religion, political party affiliation, health status, tribe, etc.) that is not necessary for academic purposes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Confidence

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
35. I am confident that the university collects information lawfully, fairly and only for the specified purposes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
36. I am confident that the university limits the collection of personal information (about religion, political party affiliation, health status, tribe, etc.) that is not necessary for academic purposes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

F - Individual participation

Awareness

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 37. I am aware that I should be able to request copies of the records of my personal information from the university. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 38. I am aware that the university should have a process whereby I can request whatever personal information the university has collected about me. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Expectations

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|--|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 39. I expect to be able to request copies of the records of my personal information from the university. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 40. I expect the university to have a process whereby I can request whatever personal information the university has collected about me. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Confidence

- | | Strongly disagree | Disagree | Do not agree or disagree | Agree | Strongly agree |
|---|-----------------------|-----------------------|--------------------------|-----------------------|-----------------------|
| 41. I am confident that I can request copies of the records of my personal information from the university. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 42. I am confident that the university has a process whereby I can request whatever personal information the university has collected about me. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Information Privacy Perception Survey
September - October 2019

G - Privacy policy

Awareness

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
43. I am aware that the university should have a privacy policy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
44. I am aware that the privacy policy should be easily understood.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Expectations

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
45. I expect the university to have a privacy policy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
46. I expect the privacy policy to be easily understood.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Confidence

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
47. I am confident that the university has a privacy policy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
48. I am confident that the privacy policy is easily understood.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Information Privacy Perception Survey
September - October 2019

H - Privacy education

Awareness

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
49. I am aware that the university should, as part of best practice, conduct privacy training for students.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
50. I am aware that the university should , as part of best practice, remind me continually of privacy issues through privacy education (e.g. privacy newsletters, magazines and notices).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Expectations

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
51. I expect the university to conduct privacy training for students.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
52. I expect the university to remind me continually of privacy issues through privacy education (e.g. privacy newsletters, magazines and notices).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Confidence

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
53. I am confident that the university conducts privacy training for students.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
54. I am confident that the university reminds me continually of privacy issues through privacy education (e.g. privacy newsletters, magazines and notices).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Information Privacy Perception Survey
September - October 2019

I - Consent

Awareness

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
55. I am aware that I should have the right to be able to opt in for (i.e. allow) the use of my personal information for other purposes (e.g. marketing, newsletters, job or product advertisements).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
56. I am aware that I should have the right to be able to opt out for (i.e. disallow) the use of my personal information for other purposes (e.g. marketing, newsletters, job or product advertisements), if I am no longer interested.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Expectations

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
57. I expect the university to enable me to exercise my right to opt in for the use of my personal information for other purposes (e.g. marketing, newsletters and job or product advertisements).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
58. I expect the university to enable me to exercise my right to opt out for the use of my personal information for other purposes (e.g. marketing, newsletters and job or product advertisements), if I am no longer interested.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Information Privacy Perception Survey
September - October 2019

Confidence

	Strongly disagree	Disagree	Do not agree or disagree	Agree	Strongly agree
59. I am confident that the university gives me the right to opt in for the use of my personal information for other purposes (e.g. marketing, newsletters, job or product advertisements).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
60. I am confident that the university gives me the right to opt out for the use of my personal information for other purposes (e.g. marketing, newsletters and job or product advertisements), if I am no longer interested.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Information Privacy Perception Survey
September - October 2019

Thank you for completing the survey!

Scroll to the bottom of the screen and click on **SU B M I T**

NOTES ON SUBMISSION:

1. Please make sure that you **click on Submit once only**.
2. If you receive a '**thank you**' message after submitting, your submission has been successful.
3. If you are unable to submit, or receive any other message, please do not close the file, wait a short while and then try to submit again.
4. If the submit button fails, please save your answers to a .pdf format and email to xxxxxx@iafrica.com
5. Contact details for technical difficulties: Ellen +27 00 000 0000 or send an e-mail to xxxxxx@iafrica.com .

Appendix F: Initial communalities for the 54 items

Communalities	
	Initial
Q12_S1: 12. I am confident that the university publishes a privacy notice.	.846
Q30_S1: 30. I am confident that the university has reasonable justification (e.g., consent, a contract, legal requirement) for processing my personal information.	.874
Q31_S1: 31. I am confident that my personal information has not been disclosed, made available or used, unless it is in line with the law.	.862
Q13_S1: 13. I am confident that the university's privacy notice is easy to understand.	.824
Q18_S1: 18. I am confident that the university takes reasonable steps to ensure that my personal information processed by them is correct (e.g., accurate, up to date, complete and relevant) for the purpose of collection.	.866
Q19_S1: 19. I am confident that the university provides me with a method whereby I can review my personal information that they have collected to ensure that it is correct (e.g., accurate, up to date, complete and relevant).	.827
Q24_S1: 24. I am confident that the university specifies the purpose of collecting my personal information.	.886
Q25_S1: 25. I am confident that the purpose is specified no later than at the point of collection.	.877
Q36_S1: 36. I am confident that the university collects information lawfully, fairly and only for the specified purposes.	.855
Q37_S1: 37. I am confident that the university limits the collection of personal information (about religion, political party affiliation, health status, tribe, etc.) that is not necessary for academic purposes.	.812
Q42_S1: 42. I am confident that I can request copies of the records of my personal information from the university.	.878
Q43_S1: 43. I am confident that the university has a process whereby I can request whatever personal information the university has collected about me.	.912
Q48_S1: 48. I am confident that the university has a privacy policy.	.900
Q49_S1: 49. I am confident that the privacy policy is easily understood.	.884
Q54_S1: 54. I am confident that the university conducts privacy training for students.	.960

issues through privacy education (e.g., privacy newsletters, magazines and notices).	
Q60_S1: 60. I am confident that the university gives me the right to opt in for the use of my personal information for other purposes (e.g., marketing, newsletters, job or product advertisements).	.901
Q61_S1: 61. I am confident that the university gives me the right to opt out for the use of my personal information for other purposes (e.g., marketing, newsletters and job or product advertisements), if I am no longer interested.	.928
Q8_S1: 8. I am aware that the university should publish a privacy notice (e.g., the privacy policy on the university website or privacy terms and conditions).	.441
Q9_S1: 9. I am aware that the university's privacy notice should be easy to understand.	.531
Q10_S1: 10. I expect the university to publish a privacy notice.	.636
Q11_S1: 11. I expect the university's privacy notice to be easily understood.	.617
Q14_S1: 14. I am aware that the university should take reasonable steps to ensure that my personal information processed by them is correct (e.g., accurate, up to date, complete and relevant) for the purpose of collection.	.780
Q15_S1: 15. I am aware that the university should have a method whereby I can review my personal information to ensure that it is correct (e.g., accurate, up to date, complete and relevant).	.698
Q16_S1: 16. I expect the university to take reasonable steps to ensure that my personal information processed by them is correct (e.g., accurate, up to date, complete and relevant) for the purpose of collection.	.680
Q17_S1: 17. I expect the university to provide me with a method whereby I can review my personal information that they have collected to ensure that it is correct (e.g., accurate, up to date, complete and relevant).	.597
Q20_S1: 20. I am aware that the university should specify the purpose of collecting my personal information.	.858
Q21_S1: 21. I am aware that the purpose should be specified no later than at the point of collection.	.851
Q22_S1: 22. I expect the university to specify the purpose of collecting my personal information.	.745
Q23_S1: 23. I expect the purpose to be specified no later than at the point of collection.	.839

Q26_S1: 26. I am aware that the university should have reasonable justification (e.g., consent, a contract, legal requirement) for processing my personal information.	.811
Q27_S1: 27. I am aware that my personal information should not be disclosed, made available or used, unless it is in line with the requirements of the law.	.870
Q28_S1: 28. I expect the university to have reasonable justification (e.g., consent, a contract, legal requirement) for processing my personal information.	.682
Q29_S1: 29. I expect my personal information not to be disclosed, made available or used, unless it is in line with the law.	.680
Q32_S1: 32. I am aware that the university should collect information lawfully, fairly and only for the specified purposes.	.786
Q33_S1: 33. I am aware that the university should limit the collection of personal information (about religion, political party affiliation, health status, tribe, etc.) that is not necessary for academic purposes.	.828
Q34_S1: 34. I expect the university to collect information lawfully, fairly and only for the specified purposes.	.783
Q35_S1: 35. I expect the university to limit the collection of personal information (about religion, political party affiliation, health status, tribe, etc.) that is not necessary for academic purposes.	.803
Q38_S1: 38. I am aware that I should be able to request copies of the records of my personal information from the university.	.882
Q39_S1: 39. I am aware that the university should have a process whereby I can request whatever personal information the university has collected about me.	.896
Q40_S1: 40. I expect to be able to request copies of the records of my personal information from the university.	.677
Q41_S1: 41. I expect the university to have a process whereby I can request whatever personal information the university has collected about me.	.753
Q44_S1: 44. I am aware that the university should have a privacy policy.	.793
Q45_S1: 45. I am aware that the privacy policy should be easily understood.	.825
Q46_S1: 46. I expect the university to have a privacy policy.	.770
Q47_S1: 47. I expect the privacy policy to be easily understood.	.754
Q50_S1: 50. I am aware that the university should, as part of best practice, conduct privacy training for students.	.880
Q51_S1: 51. I am aware that the university should, as part of best practice, remind me continually of privacy issues through privacy education (e.g., privacy newsletters, magazines and notices).	.855

Q52_S1: 52. I expect the university to conduct privacy training for students.	.849
Q53_S1: 53. I expect the university to remind me continually of privacy issues through privacy education (e.g., privacy newsletters, magazines and notices).	.831
Q56_S1: 56. I am aware that I should have the right to be able to opt in for (i.e., allow) the use of my personal information for other purposes (e.g., marketing, newsletters, job or product advertisements).	.919
Q57_S1: 57. I am aware that I should have the right to be able to opt out for (i.e., disallow) the use of my personal information for other purposes (e.g., marketing, newsletters, job or product advertisements), if I am no longer interested.	.929
Q58_S1: 58. I expect the university to enable me to exercise my right to opt in for the use of my personal information for other purposes (e.g., marketing, newsletters and job or product advertisements).	.853
Q59_S1: 59. I expect the university to enable me to exercise my right to opt out for the use of my personal information for other purposes (e.g., marketing, newsletters and job or product advertisements), if I am no longer interested.	.829
Extraction Method: Principal Axis Factoring.	

Appendix G: Summarised rotated pattern matrix for the eight-factors

<i>Item No</i>	Factor							
	1	2	3	4	5	7	8	
Factor 1: University Confidence								
q30	0.772							
q19	0.764							
q18	0.733							
q24	0.622							
q31	0.618							
q13	0.603							
q25	0.601							
q12	0.563							
Factor 2: Privacy Expectations								
q28		0.631						
q29		0.598						
q46		0.586						
q47		0.583						
q34		0.539						
q58		0.437						
q11		0.417						
Factor 3: Individual Awareness								
q56			-0.892					
q57			-0.868					
q27			-0.463					
q38			-0.445					
q39			-0.441					

<i>Item No</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>7</i>	<i>8</i>
Factor 4: External Awareness							
q20				-0.796			
q21				-0.677			
q26				-0.472			
Factor 5: Privacy Education							
q51					0.703		
q50					0.700		
q52					0.575		
q53					0.561		
Factor 7: Practice Confidence							
q61						-0.836	
q54						-0.805	
q60						-0.804	
q55						-0.740	
q43						-0.647	
q49						-0.576	
q48						-0.544	
q42						-0.526	
Factor 8: Expect Correctness							
q16							-0.753
q22							-0.630
q17							-0.575
q14							-0.532
q23							-0.478
q45							-0.451

Note: Extraction Method: Principal Axis Factoring.

Rotation Method: Oblimin with Kaiser Normalization.

^a Rotation converged in 25 iterations.

Appendix H: Correlation results

Correlations								
		UC	PE	IA	EA	PEd	PC	CE
UC	Pearson Correlation	1	0.096	.376**	.381**	.257**	.667**	.294**
	Sig. (2-tailed)		0.105	0.000	0.000	0.000	0.000	0.000
PE	Pearson Correlation	0.096	1	.205**	.182**	.185**	0.077	.436**
	Sig. (2-tailed)	0.105		0.000	0.002	0.002	0.196	0.000
IA	Pearson Correlation	.376**	.205**	1	.416**	.331**	.283**	.338**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000
EA	Pearson Correlation	.381**	.182**	.416**	1	.295**	.245**	.378**
	Sig. (2-tailed)	0.000	0.002	0.000		0.000	0.000	0.000
PEd	Pearson Correlation	.257**	.185**	.331**	.295**	1	.223**	.194**
	Sig. (2-tailed)	0.000	0.002	0.000	0.000		0.000	0.001
PC	Pearson Correlation	.667**	0.077	.283**	.245**	.223**	1	.180**
	Sig. (2-tailed)	0.000	0.196	0.000	0.000	0.000		0.002
CE	Pearson Correlation	.294**	.436**	.338**	.378**	.194**	.180**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.001	0.002	
**. Correlation is significant at the 0.01 level (2-tailed)								

Appendix I: Independent t-test for gender

Variable	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
University confidence	1.321	0.251	0.321	281	0.749	0.03431	0.10699
			0.321	279.793	0.748	0.03431	0.10689
Privacy expectations	0.688	0.407	-0.480	281	0.632	-0.02347	0.04890
			-0.480	279.859	0.631	-0.02347	0.04886
Individual awareness	2.917	0.089	-0.027	281	0.979	-0.00240	0.08906
			-0.027	275.336	0.979	-0.00240	0.08890
External awareness	0.860	0.355	-0.968	281	0.334	-0.08871	0.09166
			-0.967	276.804	0.334	-0.08871	0.09176
Privacy education	3.359	0.068	0.593	281	0.553	0.05202	0.08769
			0.594	272.895	0.553	0.05202	0.08751
Practice confidence	0.036	0.850	-0.192	281	0.848	-0.02021	0.10536
			-0.192	280.906	0.848	-0.02021	0.10532
Correction expectation	0.078	0.781	-1.605	281	0.110	-0.08655	0.05391
			-1.604	278.525	0.110	-0.08655	0.05396
Expectations test	0.139	0.709	-1.262	281	0.208	-0.05501	0.04358
			-1.262	280.694	0.208	-0.05501	0.04358

Appendix J: ANOVA test for age

Factor	Age	N	Mean	SD	SE	95% Confidence Interval for Mean		Min	Max
						Lower Bound	Upper Bound		
University confidence	1996-date	67	3.63	0.91	0.11	3.40	3.85	1.38	5.00
	1977-1995	177	3.55	0.90	0.07	3.41	3.68	1.25	5.00
	1965-1976	41	3.57	0.91	0.14	3.28	3.86	1.25	5.00
	Total	285	3.57	0.90	0.05	3.46	3.67	1.25	5.00
Privacy expectations	1996-date	67	4.60	0.42	0.05	4.50	4.71	2.88	5.00
	1977-1995	177	4.54	0.41	0.03	4.48	4.60	3.29	5.00
	1965-1976	41	4.55	0.40	0.08	4.43	4.68	3.71	5.00
	Total	285	4.56	0.41	0.02	4.51	4.61	2.88	5.00
Individual awareness	1996-date	67	4.03	0.82	0.10	3.83	4.23	1.80	5.00
	1977-1995	177	4.11	0.72	0.05	4.00	4.22	1.80	5.00
	1965-1976	41	4.01	0.82	0.13	3.75	4.27	2.40	5.00
	Total	285	4.08	0.78	0.04	3.99	4.16	1.80	5.00
External awareness	1996-date	67	4.02	0.79	0.10	3.83	4.21	1.87	5.00
	1977-1995	177	4.18	0.77	0.06	4.06	4.29	2.00	5.00
	1965-1976	41	4.16	0.76	0.12	3.92	4.40	1.87	5.00
	Total	285	4.14	0.77	0.05	4.05	4.23	1.87	5.00
Privacy education	1996-date	67	4.15	0.73	0.09	3.97	4.32	1.75	5.00
	1977-1995	177	4.11	0.75	0.06	3.99	4.22	2.00	5.00
	1965-1976	41	4.21	0.68	0.11	3.99	4.42	2.00	5.00
	Total	285	4.13	0.73	0.04	4.04	4.22	1.75	5.00
Practice confidence	1996-date	67	3.37	0.90	0.11	3.15	3.59	2.00	5.00
	1977-1995	177	3.41	0.89	0.07	3.28	3.54	1.83	5.00
	1965-1976	41	3.48	0.80	0.13	3.21	3.71	1.75	5.00
	Total	285	3.41	0.88	0.05	3.31	3.51	1.83	5.00
Correction expectation	1996-date	67	4.60	0.33	0.04	4.52	4.68	3.67	5.00
	1977-1995	177	4.51	0.47	0.03	4.45	4.58	2.33	5.00
	1965-1976	41	4.46	0.55	0.09	4.29	4.63	2.50	5.00
	Total	285	4.53	0.45	0.03	4.47	4.58	2.33	5.00
Expectations test	1996-date	67	4.60	0.33	0.04	4.52	4.68	3.43	5.00
	1977-1995	177	4.53	0.37	0.03	4.47	4.58	3.45	5.00
	1965-1976	41	4.51	0.41	0.08	4.38	4.64	3.46	5.00
	Total	285	4.54	0.37	0.02	4.50	4.58	3.43	5.00
Awareness test	1996-date	67	4.07	0.58	0.07	3.92	4.21	2.69	5.00
	1977-1995	177	4.13	0.57	0.04	4.05	4.21	2.80	5.00
	1965-1976	41	4.13	0.55	0.09	3.95	4.30	2.69	5.00
	Total	285	4.11	0.57	0.03	4.05	4.18	2.69	5.00
Confidence test	1996-date	67	3.50	0.85	0.10	3.29	3.70	1.75	5.00
	1977-1995	177	3.48	0.81	0.06	3.36	3.60	1.50	5.00

	1965-1976	41	3.52	0.78	0.12	3.27	3.78	1.50	5.00
	Total	285	3.49	0.81	0.05	3.39	3.58	1.50	5.00

Note: SD = standard deviation; SE = standard error

Factor		Sum of Squares	df	Mean Square	F	Sig.
University confidence	Between Groups	0.31	2	0.18	0.19	0.83
	Within Groups	231.89	282	0.82		
	Total	232.01	284			
Privacy expectations	Between Groups	0.19	2	0.09	0.55	0.58
	Within Groups	47.82	282	0.17		
	Total	47.80	284			
Individual awareness	Between Groups	0.48	2	0.24	0.42	0.66
	Within Groups	162.45	282	0.58		
	Total	162.93	284			
External awareness	Between Groups	1.20	2	0.60	1.02	0.36
	Within Groups	167.13	282	0.59		
	Total	168.33	284			
Privacy education	Between Groups	0.36	2	0.18	0.34	0.72
	Within Groups	152.96	282	0.54		
	Total	153.32	284			
Practice confidence	Between Groups	0.24	2	0.12	0.15	0.86
	Within Groups	217.88	282	0.77		
	Total	218.12	284			
Correction expectation	Between Groups	0.59	2	0.30	1.48	0.24
	Within Groups	57.53	282	0.20		
	Total	58.13	284			
Expectations test	Between Groups	0.33	2	0.17	1.25	0.29
	Within Groups	37.56	282	0.13		
	Total	37.89	284			
Awareness test	Between Groups	0.21	2	0.11	0.33	0.72
	Within Groups	91.49	282	0.32		
	Total	91.70	284			
Confidence test	Between Groups	0.05	2	0.02	0.04	0.96
	Within Groups	187.35	282	0.66		
	Total	187.400	284			

Appendix K: ANOVA test for mode of study

		N	Mean	SD	Std. Error	95% Confidence Interval for Mean		Mini	Maxi
						Lower Bound	Upper Bound		
University confidence	Conventional	141	3.59	0.81	0.07	3.46	3.73	1.25	5.00
	Parallel	89	3.57	1.03	0.11	3.35	3.79	1.25	5.00
	Block	47	3.65	0.88	0.13	3.39	3.91	2.13	5.00
	Total	277	3.59	0.89	0.05	3.49	3.70	1.25	5.00
Privacy expectations	Conventional	141	4.81	0.37	0.03	4.55	4.87	2.88	5.00
	Parallel	89	4.53	0.46	0.05	4.43	4.62	3.29	5.00
	Block	47	4.50	0.43	0.06	4.37	4.62	3.43	5.00
	Total	277	4.56	0.41	0.02	4.52	4.61	2.88	5.00
Individual awareness	Conventional	141	4.08	0.81	0.07	3.95	4.22	1.80	5.00
	Parallel	89	4.16	0.65	0.07	4.03	4.30	1.80	5.00
	Block	47	3.97	0.76	0.11	3.74	4.19	2.40	5.00
	Total	277	4.09	0.75	0.05	4.00	4.18	1.80	5.00
External awareness	Conventional	141	4.16	0.79	0.07	4.03	4.29	1.67	5.00
	Parallel	89	4.13	0.74	0.08	3.98	4.29	2.00	5.00
	Block	47	4.16	0.77	0.11	3.94	4.39	1.67	5.00
	Total	277	4.15	0.76	0.05	4.06	4.24	1.67	5.00
Privacy education	Conventional	141	4.04	0.79	0.07	3.91	4.17	1.75	5.00
	Parallel	89	4.25	0.68	0.07	4.11	4.39	2.50	5.00
	Block	47	4.11	0.68	0.10	3.91	4.31	2.75	5.00
	Total	277	4.12	0.74	0.04	4.03	4.21	1.75	5.00
Practice confidence	Conventional	141	3.39	0.85	0.07	3.25	3.53	1.75	5.00
	Parallel	89	3.39	0.83	0.10	3.20	3.59	1.75	5.00
	Block	47	3.61	0.88	0.13	3.36	3.87	1.63	5.00
	Total	277	3.43	0.88	0.05	3.32	3.53	1.63	5.00
Correction expectation	Conventional	141	4.57	0.38	0.03	4.51	4.63	2.50	5.00
	Parallel	89	4.49	0.49	0.05	4.39	4.60	2.33	5.00
	Block	47	4.49	0.56	0.08	4.32	4.65	2.50	5.00
	Total	277	4.53	0.45	0.03	4.48	4.58	2.33	5.00
Expectations test	Conventional	141	4.59	0.32	0.03	4.54	4.64	3.43	5.00
	Parallel	89	4.51	0.41	0.04	4.42	4.60	3.45	5.00
	Block	47	4.49	0.41	0.06	4.37	4.61	3.46	5.00
	Total	277	4.55	0.37	0.02	4.50	4.59	3.43	5.00
Awareness test	Conventional	141	4.09	0.58	0.05	4.00	4.19	2.69	5.00
	Parallel	89	4.18	0.54	0.06	4.07	4.30	2.87	5.00
	Block	47	4.08	0.56	0.08	3.92	4.24	2.69	5.00
	Total	277	4.12	0.57	0.03	4.05	4.19	2.69	5.00
	Conventional	141	3.49	0.74	0.06	3.37	3.62	1.50	5.00

Confidence test	Parallel	89	3.48	0.91	0.10	3.29	3.67	1.50	5.00
	Block	47	3.63	0.79	0.12	3.40	3.86	2.13	5.00
	Total	277	3.51	0.81	0.05	3.42	3.61	1.50	5.00

†

Factor		Sum of Squares	df	Mean Square	F	Sig.
University confidence	Between Groups	0.19	2	0.10	0.12	0.89
	Within Groups	219.66	274	0.80		
	Total	219.86	276			
Privacy expectations	Between Groups	0.61	2	0.31	1.82	0.16
	Within Groups	46.13	274	0.17		
	Total	46.74	276			
Individual awareness	Between Groups	1.22	2	0.61	1.08	0.34
	Within Groups	154.48	274	0.56		
	Total	155.70	276			
External awareness	Between Groups	0.03	2	0.02	0.03	0.97
	Within Groups	161.37	274	0.59		
	Total	161.40	276			
Privacy education	Between Groups	2.35	2	1.18	2.17	0.12
	Within Groups	148.85	274	0.54		
	Total	151.20	276			
Practice confidence	Between Groups	1.94	2	0.97	1.25	0.29
	Within Groups	212.53	274	0.78		
	Total	214.47	276			
Correction expectation	Between Groups	0.44	2	0.22	1.07	0.35
	Within Groups	56.49	274	0.21		
	Total	56.93	276			
Expectations test	Between Groups	0.52	2	0.26	1.95	0.14
	Within Groups	36.48	274	0.13		
	Total	37.00	276			
Awareness test	Between Groups	0.52	2	0.26	0.81	0.44
	Within Groups	87.69	274	0.32		
	Total	88.21	276			
Confidence test	Between Groups	0.82	2	0.41	0.62	0.54
	Within Groups	180.15	274	0.66		
	Total	180.96	276			

Appendix L: Spearman's rho for year of study

			6. Please indicate your year of study
Spearman's rho	6. Please indicate your year of study	Correlation Coefficient	1.000
		Sig. (2-tailed)	
	University confidence	Correlation Coefficient	-0.181
		Sig. (2-tailed)	0.002
	Privacy expectations	Correlation Coefficient	0.043
		Sig. (2-tailed)	0.469
	Individual awareness	Correlation Coefficient	-0.044
		Sig. (2-tailed)	0.459
	External awareness	Correlation Coefficient	-0.128
		Sig. (2-tailed)	0.031
	Privacy education	Correlation Coefficient	-0.036
		Sig. (2-tailed)	0.546
	Practice confidence	Correlation Coefficient	-0.078
		Sig. (2-tailed)	0.190
	Correction expectation	Correlation Coefficient	-0.014
		Sig. (2-tailed)	0.807
	Expectations test	Correlation Coefficient	0.019
		Sig. (2-tailed)	0.753
	Awareness test	Correlation Coefficient	-0.120
		Sig. (2-tailed)	0.042
Confidence test	Correlation Coefficient	-0.142	
	Sig. (2-tailed)	0.016	

Appendix M: ANOVA test for programme of study

Post Hoc Tests							
Multiple Comparisons							
Scheffe							
Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
External_awareness	BBM and IT	B Acc and BBM finance	0.12827	0.14388	0.939	-0.3181	0.5747
		BBM marketing	0.23476	0.20474	0.859	-0.4005	0.8700
		BA Dev studies	-0.43570	0.17749	0.201	-0.9864	0.1150
		BA Dual Honours /D. Phil	-0.12101	0.16502	0.970	-0.6330	0.3910
	B Acc and BBM finance	BBM and IT	-0.12827	0.14388	0.939	-0.5747	0.3181
		BBM marketing	0.10848	0.23488	0.995	-0.6223	0.8352
		BA Dev studies	-0.56397	0.21155	0.134	-1.2203	0.0924
		BA Dual Honours /D.Phil	-0.24929	0.20119	0.820	-0.8735	0.3749
	BBM marketing	BBM and IT	-0.23476	0.20474	0.859	-0.8700	0.4005
		B Acc and BBM finance	-0.10848	0.23488	0.995	-0.8352	0.6223
		BA Dev studies	-0.87045	0.25885	0.150	-1.4673	0.1284
		BA Dual Honours /D. Phil	-0.35577	0.24839	0.726	-1.1264	0.4149
	BA Dev studies	BBM and IT	0.43570	0.17749	0.201	-0.1150	0.9864
		B Acc and BBM finance	0.56397	0.21155	0.134	-0.0924	1.2203
		BBM marketing	0.87045	0.25885	0.150	-0.1264	1.4673
		BA Dual Honours /D. Phil	0.31469	0.22845	0.748	-0.3879	1.0173
	BA Dual Honours /D. Phil	BBM and IT	0.12101	0.16502	0.970	-0.3910	0.6330
		B Acc and BBM finance	0.24929	0.20119	0.820	-0.3749	0.8735
		BBM marketing	0.35577	0.24839	0.726	-0.4149	1.1264
		BA Dev studies	-0.31469	0.22845	0.748	-1.0173	0.3879
Practice_confidence	BBM and IT	B Acc and BBM finance	-0.25559	0.16137	0.644	-0.7562	0.2451
		BBM marketing	-0.38319	0.22963	0.595	-1.0956	0.3293
		BA Dev studies	-0.46203	0.19907	0.253	-1.0796	0.1556
		BA Dual Honours /D. Phil	0.07294	0.18507	0.997	-0.5013	0.6471
	B Acc and BBM finance	BBM and IT	0.25559	0.16137	0.644	-0.2451	0.7562
		BBM marketing	-0.12760	0.26343	0.994	-0.9449	0.6897
		BA Dev studies	-0.20844	0.23726	0.944	-0.9426	0.5297
		BA Dual Honours /D. Phil	0.32853	0.22565	0.714	-0.3716	1.0286
	BBM marketing	BBM and IT	0.38319	0.22963	0.595	-0.3293	1.0956
		B Acc and BBM finance	0.12760	0.26343	0.994	-0.6897	0.9449

		BA Dev studies	-0.07884	0.28807	0.999	-0.9726	0.8149
		BA Dual Honours /D. Phil	0.45613	0.27858	0.613	-0.4082	1.3205
	BA Dev studies	BBM and IT	0.46203	0.19907	0.253	-0.1556	1.0796
		B Acc and BBM finance	0.20644	0.23726	0.944	-0.5297	0.9426
		BBM marketing	0.07884	0.28807	0.999	-0.8149	0.9726
		BA Dual Honours /D. Phil	0.53497	0.25398	0.353	-0.2530	1.3230
	BA Dual Honours /D. Phil	BBM and IT	-0.07294	0.18507	0.997	-0.6471	0.5013
		B Acc and BBM finance	-0.32853	0.22565	0.714	-1.0286	0.3716
		BBM marketing	-0.45613	0.27858	0.613	-1.3205	0.4082
		BA Dev studies	-0.53497	0.25398	0.353	-1.3230	0.2530
Expectations_test	BBM and IT	B Acc and BBM finance	0.10488	0.06496	0.626	-0.0967	0.3084
		BBM marketing	-0.02996	0.09244	0.999	-0.3168	0.2568
		BA Dev studies	-0.16950	0.08014	0.348	-0.4181	0.0791
		BA Dual Honours /D. Phil	0.12795	0.07450	0.567	-0.1032	0.3591
	B Acc and BBM finance	BBM and IT	-0.10488	0.06496	0.626	-0.3084	0.0967
		BBM marketing	-0.13484	0.10605	0.806	-0.4639	0.1942
		BA Dev studies	-0.27438	0.09551	0.086	-0.5707	0.0220
		BA Dual Honours /D. Phil	0.02307	0.09084	0.999	-0.2588	0.3049
	BBM marketing	BBM and IT	0.02996	0.09244	0.999	-0.2588	0.3168
		B Acc and BBM finance	0.13484	0.10605	0.806	-0.1942	0.4639
		BA Dev studies	-0.13954	0.11597	0.836	-0.4993	0.2203
		BA Dual Honours /D. Phil	0.15791	0.11215	0.739	-0.1900	0.5059
	BA Dev studies	BBM and IT	0.16950	0.08014	0.348	-0.0791	0.4181
		B Acc and BBM finance	0.27438	0.09551	0.086	-0.0220	0.5707
		BBM marketing	0.13954	0.11597	0.836	-0.2203	0.4993
		BA Dual Honours /D. Phil	0.29745	0.10224	0.079	-0.0198	0.6147
	BA Dual Honours /D. Phil	BBM and IT	-0.12795	0.07450	0.567	-0.3591	0.1032
		B Acc and BBM finance	-0.02307	0.09084	0.999	-0.3049	0.2588
		BBM marketing	-0.15791	0.11215	0.739	-0.5059	0.1900
		BA Dev studies	-0.29745	0.10224	0.079	-0.6147	0.0198

Appendix N: Author's publications

The following publications were produced by the author from this thesis. All these papers were peer-reviewed:

1. **Maguraushe K.**, Da Veiga A. & Martins N. (2020) Validation of an Information Privacy Perception Instrument at a Zimbabwean University. In: *Clarke N., Furnell S. (eds) Human Aspects of Information Security and Assurance. HAISA 2020. IFIP Advances in Information and Communication Technology*, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_23
2. **Maguraushe K.**, Da Veiga A. & Martins N. (2019) A conceptual model for student personal information privacy culture in Zimbabwe universities, *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019*, Volume 12, pages 143--156, Published in Kalpa Publications in Computing ISSN: 2515-1762, Available at: <https://easychair.org/publications/paper/kgNN>. 31 October – 1 November 2019, Johannesburg, South Africa

Validation of an information privacy perception instrument at a Zimbabwean university

Kudakwashe Maguraushe ¹[0000-0003-2405-564X], Adèle da Veiga ²[0000-0001-9777-8721], and Nico Martins ³[0000-0002-6103-0217]

School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa

¹kmagraushe@gmail.com, ²dveiga@unisa.ac.za, ³martin@unisa.ac.za

Abstract

Privacy issues extend to students as universities acquire and use their personal information for various reasons. This research study was aimed at determining the awareness, expectations and confidence levels of students when the university processes their personal information. The research was also aimed at validating the Information Privacy Perception Survey (IPPS) instrument. The instrument was designed based on the Fair Information Practice Principles, incorporating privacy principles and guidelines from the Organisation for Economic Cooperation and Development's Protection of Privacy and Transborder Flows of Personal Data document, the General Data Protection Regulation and the Zimbabwe Data Protection Act bill. A survey research strategy was used following a quantitative research design where data were collected from 287 students at a selected university using a convenience sampling method. The IPPS instrument was validated using exploratory factor analysis. Seven factors resulted; university confidence, privacy expectations, individual awareness, external awareness, privacy education, practice confidence and correctness expectations. The IPPS can be used by universities to establish the level of awareness and confidence students have regarding how their privacy is upheld by the university. The results show the areas of improvement in the university's privacy practices to create an environment that instils and favours upholding the privacy of students' personal information. Aspects for improvement can be integrated in the university's awareness programmes or policies.

Keywords: Privacy, personal information, expectations, awareness, confidence, questionnaire

1 Introduction

Privacy of personal information differs from country to country and many nations now have privacy laws aligned to the international privacy principles [1]. This research focuses on privacy expectations, student privacy awareness and confidence levels of students in universities' capability to uphold privacy values. The protection of privacy within the Zimbabwean context is partly enshrined in the constitution, although there is no prescription on how it will be executed and enforced [2]. This led to the drafting of the Zimbabwe Data Protection Act (ZDPA) bill with the objective of guiding and

protecting the privacy of personal information of individuals/people and organisations/institutions [3], [4].

Many studies have been carried out on privacy, privacy breaches and concerns, privacy compliances, privacy culture, privacy practices, privacy and trust, privacy when online, privacy in eLearning environments, and all this was done in industries, the health sector, for consumers and for employees of organisations [5]–[9]. According to [10], it is not easy and clear as yet within the Zimbabwean context to comprehend the privacy expectations of students, their privacy awareness levels and their confidence in the university's ability to uphold the privacy of their personal information.

The objectives of this research were to determine the awareness, expectations and confidence levels of students when the university processes their personal information and to validate the Information Privacy Perception Survey (IPPS) instrument using factor and item analysis.

2 Background

Privacy has been defined [11] in terms of the confined mentality of individuals that it is always limited to the ability to access personal data and the impact of self-disclosure, especially on the internet. This is in line with the privacy definition that privacy is “the ability of an individual to control the terms under which their personal information is acquired and used” [12]. Privacy of students personal information at universities is now equally important, especially in the digital context where information can be collected anytime from anywhere [13]. According to research [10], it is important that a university has measures that help in improving students' personal information protection after grasping their awareness, expectations and confidence levels in privacy-related issues.

2.1 Privacy awareness

Students' awareness of their privacy rights, university privacy policies and university awareness programmes is prudent. Awareness provides a perception about a situation, similar to notice, which is one of the fundamental Fair Information Practice Principles (FIPPs) for information privacy [14]. The awareness is normally concealed through privacy notices by the university [14]. So it follows that students, as users, also need to be aware of the importance of awareness about their privacy rights and university privacy policies, especially when using electronic means [15]. University compliance with the privacy policies, as alluded to by [16] and [17], goes hand in hand with awareness because a lack of awareness means that a user is not privy to the finer details needed to comply, which may result in non-compliance with privacy issues even by the student. Research [18] has shown that awareness of privacy can also be used in creating an atmosphere where all students are knowledgeable about all privacy-related issues, which also assists in their participation in university-related tasks. This must be initiated by universities through the use of privacy policies and other awareness means. As acclaimed by [17], institutions are indebted in making sure that students are aware of

the legal, moral and ethical expectations when they share their personal information and one way of accomplishing that is through countless and timeous awareness campaigns.

Awareness is typically conducted within organisations (universities) through privacy notices [14]. Research results [19] indicated students' lack of knowledge in appreciating privacy awareness within universities. Awareness is deemed a precondition for achieving compliance, as indicated by [20]. Results [21] also indicated that compliance to laws, privacy policies and privacy concerns are an end product of appropriate awareness lineups in organisations. Universities need to stimulate privacy awareness, which permits students to consent, particularly when handling personal information [22]. The Zimbabwean constitution declares that it is the prerogative of the data controller (university, in this case) to propagate and publicise knowledge, and hence awareness, to students [8].

2.2 Privacy expectations

FIPPs claim that individuals (students) expect privacy of their personal information [23]. There is an expectation that the collection of personal information will be as minimal as possible and relevant to the purpose of collection, even when there is a requirement that the organisation (university) acquire personal information and process it [23]. Research results [6] point to the fact that consumers regard organisations (institutions) with expectations of privacy when they process their personal information. In the event that the consumers (students) start to perceive the organisation (university) as having shortfalls in meeting their privacy expectations, they tend to become impassioned and consequently and might reject personal information sharing with the data collector (university) [24].

2.3 Privacy confidence

It was proved that sometimes students do not have a need to seek documentation related to privacy from the university because they have full confidence in their institutions upholding privacy [7]. According to [25], a sense of trust that implants confidence is strengthened if universities make privacy pledges which will eventually create a privacy culture that saturates the whole university as an institution. Research [26] corroborated by [27] indicated that trust is an element of confidence, which is to be tested within this research to validate its relevance for students' expectations and awareness. This implies that if privacy regulations and protection are improved and prioritised, the confidence levels of the users (students) will increase proportionally [28]. The lack of trust in using personal information can have negative implications like low confidence levels of students in the university [26], [29]. This was also emphasized by [27], which indicated that it would have undesirable retrogressive consequences. Low confidence levels in the business (university) by customers (students) can be a result of data and privacy breaches [30]. In the end, it is the mandate of the university to come up with privacy policies and make the students knowledgeable about it in a bid to increase confidence and compliance with the privacy policies [31]. The

implementation of an information privacy culture within institutions inspires trust and hence confidence as attested by [29].

3 Methods

This research study was conducted using a survey research strategy in a deductive approach of a quantitative research design. The questionnaire survey was used as a research method to gather information on students' perceptions and behaviour [32]. In terms of ethics [33], surveys tend to have the advantage of not exposing participants as it can be anonymous. The online distribution of a questionnaire is fast, inexpensive, with moderately faster turnaround time, easier administration and easy follow-ups, which all help to increase the reliability of the instrument since many responses reveal more detail [34]. Furthermore, most quantitative research adopts the survey design, as posited by [35]. Online surveys were chosen and according to [35], surveys are efficient and effective when the respondents are all information technology literate and have access to the internet, like in the case of students in this research.

3.1 Questionnaire

The quantitative IPPS instrument was developed with a set of 54 items based on a theoretical framework [10], all perceived to be of similar value, to which the respondents responded by agreeing or disagreeing with each item or statement. A five-point Likert scale was used with options being strongly disagree, disagree, do not disagree or agree, agree and strongly agree. After using theories from the literature to design the statements, the statements were subjected to a process of expert panel review. The experts assisted by undertaking a focused and comprehensive review of the questions, structure of the questionnaire and its suitability, and provided feedback or made recommendations [35], [36]. The expert review panel consisted of four people with experience in privacy consultancy, data protection, privacy compliance and privacy advisory services. The experts recommended the restructuring of some questions for clarity and some statements which were deemed inessential were adjusted.

After the expert review, the instrument was used with a total of 15 students in a pilot study. The purpose was to make sure that the statements were clear, easily understood and comprehensive. A pilot study helps in assessing if the questions are comprehensible to the targeted audience, ensuring that the instrument used in the study is reliable and valid measures of the constructs of interest (i.e. face and construct validity) [37]. After the pilot study, the time was reduced from 20 to 15 minutes. Also, clarity was added to reduce the notion that some questions were repeated, since each statement was assessed from the three dimensions of awareness, expectations and confidence. A statement was consequently added to the instrument to this effect.

In the design of the IPPS, an introduction with a preface and some privacy definitions used in the research study were included in the front section. The research instrument was divided into two sections that would assist in achieving the stated purpose of the study: Section 1: Biographical Information and Section 2: Personal information privacy

– Awareness, expectations and confidence questions. Section 1 required personal information such as the age, gender, nationality, learning mode, year of study and programme. Section 2 contained nine components of the questionnaire. Each was measured in terms of the three dimensions (i.e. awareness, expectations and confidence). The nine components used the FIPPs as the baseline and were underpinned in the OECD's Protection of Privacy and Transborder Flows of Personal Data document of 2013, the General Data Protection Regulation and the Zimbabwe Data Protection Act [10].

3.2 Sampling

Students at a university in Zimbabwe were selected as the sample by virtue of them being registered students. The sample size was derived using the rule of thumb suggested by [32], multiplying the five-point scale with the number of items in the questionnaire in order to have enough responses to statistically validate the questionnaire. This gives the minimum number of responses expected from the respondents in the research. For the sample size, 270 was the minimum number of students required to participate. A non-probability sampling technique was used for the survey. The researchers chose purposive sampling for the selection of experts to participate in the expert panel research on the survey questions. The experts were recruited based on their expertise in the field of information privacy. The researchers also chose convenience sampling for the pilot study participants because it allows for a quicker way of obtaining the data since the researcher picks "whomever is convenient as a participant in the study" [38]. For the final survey, the convenience sampling method was considered the most appropriate [35], [39]. Two hundred and seventy eight students participated in the survey, which was an adequate sample. The researcher recruited the participants by means of a presentation to the students highlighting the purpose of the research and also seeking their participation. Participation in the research was voluntary, anonymous and confidential.

3.3 Questionnaire administration

In this research study, an invitation with a hyperlink to the html questionnaire was sent to the respondents through email as the primary method for sending out the survey. Hard-copy questionnaires were provided to some students who indicated their unavailability on the internet. The estimated completion time for the questionnaire was approximately 15 minutes and the collection period was five weeks. The electronic/online IPPS was administered using the Survey Tracker software [40]. There was a "Yes" and a "No" button to the questionnaire where the students could click on "Yes" if they consented to continue to participating and move to the next page or "No" if they no longer wanted to participate and it would move to the last page.

3.4 Data analysis

The data analysis was done using SPSS version 25 for the descriptive statistics per subscale (such as the means and standard deviations) and for the questionnaire

validation using the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's Test of Sphericity (BTS), factor analysis and Cronbach alpha analysis.

4 Results

The results of the responses per age band are shown in Table 1.

Table 1: Survey responses

Response	Frequency	Percentage
1996–2019	67	23.3
1977–1995	177	61.7
1965–1976	41	14.3
1946–1964	1	0.3
Born 1945 or earlier	1	0.3
No response	0	0.0

Of the 287 responses, 143 were female and 140 male respondents with four who selected the "Other" option. 284 were Zimbabweans and three were from other African countries.

4.1 Validation of measurement instrument

The collected data was first subjected to the KMO to measure the sampling adequacy and the BTS to ascertain the presence of correlations and significance among the variables [41]. The BTS is considered significant at the level of $p < 0.05$ [41].

Table 2: Test for sample adequacy and significance

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.647
Bartlett's Test of Sphericity	Approx. Chi-Square	231.517
	df	6.000
	Sig.	0.000

In this research, a KMO value of 0.647 was obtained – greater than the threshold value of 0.60 postulated by [41], [42], implying that there was a strong correlation structure. The BTS was significant at $p < 0.00$ for overall significance for the awareness, expectations and confidence concepts, adding further evidence of sampling validity and the conduct of exploratory factor analysis (EFA). The value showed that a meaningful factor analysis could be conducted, as attested to by [43].

4.2 Factor analysis

The IPPS was subjected to the EFA using the principal axis factoring with Oblimin rotation with Kaiser normalisation. The rotated pattern matrix for the 54-item instrument is shown in Table 3 in Appendix A.

In research, items with factor loadings that are less than the agreed threshold (≤ 0.40) [43] and those with cross loadings that are high (with < 0.20 difference) in a single factor are eliminated. In this research, items with lower factor loadings but above the cut-off loading included items 11, 23, 26, 27, 36, 38, 39, 45, 58 and 59. They were all retained except item 59, which had a cross loading together with item 41 which were excluded. Factor 6 had two items and therefore it was excluded. Furthermore, the Cronbach alpha of factor 6 was very low (0.225), which falls outside the cut-off Cronbach value (≥ 0.7).

The new factors were labelled based on the items in the respective factors. The Cronbach alpha measures the internal consistency of a scale [43]. The Cronbach alpha values for the new factors, number of items and the Cronbach alpha are shown in Table 4 below.

Table 4: Cronbach alpha values for the new factors

Factor/Dimension	Number of items	Cronbach alpha
Factor 1: University confidence (UC)	8	0.922
Factor 2: Privacy expectations (PE)	7	0.789
Factor 3: Individual awareness (IA)	5	0.820
Factor 4: External awareness (EA)	3	0.807
Factor 5: Privacy education (PE)	4	0.737
Factor 6 (eliminated factor)	2	0.225
Factor 7: Practice confidence (PC)	8	0.917
Factor 8: Correctness expectations (CE)	6	0.781
Total	43	

The final seven factors had Cronbach alpha coefficient values that were higher than 0.7, which indicated that there was a strong item covariance [32], [35] of between 0.7 and 0.9, rendering the values adequate as posited by [34]. This resulted in the Cronbach alpha values being considered suitable and adequate for the purpose of this study. The Cronbach alpha values for factor 6 (eliminated factor) was very low, with a loading of 0.225, and thus it was removed. An extract of the questionnaire statements per factor is shown in Table 5.

Table 5: Questionnaire statements extract for the new factors

New Factor	Statement	Component examined
University Confidence	I am confident that the university has reasonable justification (e.g. consent, a contract, legal requirement) for processing my personal information.	Use limitation
	I am confident that the university's privacy notice is easy to understand.	Notice/ openness
Privacy Ex- pectations	I expect my personal information not to be disclosed, made available or used, unless it is in line with the law.	Use limitation
	I expect the privacy policy to be easily understood.	Privacy policy
Individual Awareness	I am aware that I should be able to request copies of the records of my personal information from the university.	Individual participation
	I am aware that the university should have a process whereby I can request whatever personal information the university has collected about me.	Individual participation
External Awareness	I am aware that the university should specify the purpose of collecting my personal information.	Purpose specification
	I am aware that the purpose should be specified no later than at the point of collection.	Purpose specification
Privacy Edu- cation	I am aware that the university should, as part of best practice, conduct privacy training for students.	Privacy education
	I expect the university to conduct privacy training for students.	Privacy education
Practice Con- fidence	I am confident that the university conducts privacy training for students.	Privacy education
	I am confident that the privacy policy is easily understood.	Privacy policy
Expect Cor- rectness	I expect the university to take reasonable steps to ensure that my personal information processed by them is correct (e.g. accurate, up to date, complete and relevant) for the purpose of collection.	Information quality
	I expect the university to specify the purpose of collecting my personal information.	Purpose specification

4.3 Means and standard deviations of the factors interpretation

Research conducted by [44] used an average of 4.0 as a threshold for distinguishing between positive and potential negative perceptions given the importance of privacy and information security together with the legal requirements for privacy, and this was used as a baseline for this research. Table 6 shows the mean and the standard deviation values for the final seven factors.

Table 6: Mean and standard deviation values for the final seven factors

Descriptive statistics					
Factor	N	Min	Max	Mean	Std deviation
University confidence	287	1.25	5.00	3.5740	0.90282
Privacy expectations	287	2.86	5.00	4.5610	0.41050
Individual awareness	287	1.80	5.00	4.0774	0.75485
External awareness	287	1.67	5.00	4.1429	0.77054
Privacy education	287	1.75	5.00	4.1254	0.73406
Practice confidence	287	1.63	5.00	3.4194	0.88332
Correction expectation	287	2.33	5.00	4.5296	0.45205
Valid N (listwise)	287				

Using the cut-off value adopted from [44] as the baseline, the following were observed:

- A mean value of 4.56 was recorded for the privacy expectations (factor 2), which is more than the cut-off value of 4.0 prescribed. It shows that students had positive perceptions about how the university handled and used their personal information.
- Correction expectation (factor 8) showed a mean value of 4.53, which was also considered to be highly positive in terms of students' perceptions.
- External awareness (factor 4) recorded a mean value of 4.14. This also shows positive perceptions.
- Privacy education (factor 5) recorded a mean value of 4.13, which is also above the cut-off value. This also shows positive perceptions of students.
- Individual awareness (factor 3) recorded a mean value of 4.08, showing slightly positive perceptions of students.
- University confidence (factor 1) scored 3.57, which is lower than the cut-off mean value. This shows that the perceptions of confidence and the confidence in the university could be improved.
- The lowest mean value was recorded under practice confidence (factor 7) with a value of 3.43. This represents the most negative dimension, for which improvement was required.

From the results, it can be drawn that privacy expectations and correction expectation are meaningful factors which are pivotal for the development of personal information privacy for a university, resulting in students developing confidence with the university in upholding the privacy of their personal information.

5 Discussion

The results show that the students had both positive and negative perceptions about how the university handled and used their personal information. Based on the research instrument used, the students had positive perceptions and expectations of privacy components like the use limitation, privacy policy, collection limitation, consent and notice/openness privacy components. These included the expectation and awareness that the university would justify the need for information collection and processing, confidence to be given, the provision to review collected personal information, confidence in the existence of the publishing privacy notices and privacy policy, and that these would be easy to comprehend.

The students had positive perceptions on the correction expectations. This focused on students' expectations of the university, on how the university had to come up with privacy policies and notices that were easily understandable, that the university would only use students' personal information for extreme scenarios like legal requirements and that this would be done with the students' consent. They expected the university to justify the collection and processing of their personal information, the information should not be just disclosed. Students also seemed to be aware of what they needed to do individually to uphold the privacy of their personal information. Individual awareness recorded positive perceptions by students in terms of consent, use limitation and individual participation. These included being aware of when to opt in for the use of their personal information, their rights to opt out in case they no longer chose to share their personal information and being aware that they had the right to decide who to share their personal information with. The university can focus on increasing the students' individual awareness levels by engaging in privacy training sessions, sending short message service (sms) or emails, letters and other notices.

External awareness also showed positive perceptions. This revealed perceptions about students' awareness levels in specifying the purpose of collection and the limitations of information use thereof. Students seemed to be aware and expected the university to remind them continuously of privacy-related issues through privacy newsletters, magazines, notices and so on as part of privacy best practices. Students were aware and expected the university to conduct privacy training to increase their privacy awareness.

The results showed that practice confidence was an area needing improvement, especially in terms of how to handle consent, privacy education, individual participation and privacy policy. Another area of improvement could be the university's privacy practices in creating an environment that favours the upholding of privacy of personal information. The university has to improve and create an environment that instils student confidence in the university regarding privacy.

The contribution is the identification of the factors and validation of the questionnaire. Further more the questionnaire can aid universities to identify how to further improve student awareness about privacy to be in line with their expectations. This will ultimately aid in better protection of student personal information also aiding in addressing concerns for information privacy amongst students.

6 Limitations and future research

This research was conducted on one institution. In future, research will aim to extend the study to wider sample of universities. There is also need to validate the conceptual framework using structural equation modelling (SEM).

7 Conclusion

An IPPS questionnaire was developed for this research to measure the expectations, awareness and confidence of students in the university upholding the privacy of their personal information. After the questionnaire was used at a university in Zimbabwe, the data obtained was used to validate it by means of the EFA. The results from the validated instrument led to the formulation of seven new factors. The questionnaire can be used by other universities to measure and improve the privacy awareness and confidence based on the expectations of students thereby aiding to improve the protection of personal information

Acknowledgement - The researchers are grateful to Organisational Diagnostics for hosting the survey and Liezel Korf Associates for assisting in the statistical analysis. This research paper is wholly supported by Unisa's Master's and Doctoral Research Bursary funding.

Appendix A

Table 3: Rotated pattern matrix for the eight-factor model

Item number	Factor							
	1	2	3	4	5	6	7	8
q30	0.77							
q19	0.76							
q18	0.73							
q24	0.62							
q31	0.62							
q13	0.60							
q25	0.60							
q12	0.56							
q28		0.63						
q29		0.60						
q46		0.59						
q47		0.58						
q34		0.54						

Item Number	1	2	3	4	5	6	7	8
q58		0.44						
q11		0.42						
q56			-0.89					
q57			-0.87					
q27			-0.46					
q38			-0.45					
q39			-0.44					
q20				-0.80				
q21				-0.68				
q26				-0.47				
q59			-0.40	0.47				
q51					0.70			
q50					0.70			
q52					0.58			
q53					0.56			
q41		0.46				0.61		
q40						0.56		
q36						0.40		
q61							-0.84	
q54							-0.81	
q60							-0.80	
q55							-0.74	
q43							-0.65	
q49							-0.58	
q48							-0.54	
q42							-0.53	
q16								-0.75
q22								-0.63
q17								-0.58
q14								-0.53
q23								-0.48
q45								-0.45
Extraction method: Principal axis factoring								
Rotation method: Oblimin with Kaiser normalization								
a. Rotation converged in 25 iterations								

References

- [1] D. L. A. Piper (2020) Data protection laws of the world, Attorney Advertising, [Online]. Available: <https://www.dlapiperdataprotection.com/index.html>.
- [2] Republic of Zimbabwe (2013) Constitution of the Republic of Zimbabwe 2013.
- [3] Chetty P (2013) Presentation on Zimbabwe Data Protection Bill, Harmon. ICT Policies Sub-Sahara Africa.
- [4] Zimbabwe Data Protection Act Bill (2013) The Zimbabwe Data Protection Act Bill. Harare, Zimbabwe, pp. 1–47.
- [5] Ivanova M, Grosseck G, Holotescu C (2015) Researching data privacy in eLearning, in 2015 International Conference on Information Technology-Based Higher Education and Training (ITHET), pp. 1–6.
- [6] Da Veiga A (2018) An information privacy culture instrument to measure consumer privacy expectations and confidence, *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 338–364.
- [7] Stange C (2011) Privacy concern and student engagement in the virtual classroom, *Univ. Victoria*, pp. 1–73.
- [8] Chua HN, Herbland A, Wong SF, Chang Y (2017) Compliance to personal data protection principles: A study of how organizations frame privacy policy notices, *Telemat. Informatics*, vol. 34, no. 4, pp. 157–170.
- [9] Katurura M, Cilliers L (2016) The extent to which the POPI Act makes provision for patient privacy in mobile personal health record systems, in Conference, IST-Africa 2015, pp. 1–8.
- [10] Maguraushe K, Da Veiga A, Martins N (2019) A conceptual framework for a student personal information privacy culture at universities in Zimbabwe, *Kalpa Publ. Comput.*, vol. 12, pp. 143–156.
- [11] Miltgen CL (2009) Online consumer privacy concerns and willingness to provide personal data on the internet, *Int. J. Netw. Virtual Organ.*, vol. 6, no. 6, p. 574.
- [12] Schwaig SK, Kane GC, Storey VC (2006) Compliance to the fair information practices : How are the Fortune 500 handling online privacy disclosures? *Inf. Manag.*, vol. 43, no. 7, pp. 805–820.
- [13] Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Comput. Secur.*, vol. 64, pp. 122–134.
- [14] Vail MW, Earp JB, Antón AL (2008) An empirical study of consumer perceptions and comprehension of web site privacy policies, *IEEE Trans. Eng. Manag.*, vol. 55, no. 3, pp. 442–454.
- [15] Kyobe M (2010) Knowledge management using information technology: Ethical and legal issues in a university, *Inf. Soc. Int. Conf.*, pp. 592–597.
- [16] Botha JG, Eloff MM, Swart I (2015) The effects of the POPI Act on small and medium enterprises in South Africa, 2015 *Inf. Secur. South Africa – Proc. ISSA 2015 Conf.*
- [17] Kyobe M (2010) Towards a framework to guide compliance with IS security policies and regulations in a university, *Proc. 2010 Inf. Secur. South Africa Conf. ISSA 2010*.
- [18] Fink C (2012) Privacy and confidentiality in the virtual classroom : Instructor

- perceptions, knowledge and strategies.
- [19] Chen LF, Ismail R (2013) Information technology program students' awareness and perceptions towards personal data protection and privacy, in *International Conference on Research and Innovation in Information Systems (ICRIIS)*, vol. 2013, pp. 434–438.
- [20] Aghasian E, Garg S, Gao L, Yu S, Montgomery J (2017) Scoring users' privacy disclosure across multiple online social networks," *IEEE Access*, vol. 5, pp. 13118–13130.
- [21] Nwaeze AC, Zavorsky P, Ruhl R (2018) Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011, 2017 12th Int. Conf. Digit. Inf. Manag. ICDIM 2017, vol. 2018–Janua, no. Icdim, pp. 98–102.
- [22] Isabwe GMN, Reichert F (2013) Revisiting students' privacy in computer supported learning systems, in *International Conference on Information Society (i-Society)*, pp. 256–262.
- [23] Cate F (2006) The failure of fair information practice principles, in *Conference on Consumer Protection in the Age of the Information Economy*, pp. 341–378.
- [24] Morton A, Sasse AM (2014) Desperately seeking assurances: Segmenting users by their information-seeking preferences A Q methodology study of users' ranking of privacy, security & trust cues, in *PST2014 International Conference on Privacy, Security and Trust Proceedings*. IEEE, April, pp. 1–10.
- [25] Alnatheer M, Chan T, Nelson K (2012) Understanding and measuring information security culture, in *Pacific Asia Conference on Information Systems (PACIS)*, vol. 144, no. 12, pp. 1–15.
- [26] Dwyer N, Marsh S (2016) How students regard trust in an elearning context, in *14th Annual Conference on Privacy, Security and Trust, PST*, pp. 682–685.
- [27] OECD (2013) Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, no. C(2013)79, pp. 11–37.
- [28] BSA (2018) BSA privacy framework, The Software Alliance, pp. 1–2.
- [29] OAIC (2015) Privacy management framework. Office of the Australian Information Commissioner, pp. 1–4.
- [30] Bush D (2016) How data breaches lead to fraud, *Network Security*. pp. 11–13.
- [31] Kurkovsky S, Syta E, "Monitoring of electronic communications at universities: Policies and perceptions of privacy," in *Proceedings of the 44th Annual Hawaii International Conference on System Sciences*, 2011, pp. 1–10.
- [32] Gerber H, Hall R (2017) Quantitative research design. HR Statistics, Pretoria, pp. 1–64.
- [33] Mathers N, Fox N, Hunn A (2009) Implementing administrative surveys and questionnaires.
- [34] Creswell JW, Creswell JD (2018) *Research design: Qualitative, quantitative and mixed methods approaches*, 5th ed. Los Angeles, USA: Sage Publications.
- [35] Saunders M, Lewis P, Thornhill A (2016) *Research methods for business students*, 7th ed. Essex, England: Pearson.
- [36] Kumar R (2011) *Research methodology: A step-by-step guide for beginners*, 3rd Editio. London: Sage Publications.
- [37] Bhattacharjee A (2012) *Introduction to research, social science research:*

- Principles, methods, and practices.
- [38] Jackson SL (2009) *Research methods and statistics: A critical thinking approach*.
 - [39] Salkind NJ (2017) *Exploring research*, 9th ed. Essex, England: Pearson Education Limited.
 - [40] Scantron, Online & paper survey management – SurveyTracker,. [Online]. Available: <https://www.scantron.com/assessment-solutions/surveys/online-paper-survey-management-survey-tracker-plus/#surveytracker-plus>. [Accessed: 15 April 2020].
 - [41] Gie A, Pearce S, “A beginner’s guide to factor analysis: Focusing on exploratory factor analysis,” 2012.
 - [42] O’Rourke N, Hatcher A (2013) *A step-by-step approach to using SAS for factor analysis and structural equation modelling*. Cary, NC.
 - [43] Hair JF, Black WC, Babbini BJ, Anderson RE (2014) *Univariate data analysis*, 7th ed. Essex, England: Pearson Education Limited.
 - [44] Da Veiga A, Martins N (2014) *Information security culture : A comparative analysis of four assessments*.



A conceptual framework for a student personal information privacy culture at universities in Zimbabwe

Kudakwashe Maguraushe¹, Adéle da Veiga² and Nico Martins³

^{1,2,3} School of Computing, College of Science, Engineering and Technology
University of South Africa, Florida, Johannesburg, South Africa

¹kmaguraushe@gmail.com, ²dveiga@unisa.ac.za, ³martinsn@web.co.za

Abstract

In this research, an information privacy culture is proposed to be embedded in three basic concepts: students' privacy expectations, privacy awareness and confidence in universities' capability to uphold information privacy. The aim of this research was to address the lack of an information privacy culture framework in the context of universities in Zimbabwe, the upsurge of privacy breaches in these institutions and the need to assist them in processing the information in line with regulatory requirements. The main objective of this study was therefore to ascertain the key components of a student personal information privacy culture (SPIPC) conceptual framework for universities in Zimbabwe. A scoping review was conducted and a SPIPC conceptual framework is proposed.

1 Introduction

The protection of any natural person in relation to the processing of their personal data is a fundamental human right (Zimbabwe Data Protection Bill, 2013). The protection of privacy is enshrined in the Constitution of Zimbabwe (Zimbabwe Constitution Parliamentary Committee, 2013). However, the Zimbabwe Data Protection Bill (ZDPB) still awaits presidential assent and promulgation (Chetty, 2013). Universities are public entities and hence the ZDPB will apply to them in terms of personal information usage. Universities will need guidance, like a framework (Ivanova, Grosseck & Holotescu, 2015), to implement the provisions of the bill but there are none yet. A privacy framework can assist institutions in leveraging student personal information self-determination (Mulligan, Koopman, Doty & Mulligan, 2016) and creating a culture of protecting student information.

Since an information security culture can be extended to encompass the concept of privacy by virtue of privacy being a subset of security (Da Veiga & Martins, 2015), it follows that awareness and training

are critical to the success of any information security initiative. This implies that in order to instil a privacy culture, awareness of personal information privacy is critical. It also follows that if an organisation (university) is to comply with regulatory requirements and protect their customers' (students') personal information, trust has to be accumulated (Da Veiga, 2017). Currently, in the Zimbabwean context, it is a difficult task to analyse and comprehend students' expectations of information privacy, their awareness levels of information privacy as well as their privacy confidence levels in universities' ability to indeed, meet privacy expectations and legal obligations. This is so because there is no reference point to measure these concepts from an industry or academic literature perspective. Privacy as a research area requires attention given the increase in data privacy breaches such as on Facebook where personal data were harvested to influence the 2016 US elections without users' knowledge (Santanen, 2018). In the Zimbabwean context, Harare Institute of Technology (a university) was attacked twice in the space of two years and sensitive information like names, registration numbers and passwords were stolen (Mudziringwa, 2018), which amounts to privacy breaches in terms of the personal information of students. With this background, it becomes essential to implement measures in order to improve the protection of personal information, including students' personal information.

The ZDPB, together with the Organisation for Economic Cooperation and Development's (OECD) Privacy Framework of 2013, the privacy principles of the General Data Protection Regulation (GDPR) and the Fair Information Practice Principles (FIPPs) as the baseline, will be used in designing a conceptual student personal information privacy culture (SPIPC) framework that universities can use when processing students' personal information to create a culture of privacy. This study was conducted in the context of information systems, considering the concept of data privacy to protect personal information from a regulatory perspective.

2 Background

An information privacy culture is defined by Da Veiga (2018a:2) as "the perceptions and beliefs a nation has about the processing of citizens' personal information, what expectations they have and how they believe organisations are meeting those expectations given certain information privacy principles (or requirements)". This privacy culture must be cultivated within an organisation so that individuals preserve information privacy, thereby upholding the confidentiality, integrity and availability aspects, which is evident when people comply with regulatory requirements (Da Veiga & Martins, 2015).

Within the context of this research, an information privacy culture is proposed to be embedded in three basic concepts: students' privacy expectations, privacy awareness and confidence that universities uphold information privacy.

The proposed information privacy framework hinges on privacy guidelines like the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data of 2013, GDPR and ZDPB in order to direct individuals within institutions in improving regulatory compliance (Chua, Herbrand, Wong & Chang, 2017). Universities need to understand the privacy expectations of students so that they can better protect students' personal information that they collect. This will increase students' confidence in the processing of their personal information by the university and help them to have less privacy concerns (Iachello & Hong, 2007), and is a new dimension of information technology research (Mamonov & Benbunan-Fich, 2018).

From a broader perspective on privacy compliance and abuse in Zimbabwe, Kaseke (2018) highlights that Zimbabwe needs legislation to protect its citizens against the misuse and abuse of their personal information. This follows the ruling party's use of citizens' personal information for campaigning purposes without their consent. This information was harvested by the Zimbabwe Electoral Commission (ZEC) for the biometric voters' roll and included names, addresses and cell phone details. Unfortunately, the lack of legislation and a well-articulated data controller for accountability purposes meant that no remedial action was taken. In addition, it is a norm that the voters' roll should be highly secured since it contains very sensitive information. In the case of Zimbabwe, this was made public online for anyone to see. If this could happen to the whole nation, there is no guarantee that universities will not fall victim to information privacy abuse. All these problems attest to the lack of a regulator and no documented penalties for the misuse of personal information as prescribed by the ZDPB.

Research (Chua et al., 2017) has revealed and exposed the failure of institutions to comply with privacy policies as well as regulatory requirements. A major concern with universities collecting students' personal information is that they often use it for purposes for which it was not originally intended and which result in privacy breaches (Arnold & Sclater, 2017). Personal information requires better safeguarding in order to prevent breaches and there is a need to develop incident response plans to improve the protection of privacy (OECD, 2013). Privacy breaches are mainly attributed to those who are supposed to safeguard the data (Iachello & Hong, 2007). The university is the safeguarding entity in the context of this research and they have a responsibility of instilling an information protection culture to aid in meeting students' expectations and regulatory requirements, suppressing privacy concerns. Information privacy concerns can affect one's intention to provide information due to lack of trust and willingness to engage with the university (Chua et al., 2017). Privacy breaches could be an indication of non-compliance with the regulations on data protection (Da Veiga, 2018a). Compliance can be achieved if suitable standards are incorporated in privacy regulatory frameworks in an effective manner.

2.1 Related Work

Limited frameworks for the privacy of students' personal information and the privacy of personal information in general are in use. Of note is the University of California, whose privacy framework derives from various privacy principles, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Yudof, 2013). It contains privacy principles guided by the Autonomy Privacy Principles (free inquiry, respect for individual privacy and surveillance) as well as information privacy principles guided by the six principles of privacy by design, choice, notice and transparency, information correction and review, information protection and accountability (Yudof, 2013). However, the framework does not touch on students' awareness of privacy regulations and there is no roadmap for how students can develop confidence in the university in terms of privacy. BSA, which is a leading global software company, has a 10-component privacy framework to uphold the privacy and security of their clients' personal data (BSA, 2018). These are transparency, purpose specification, informed choice, data quality, consumer control, security, facilitating data use for legitimate interest, accountability, legal compliance and enforcement, and international interoperability. The purpose of this is to give users more control over their personal information, which is in line with consumers' expectations (BSA, 2018). Another generalised privacy framework is that of the Office of the Australian Information Commissioner (OAIC) which was designed to assist in developing a privacy roadmap for any entity (including a university), with the explicit target being how it can be achieved (OAIC, 2015). The framework focuses more on information privacy compliance, with nothing in place for expectations and awareness thereof.

In comparison to this research, the abovementioned frameworks do not incorporate student privacy awareness and student privacy expectations. Although studies have been carried out to assess various concepts within university environments, none has been done on the awareness of students, their expectations and the attributes that increase students' confidence in the university's ability to uphold their privacy. The few frameworks do not take cognisance of the FIPPs, which is another motivating factor for this research as this study incorporates the FIPPs as the grounding privacy principles. Moreover, most of the frameworks focus on the implementation of privacy, highlighting various steps to be adhered to without necessarily looking at other components like awareness, expectations and confidence in the institution. Thus the need for a framework and diagnostic tool to assist universities in understanding students' privacy concerns and expectations of the protection of personal information, privacy and aid in giving effect to the constitutional right to privacy.

This study focused on the development of a SPIPC conceptual framework for the processing of students' personal information in Zimbabwe. This framework will not only incorporate students' privacy expectations but will also enhance their awareness in the process and instil confidence in them that the university is committed to preserving their privacy rights. The SPIPC framework will be used as a theoretical framework for the development of a validated SPIPC diagnostic instrument in future research.

2.2 Problem Statement

Partly inscribing the privacy requirements in the constitution is insufficient for providing a privacy compliance guideline on how personal information should be used. Since universities are public entities, the ZDPB will apply to them when processing the personal information of students. Universities will require guidance such as a framework to implement the requirements in the constitution and the ZDPB, but as yet, there are none in the context of Zimbabwe. A SPIPC conceptual framework can provide guidance to universities in the implementation of privacy requirements while addressing students' expectations of privacy in order to create a culture where privacy is uphold.

2.3 Research Question

This research study was guided by the following research question:

What are the key components of an SPIPC conceptual framework in the context of universities in Zimbabwe?

The remainder of this paper is structured as follows: In Section 3, the scoping review and methodology of the study are discussed. Section 4 contains a discussion of the privacy concepts of the SPIPC framework, Section 5 focuses on the privacy components of the SPIPC framework and Section 6 details the SPIPC framework. In Section 7, the expected contributions and some future work on this research were discussed; Section 8 concludes the study.

3 Methodology

A scoping review was conducted and the conceptual SPIPC framework is proposed. A scoping review is "a form of knowledge synthesis that addresses an exploratory research question aimed at mapping key concepts, types of evidence and gaps in research related to a defined area or field by systematically searching, selecting, and synthesising existing knowledge" (Colquhoun et al.,

2014:1292). It is an overview of a larger field of research aimed at mapping the key concepts underpinning a research area and the main sources and types of evidence available (Colquhoun, 2016).

Data collection was in the form of literature searches of databases that include Web of Science, ACM, IEEE Xplore, Google Scholar and Scopus. The literature search period included years of publication ranging from 2000 to 2018. Relevant articles that matched the search were read and relevant ones were selected. Studies outside the publication dates were excluded; studies that did not address student expectations on privacy, awareness levels on privacy and confidence levels on privacy were also excluded.

Since the scoping review was adopted for this study, Figure 1 is a summary of how it was conducted during the literature search.

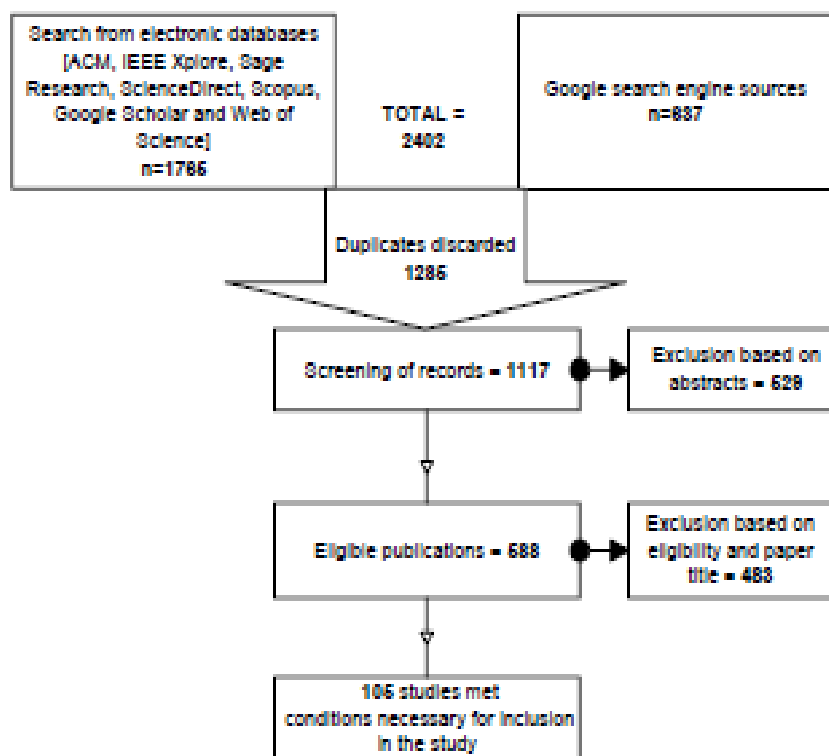


Figure 1: Scoping review literature search summary

The above figure of the scoping review for this study shows that a total of 1765 searches of electronic material from various electronic databases were done. These were uploaded to the Mendeley desktop library for easier management. Searches of literature material were also done, with 637 Google retrievals. This gives a total of 2402 literature sources. Among these, 1285 were discarded as duplicates, leaving 1117 literature sources for screening. For inclusion, the focus was on keywords such as the following: "personal information", "privacy", "information privacy culture", "student privacy awareness", "privacy and expectations", "privacy and confidence", "privacy concerns", "privacy breaches", "privacy compliance", "privacy perceptions" and "student privacy frameworks". For exclusion, two steps were followed. The first step was based on abstracts and 629 literature sources were excluded, leaving 688 sources. In the second step, sources were excluded based on title and

eligibility; 483 sources were excluded. This left 105 literature sources that met the conditions for inclusion into this study. These 105 sources were used to define the concepts of the SPIPC framework.

4 Privacy Concepts

Privacy is a paramount concept that needs to be observed within the university environment. Students have their own expectations as well as awareness levels of privacy, which must lead to the development of confidence that the university observes and upholds the privacy of their personal information. As pointed out by Da Veiga (2018b), confidence in terms of privacy indicates that an organisation implements privacy regulatory requirements when handling customers' (students') personal information. The three concepts namely, students' privacy awareness, privacy expectations and confidence in the university are depicted in Figure 2 as the first building blocks of the SPIPC framework. The three concepts are discussed from the student's perspective (i.e. the study was student centred).

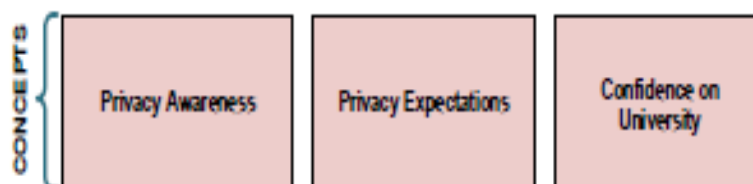


Figure 2: Privacy concepts

4.1 Privacy Awareness

Awareness is created through the privacy notices of the university (Vail, Earp & Antón, 2008). Research results (Chen & Ismail, 2013) show that students lack knowledge and understanding of privacy within universities. Awareness is a prerequisite of compliance (Aghasian, Garg, Gao, Yu & Montgomery, 2017). Research by Nwaeze, Zavorsky and Ruhl (2018) also show that compliance with privacy policies and laws, and privacy concerns, are a result of proper awareness programmes in organisations. Lawler and Molluzzo's (2011) research resonates with that of Isabwe and Reichert (2013) in recommending that universities should promote privacy awareness and allow students to exercise their right to privacy and have consent control, especially when processing personal information. As indicated in the Constitution of Zimbabwe, it is the duty of the data controller (the university) to disseminate knowledge and awareness about privacy (Republic of Zimbabwe, 2013). Awareness increases users' (students') compliance with policies and willingness to give or disclose their personal information for positive use by the data controller (university) (Kurkovsky & Syta, 2011).

4.2 Privacy Expectations

FIPPs recommend that individuals (students) must have the expectation of personal information privacy (Cate, 2006). Even when there is a need to obtain personal information for processing by the organisation (university), a considerable degree of expectation of privacy rests on the belief that the collection will be minimal and based on relevance (Cate, 2006). Empirical results obtained by Da Veiga (2018a) indicated that consumers have high expectations of privacy in organisations (institutions) when processing their personal information. If consumers (students) perceive the organisation (university) as failing to meet their privacy expectations, they tend to become impassioned and reject sharing their personal information with the organisation (university) (Morton & Sasse, 2014).

4.3 Confidence in the University

In some cases, students have confidence in their institutions to the extent that they do not seek privacy related to documentation (Stange, 2011). Privacy pledges by universities provide a sense of trust that instils confidence and this results in an information privacy culture that can permeate the whole institution (Alnatheer, Chan & Nelson, 2012). As Dwyer and Marsh (2016) point out, trust is an element of confidence; this is corroborated by the OECD (2013). If there is an improvement in privacy protection and privacy regulations, users' confidence tend to increase (BSA, 2018). Lack of trust in the use of personal information has a negative impact on the confidence levels of students (Dwyer & Marsh, 2016; OAIC, 2015). Data and privacy breaches result in low confidence in customers (students) towards the business (university) (Bush, 2016). Any loss of confidence or trust in the organisation or university will have undesirable retrogressive consequences (OECD, 2013). Therefore, there is a need for the university to be conversant of privacy policies with regard to students, which will eventually increase compliance with privacy policies (Kurkovsky & Syta, 2011). A personal information privacy culture within an organisation or institution inspires trust and confidence in the entity (OAIC, 2015).

5 Privacy Components

The FIPPs were used as the baseline for the components of this study and were complemented by the OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPB. The FIPPs were used as the baseline because they are believed to be the founding and underlying guidelines for personal information self-regulation in the digital world (Cate, 2006; Gellman, 2017). The OECD Protection of Privacy and Transborder Flows of Personal Data of 2013 was a revision of the original FIPPs, underpinning the fact that most privacy principles are anchored on the FIPPs (Gellman, 2017). In the context of this study, discussions on the SPIPC framework were done from the student's perspective. Two of the FIPPs components (i.e. security and accountability) are enforceable by the university since it is the university's prerogative. Accordingly, these components were excluded from adoption into the SPIPC framework. The final six components are notice/openness, information quality, purpose specification, use limitation, collection limitation, and individual participation or choice. Privacy policy, education and consent were added to these components.

5.1 Notice/Openness

While notices are believed to make students aware of privacy-related issues, they also provide trust and confidence in the data subject (student, in this case), which is important for fostering a relationship between the parties concerned (Guffin, 2017; Stange, 2011). Appropriate notice is needed before personal information is collected (Guffin, 2017). Students expect notices to be short, flexible and non-ambiguous (Preuveeners, Joosen & Ilie-Zudor, 2016). Notices are assumed to make institutions transparent and open in terms of how they use the personal information of the students as data subjects (Gellman, 2017). It is also important that if there is a privacy breach of a student's personal information, he or she has to be notified within the shortest period of time (Cornock, 2018).

5.2 Information Quality

Information quality is important in achieving integrity of information within an organisation (university) (Guffin, 2017; OECD, 2013; Zimbabwe Data Protection Bill, 2013). Personal information should be up to date, complete and accurate, without compromising its relevance to the purpose for which it is to be used (Gellman, 2017). It is the prerogative of the university to uphold personal information privacy for information quality (Guffin, 2017). This will increase students' confidence in

the university. The assurance of information quality is also measured by the presence of information security (Banerjee, 2015).

5.3 Purpose Specification

In terms of the ZDPB, Chetty (2013) highlights that individual personal information has to be processed for an explicit, specified and legitimate reason; and this must be done on or before the time of collection. In addition, once the information is collected, it must not be directed to or used for a purpose not previously specified unless this is done to comply with the law (Katurura & Cilliers, 2016). Before any collection of personal information is done, consent must be obtained from the subject matter (the student, in this case) (Johnston & Wilson, 2012).

5.4 Use Limitation

The individual (student) will expect the organisation (university) to limit the amount of information they collect for use (Cate, 2006). The OECD Privacy Framework of 2013 specifies that "personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except: with the consent of the data subject, or by the authority of law" (OECD, 2013:14). The importance of mandatory and fundamental consent in the collection or use of any personal information is also stressed (Cate, 2006). The purpose has to be explicit and clearly spelt out (Robbins & Sabo, 2006).

5.5 Collection Limitation

Collection minimisation is important because the organisation (university) should collect information lawfully, fairly and only for the specified purposes (Chetty, 2013). In this case, the university should limit collection of personal information that is not necessary for academic purposes. If the organisation (university) is to collect a large amount of personal information from the user (student), it will raise privacy concerns among the students (Rasmussen & Dara, 2014). In reality, limiting the amount of information collected increases participation by students and consequently information privacy (Kokolakis, 2017).

5.6 Individual Participation/Choice

Individuals, including students, must be given the right to participate in activities related to their personal information (OECD, 2013; Zimbabwe Data Protection Bill, 2013). Their participation increases the knowledge and assurance on how their personal information is being used by the university, ultimately building confidence in the university (Cate, 2006). The right of participation principle increases transparency in the use of students' personal information (Tikkanen-Piri, Rohunen & Markkula, 2018). The university must be able to provide a response as confirmation to the data subject (student) about personal information collected (OECD, 2013). When making a request for conformation about personal information collected, the data subject (student) has the right to follow clearly set processes as stated in the individual participation principle (OECD, 2013). Moreover, students must be able to amend their personal information as and when the need arises (Gellman, 2017). Technology must not affect how personal information is accessed by students (Chetty, 2013).

Studies have shown that privacy policies address privacy concerns and universities need it to instil awareness in students (Chua et al., 2017). Students also need to be educated on privacy-related issues. Farooq, Kakakhel, Virtanen and Isoaho (2016) reveal that privacy education is a key measure for reducing information privacy concerns. Central to the processing of any personal information is consent, which must be granted by the student as a basic human right (European Union, 2016; OECD,

2013; Zimbabwe Data Protection Bill, 2013). This creates three more components, which were added to the SPIPC framework (i.e. privacy policy, privacy education and consent).

5.7 Privacy Policy

A privacy policy is a document that discloses how organisations should collect, manage, disclose or use an individual's personal information (Chua et al., 2017). It is a way of achieving privacy of personal information and it should be in place (Chua et al., 2017). Privacy policies should be easily understood and should be short, precise and to the point (Vail et al., 2008). It is an expectation of the university administrators that students need to read the whole privacy policy document in order to be aware of privacy-related issues (Lawler, Molluzzo & Doshi, 2012). Changing privacy policies continuously and frequently will confuse students (OECD, 2013).

5.8 Privacy Education

Education increases awareness (Rezgui & Marks, 2008). Privacy education is very important as it informs the students about the reasons for collecting their personal information, how the information will be used, the sensitivity of the personal information and what they will receive after sharing their personal information with the university (Isabwe & Reichert, 2013). Students need to be continuously reminded of the privacy-related issues through privacy education (Sargsyan, 2016). The Expert Group on privacy proposed that in order for the OECD Protection of Privacy and Transborder Flows of Personal Data framework to be effective, privacy education is critical in reducing privacy breaches (Gellman, 2017). Therefore, lack of privacy awareness can be solved by providing privacy education to the students (Fink, 2012).

5.9 Consent

Consent is not a principle but rather a fundamental right that should be clear before information is shared (European Union, 2016; OECD, 2013; Tikkinen-Piri et al., 2018; Zimbabwe Data Protection Bill, 2013). It is an individual's right to receive communication about, and to give confirm or withhold confirmation for, when information about them is to be used (OECD, 2013; Zimbabwe Data Protection Bill, 2013). Students have the right and choice of consent to opt to share their personal information (Chua et al., 2017). If a student does not require the continued sharing or receiving of certain messages, he/she has the right to opt out (Krishnan & Vorobyov, 2015). Individuals, including students, must not be harassed or intimidated into giving consent (Cormock, 2018; Zimbabwe Data Protection Bill, 2013). It is imperative that the university is clear when they want to collect personal information by consent (Taddei & Contena, 2013). By seeking consent from the students, the university will increase the students' trust in the institution regarding the use of their personal information (OAIC, 2015; Sargsyan, 2016).

6 Conceptual Framework

The SPIPC framework has two sections: the privacy components section and the privacy concepts section. When combined, the researcher perceives the two sections as formulating the information privacy culture within the university environment, which must be cultivated to enhance privacy of personal information. Figure 3 shows the SPIPC framework: expectations, awareness and confidence in the university, with the adopted components.

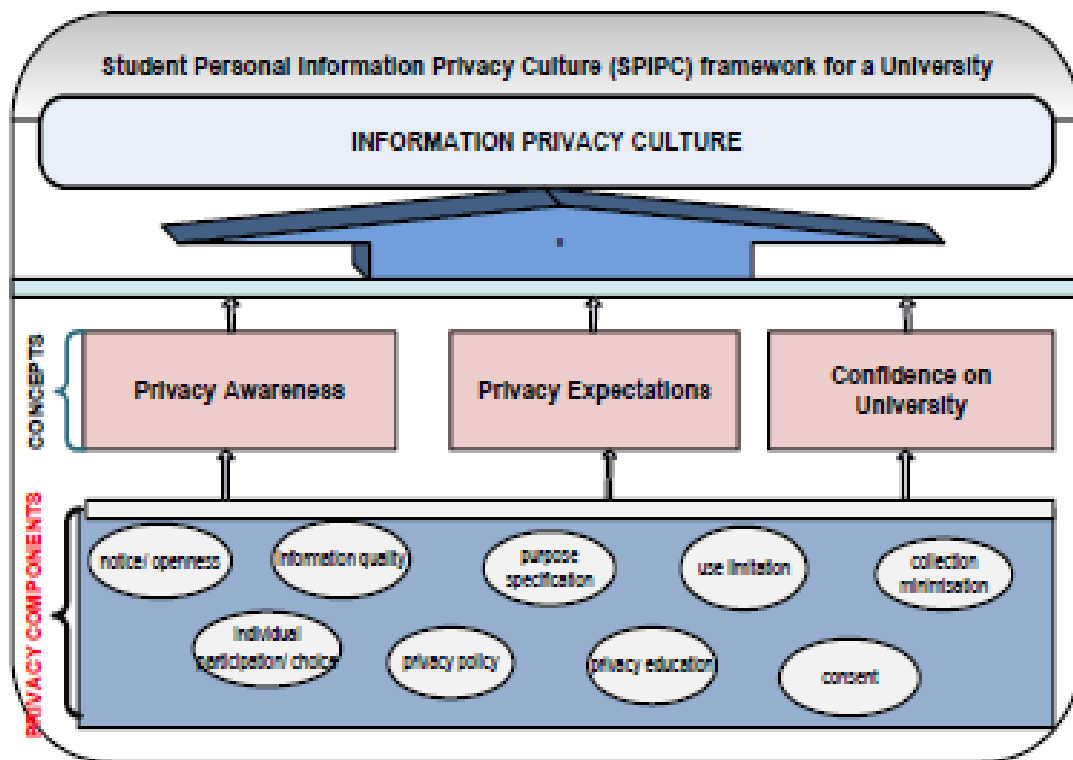


Figure 3: The SPIPC framework

The privacy concepts and privacy components in the above diagram are discussed below:

Privacy Concepts: A university must thrive to fulfil and meet the three privacy concepts so that privacy of students' personal information is well articulated. The three privacy concepts are used to measure the components. This means that every component must be tested for awareness, expectations and confidence.

Privacy Components: The framework's scope is grounded on personal information from the student's perspective on the university, as derived from the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPB. The components are considered fundamental and every student must play a role in adhering to them in a bid to have a positive information privacy culture. When combined, these components aid in understanding the information privacy culture in terms of students' awareness, expectations and confidence in the university.

7 Expected Contributions and Future Work

This study involved developing the SPIPC framework based on the three concepts of students' privacy awareness, privacy expectations and confidence in the university. The research also contributed to articulating the three concepts from a student perspective. The integration of the principles of the OECD Protection of Privacy and Transborder Flows of Personal Data, the privacy guidelines of the FIPPs, the GDPR directive and the ZDPB allows for easy adoption even beyond Zimbabwe.

The SPIPC will be used to develop a diagnostic instrument (questionnaire) with statements addressing each concept of the FIPPs, together with the additional concepts from an awareness, expectation and confidence perspective. The questionnaire will be validated in a university environment and the framework will be validated using structural equation modelling (SEM). This will aid universities in implementing privacy expectations while aiming to meet regulatory requirements. The SPIPC framework can also be used in other universities in Africa and other parts of the world to improve the protection of privacy of students.

8 Conclusion

The SPIPC framework was presented as formulated from the FIPPs, OECD Protection of Privacy and Transborder Flows of Personal Data, GDPR and ZDPB, with nine components for building and ensuring a privacy culture within a university environment. Relevant literature relating to the concepts and components were explored to develop the framework. The framework will be used in future studies for the empirical investigation of the relationships between the various concepts and components. It can also be used in other parts of the world or by industry in a bid to uphold information privacy.

Acknowledgment

This paper is based on the thesis document for the Doctor of Philosophy in Information Systems degree at the University of South Africa (Unisa) and was wholly supported by the Unisa Master's and Doctoral (M+D) Research Bursary disbursed in 2019.

References

- Aghasian, E., Garg, S., Gao, L., Yu, S., & Montgomery, J. (2017). Scoring users' privacy disclosure across multiple online social networks. *IEEE Access*, 5, 13118–13130. Retrieved from <https://doi.org/10.1109/ACCESS.2017.2720187>
- Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Pacific Asia Conference on Information Systems (PACIS)*, 144(12), 1–15. Retrieved from <http://aisel.aisnet.org/pacis2012/144>
- Arnold, K. E., & Sclater, N. (2017). Student perceptions of their privacy in leaning analytics applications. *Proceedings of the Seventh International Learning Analytics and Knowledge Conference*, 66–69. Retrieved from <https://doi.org/10.1145/3027385.3027392>
- Banerjee, S. (2015). Development and validation of a conceptual framework for IT offshoring engagement success (University of Bedfordshire). Retrieved from <http://hdl.handle.net/10547/583209>
- BSA. (2018). *BSA PRIVACY FRAMEWORK* (pp. 1–2). Retrieved from https://www.bsa.org/files/policy-filings/BSA_2018_PrivacyFramework.pdf
- Bush, D. (2016). How data breaches lead to fraud. *Network Security* (pp. 11–13). Retrieved from [https://doi.org/10.1016/S1353-4858\(16\)30069-1](https://doi.org/10.1016/S1353-4858(16)30069-1)
- Cate, F. H. (2006). The failure of fair information practice principles. *Conference on Consumer Protection in the Age of the Information Economy*, 341–378. Retrieved from <https://ssrn.com/abstract=1156972>

- Chen, L. F., & Ismail, R. (2013). Information technology program students' awareness and perceptions towards personal data protection and privacy. *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 434–438. Retrieved from <https://doi.org/10.1109/ICRIIS.2013.6716749>
- Chetty, P. (2013). Presentation on Zimbabwe Data Protection Bill. *Harmonization of the ICT policies in sub-Saharan Africa*. Retrieved from
- Chua, H. N., Herbrand, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. Retrieved from <https://doi.org/10.1016/j.tele.2017.01.008>
- Colquhoun, H. (2016). Current best practices for the conduct of scoping reviews. *Impactful Biomedical Research: Achieving Quality and Transparency*, 1–24. Retrieved from <https://doi.org/10.1093/ptj/pzw074>
- Colquhoun, H. L., Levac, D., O'Brien, K. K., Straus, S., Tricco, A. C., Perrier, L., ... Moher, D. (2014). Scoping reviews: Time for clarity in definition, methods, and reporting. *Journal of Clinical Epidemiology*, 67(12), 1291–1294. Retrieved from <https://doi.org/10.1016/j.jclinepi.2014.03.013>
- Cormock, M. (2018). General Data Protection Regulation (GDPR) and implications for research. *Maturitas*, 111, 20–21. Retrieved from <https://doi.org/10.1016/j.maturitas.2018.01.017>
- Da Veiga, A. (2017). An information privacy culture index framework and instrument to measure privacy perceptions across nations : Results of an empirical study. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security and Assurance (HAISA)*, 196–209. Retrieved from <http://hdl.handle.net/10500/23566>
- Da Veiga, A. (2018a). An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information and Computer Security*, 26(3), 338–364. Retrieved from <https://doi.org/10.1108/ICS-03-2018-0036>
- Da Veiga, A. (2018b). An online information privacy culture: A framework and validated instrument to measure consumer expectations and confidence. *2018 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. Retrieved from <https://doi.org/10.1109/ICTAS.2018.8368759>
- Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243–256. Retrieved from <https://doi.org/10.1016/j.clsr.2015.01.005>
- Dwyer, N., & Marsh, S. (2016). How students regard trust in an elearning context. *14th Annual Conference on Privacy, Security and Trust (PST) 2016*, 682–685. Retrieved from <https://doi.org/10.1109/PST.2016.7906956>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation). 59 Official Journal of the European Union §.
- Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2016). A taxonomy of perceived information security and privacy threats among IT security students. *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 280–286. Retrieved from <https://doi.org/10.1109/ICITST.2015.7412106>
- Fink, C. (2012). Privacy and confidentiality in the virtual classroom: Instructor perceptions, knowledge and strategies (University of Victoria). Retrieved from <http://hdl.handle.net/1828/4176>
- Gellman, R. (2017). Fair information practices: A basic history. *SSRN Electronic Journal* (Version 2.18), 1–46. Retrieved from <https://doi.org/10.2139/ssrn.2415020>
- Guffin, P. (2017). FIPPs and PIA. State of the Judicial Branch, 1–6. Retrieved from https://www.courts.maine.gov/maine_courts/committees/tap/FIPPs-and-PIA-email.pdf
- Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends® in Human-Computer Interaction*, 1(1), 1–137. Retrieved from <https://doi.org/10.1561/11000000004>
- Isabwe, G. M. N., & Reichert, F. (2013). Revisiting students' privacy in computer supported learning

- systems. *International Conference on Information Society (i-Society)*, 256–262.
- Ivanova, M., Grosseck, G., & Holotescu, C. (2015). Researching data privacy in eLearning. *2015 International Conference on Information Technology Based Higher Education and Training (ITHET)*, 1–6. Retrieved from <https://doi.org/10.1109/ITHET.2015.7218033>
- Johnston, A., & Wilson, S. (2012). Privacy compliance risks for Facebook. *IEEE Technology and Society Magazine*, 31(2), 59–64. Retrieved from <https://doi.org/10.1109/MTS.2012.2185731>
- Kaseke, P. (2018). Protect personal data breaches. *Newsday*. Retrieved from <https://www.newsday.co.zw/2018/10/protect-personal-data-breaches/>
- Katurura, M., & Cilliers, L. (2016). The extent to which the POPI Act makes provision for patient privacy in mobile personal health record systems. *2016 IST-Africa Week Conference*, 1–8. Retrieved from <https://doi.org/10.1109/ISTAFRICA.2016.7530595>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64(C), 122–134. Retrieved from <https://doi.org/10.1016/j.cose.2015.07.002>
- Krishnan, P., & Vorobyov, K. (2015). ScienceDirect enforcement of privacy requirements. *Computers & Security*, 52, 164–177.
- Kurkovsky, S., & Syta, E. (2011). Monitoring of electronic communications at universities: Policies and perceptions of privacy. *Proceedings of the 44th Annual Hawaii International Conference on System Sciences*, 1–10. Retrieved from <https://doi.org/10.1109/HICSS.2011.312>
- Lawler, J. P., & Molluzzo, J. C. (2011). A survey of first-year college student perceptions of privacy in social networking. *Journal of Computing Sciences in Colleges*, 26(3), 36–41.
- Lawler, J. P., Molluzzo, J. C., & Doshi, V. (2012). An expanded study of net generation perceptions on privacy and security on social networking sites (SNS). *Information Systems Education Journal*, 10(1), 21–36.
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83(C), 32–44. Retrieved from <https://doi.org/10.1016/j.chb.2018.01.028>
- Morton, A., & Sasse, A. M. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences: A Q methodology study of users' ranking of privacy, security & trust cues. *PST2014 International Conference on Privacy, Security and Trust Proceedings*, (April), 1–10. Retrieved from <https://www.researchgate.net/publication/324167424%0ADesperately>
- Mudzingwa, F. (2008). HIT hacked again? More than 3 500 student cccount credentials leaked [Blog post]. Retrieved from <https://www.techzim.co.zw/2018/05/hit-hacked-again-more-than-3-500-student-account-credentials-leaked/>
- Mulligan, D. K., Koopman, C., Dory, N., & Mulligan, D. K. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy subject areas. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), 1–17. Retrieved from <https://doi.org/http://dx.doi.org/10.1098/rsta.2016.0118>
- Nwaeze, A. C., Zavorsky, P., & Ruhl, R. (2018). Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011. *2017 12th International Conference on Digital Information Management (ICDIM)*, 98–102. Retrieved from <https://doi.org/10.1109/ICDIM.2017.8244644>
- OAIC. (2015). *Privacy management framework*, 1–4. Retrieved from <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/privacy-management-framework.pdf>
- OECD. (2013). Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data. The OECD Privacy Framework § (2013) 11-37. Retrieved from <https://www.oecd.org/sti/economy/2013-oecd-privacy-guidelines.pdf>

- Preuveneers, D., Joosen, W., & Iie-Zudor, E. (2016). Data protection compliance regulations and implications for smart factories of the future. *12th International Conference on Intelligent Environments (IE'16)*, 40–47. Retrieved from <https://doi.org/10.1109/IE.2016.15>
- Rasmussen, C., & Dara, R. (2014). Recommender systems for privacy management: A framework. *IEEE 15th International Symposium on High-Assurance Systems Engineering Recommender*, 243–244. Retrieved from <https://doi.org/10.1109/HASE.2014.43>
- Republic of Zimbabwe. (2013). Zimbabwe's Constitution of 2013, www.constituteproject.org § (2013). Retrieved from https://www.parl.zim.gov.zw/component/k2/download/1290_da9279a81557040d47c3a2c27012f6e1
- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers and Security*, 27(7–8), 241–253. Retrieved from <https://doi.org/10.1016/j.cose.2008.07.008>
- Robbins, J., & Sabo, J. (2006). Managing information privacy: Developing a context for security and privacy standards convergence. *IEEE Security and Privacy Magazine*, 4(4), 92–95. Retrieved from <https://doi.org/DOI:10.1109/MSP.2006.98>
- Santanen, E. (2018). The value of protecting privacy. *Business Horizons*, 62(1), 5–14. Retrieved from <https://doi.org/10.1016/j.bushor.2018.04.004>
- Sargsyan, T. (2016). The privacy role of information intermediaries through self-regulation. *Internet Policy Review Journal on Internet Regulation*, 5(4), 1–17. Retrieved from <https://doi.org/10.14763/2016.4.438>
- Stange, C. (2011). Privacy concern and student engagement in the virtual classroom (University of Victoria). Retrieved from <https://docplayer.net/13882757-Privacy-concern-and-student-engagement-in-the-virtual-classroom.html>
- Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29(3), 821–826. Retrieved from <https://doi.org/10.1016/j.chb.2012.11.022>
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 34(1), 134–153. Retrieved from <https://doi.org/10.1016/j.clsr.2017.05.015>
- Vail, M. W., Earp, J. B., & Antón, A. L. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management*, 55(3), 442–454. Retrieved from <https://doi.org/10.1109/TEM.2008.922634>
- Yudof, M. (2013). *Privacy and Information Security Initiative Steering Committee Report to the President*, 1–43. California, USA.
- Zimbabwe Constitution Parliamentary Committee. (2013). *The Constitution of Zimbabwe Amendment (No. 20) Act, 2013*, 51 § (2013).
- Zimbabwe Data Protection Bill. (2013). *The Zimbabwe Data Protection Bill Draft*. Retrieved from <https://t3n9sm.c2.acecdn.net/wp-content/uploads/2016/08/Zimbabwes-Draft-Data-Protection-Bill-v-1-June-2013.pdf>

Appendix O: Editors Certificate



BE STILL COMMUNICATIONS
For effective communication solutions

landamasuku@gmail.com
+27833841534; +27618043021

Professional
EDITORS
Guild

CERTIFICATE OF EDITING

This document certifies that a copy of the thesis/dissertation whose title appears below was proofread for proper English language usage, grammar, punctuation, spelling, and overall style by Dr Nhlanhla Landa whose academic qualifications and professional affiliation appear in the footer of this document. The research content and the author's intentions were not altered during the editing process. The formatting of the document is the responsibility of the client.

TITLE: DEVELOPMENT OF A DIAGNOSTIC INSTRUMENT AND PRIVACY MODEL FOR STUDENT PERSONAL INFORMATION PRIVACY PERCEPTIONS IN ZIMBABWE


AUTHORS: KUDAKWASHE MAGURAUSHE (61945218)

Note: The edited work described here may not be identical to that submitted. The author, at their sole discretion, has the prerogative to accept, delete, or change amendments made by the editor before submission.

DATE: 6 JANUARY 2021

EDITOR'S COMMENT

The author was advised to effect suggested corrections in regards to consistency in structure and logic, grammar and expression. The reference list also needed attention.


Signature

PhD Applied Linguistics (UFH), MA Applied Linguistics (MSU), BA (Honours) English and Communication (MSU)

Professional Membership: A member of the Professional Editors Guild