

UNIVERSITY OF ZULULAND
CYBERETHICAL BEHAVIOUR OF UNDERGRADUATE STUDENTS OF THE
UNIVERSITY OF ZULULAND, SOUTH AFRICA, AND THE FEDERAL UNIVERSITY
OF AGRICULTURE, ABEOKUTA, NIGERIA

By

ADERIBIGBE NURUDEEN ADENIYI

A thesis submitted to the Faculty of Arts

Department of Information Studies

of the

University of Zululand

In partial fulfilment of the requirements for the degree

of Doctor of Philosophy

In Information Studies

Supervisor: Prof. D. N. Ocholla

(University of Zululand)

Co-supervisor: Prof. Johannes Britz

(University of Wisconsin, Milwaukee)

Date of Submission: 18 March 2019

DECLARATION

I hereby declare that I am the sole author of this thesis and I have not submitted it to any other university for a qualification. This is a true copy of the thesis, including the required final revisions, as recommended by my supervisors and examiners. All the sources I have used or quoted have been indicated and acknowledged as complete references. I understand that my thesis may be made electronically available to the public.



NURUDEEN ADERIBIGBE

Date: 18 March 2019

STUDENT NUMBER: 201445518



.....
Supervisor

PROF. D. N. OCHOLLA

Date: 19th March 2019



.....
Co-supervisor

PROF. J. BRITZ

UNIVERSITY OF WISCONSIN, MILWAUKEE

Date: 19th March 2020

DEDICATION

For my family: Basirah, Mohammad, Mahmoud, Mustapha, Mariam and
Maymouna, Semiyu, Tajudeen, Taufique and Senoir Girls
Thank you for enduring the pains of my perennial absence.

ACKNOWLEDGEMENTS

Alhamdulillah! This wouldn't have been possible but for the mercy and guidance of Allaah almighty.

I am deeply indebted to my supervisor extraordinaire who, despite the rough roads towards the completion of this effort, has been a source of inspiration. The insightful observations and comments from Prof. Dennis Ocholla has afforded me the privilege of seeing the big picture of humanity and scientific research, especially as it relates to the field of information studies. It was also a pleasure to work with my second supervisor, Prof. Johannes Britz, of the University of Wisconsin, USA, whose earlier guidance at the proposal stage informed the focus of the study. For all these, I am most grateful to Prof. Dennis Ocholla and Prof. Johannes Britz. Thank you for your support, guidance, encouragement and the invaluable interactions that made me a better student and learner.

I will like to extend my appreciation to Dr Neil Evans, whose earlier advice on theoretical framework and psychological theories challenged my psychological knowledge in the world of theory in research. It was also a pleasure to work with the staff and students of the Department of Information Studies at the University of Zululand.

It is equally important to add here, the special contributions of very good friend whom we started this journey together but was able to complete the track in record time Dr Owolabi Abayomi and other staffs at 'Nimbe Adedipe Library Funaab and others who have contributed in no small measure in bringing this about. To them all I say a very big thank you.

ABSTRACT

This study examined the cyberethical behaviour of undergraduate students of the University of Zululand, South Africa, and the Federal University of Agriculture Abeokuta, Nigeria. Cyberethical behaviour is the study and understanding of users' attitudes towards the use of cybertechnology and their interaction with other aspects of the Internet and its environment.

The specific objectives of the study were to: explore the relationships between students' demographic characteristics and their cyberethical behaviour; determine their level of awareness of cyberethical behaviour; explore the types of cyberethical behaviour exhibited by undergraduate students; determine the influence of the Theory of Planned Behaviour on cyberethical behaviour; find out the challenges faced by students in order to act ethically in cyberspace; and establish the impact of cyberethics policy in strengthening or promoting cyberethics in the two universities.

The study adopted the pragmatic research paradigm that combines both quantitative and qualitative research methods. The sample for the study was drawn from undergraduate students in two purposively selected universities in South Africa and Nigeria. The respondents were drawn from all faculties and colleges in the two universities. A combination of quantitative and qualitative approaches was used in the data analysis. Data collected using the quantitative instrument were coded and the analyses were carried out using the Statistical Package for the Social Sciences (SPSS) version 25.0. Data from the interview schedule were analysed using thematic analysis. Overall, 450 undergraduate students were invited to participate in the survey, but 380 respondents completed and returned the questionnaire, giving a response rate of 84.4%. From the expected 16 members of staff of both Information Technology Section (ITS) and Information & Communication Technology Resources Centre (ICTREC), 14 were interviewed, giving a response rate of 88%.

The findings of the study indicated a demographic dominance of female respondents from South Africa and male respondents from Nigeria. The majority of the undergraduate students in the studied universities are in the 21-25 age brackets, which is not unique. The study also showed moderate influences of demographic characteristics on cyberethical behaviour. Most of the respondents from the sampled universities reported that they were aware of cyberethical behaviour. A high percentage of participants, 98 (52.1%), revealed that they had never received ethical orientation in the university.

Top on the list of types of cyberethical violations is cyber piracy, with the highest mean scores of ($\bar{x}$ = 3.6 and SD = 1.5) and ($\bar{x}$ = 3.6, SD = 1.3) among students in Nigeria and South Africa respectively. The three variables - attitude, subjective norm and perceived behavioural control from the Theory of Planned Behaviour (TPB) - were individually statistically significant in influencing students' cyberethical behaviour. Furthermore, the study revealed a significant number of challenges that were associated with appropriate cyberethical behaviour. Despite the importance of cyber technology to the university community, the universities provided access, but with some restrictions. While UNIZULU provides round the clock internet access, FUNAAB has limited and regulated access for users on their network.

The study recommends that universities should sustain orientation programmes on cyberethics and cyber security awareness at the start of each academic year, especially for fresh students, so that they can act responsibly when in the university cyberspace. It is also suggested that universities establish strong policies and corresponding penalties for cyberethical violations or misuse behaviour. Universities should revisit or review existing computer laboratory ethical conduct and policies to attune to the demands of present reality.

The findings of this study may spark further investigation into the impact of cyber technology on the ethical conduct of undergraduate and graduate students in academic institutions in the studied countries, and perhaps elsewhere. The study also contributes to extant literature on the application of the Theory of Planned Behaviour (TPB).

The originality and value of this study can be viewed from the application of a socio-psychology theory to determine cyberethical behaviour, which provides further evidence that the TPB can be applied to cyberethics research. The study also contributes to literature by conceptualising the phenomenon of cyberethics in the context of South Africa and Nigeria, which can generate debates for further discussions on cyberethics among African scholars. In addition, the findings will help university executives to consider developing policy and standards that will encourage ethical behaviour by all the cyber technology users in their cyberspaces. The empirical findings from this study can help to create awareness about cyberethics and motivate academics and institutions in these African countries to accept the challenge of establishing, monitoring, evaluating and strengthening their environments so that academic integrity will be valued and carefully protected. The principal theoretical implication of this study is that, while it is not enough to declare that unethical cyber behaviour is against an institution's code of conduct and acceptable use, university managements need to initiate forums to bridge the gap between students' knowledge and their actual behaviour.

Keywords: cyberethics, ethical behaviour, university cyberspace, Theory of Planned Behaviour (TPB), South Africa, Nigeria, undergraduate students, cyberethics policy.

CONTENTS

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	v

CHAPTER ONE

INTRODUCTION AND BACKGROUND OF THE STUDY	1
1.1 Introduction and Conceptualisation	1
1.2 Contextual Setting.....	6
1.2.1 Law and ethics.....	6
1.2.2 Cyber law in South Africa	7
1.2.3 Cyberethics policy of the University of Zululand.....	7
1.2.4 Cyber law in Nigeria	8
1.2.5 Cyberethics policy of the Federal University of Agriculture, Abeokuta.....	9
1.3 Statement of the Problem	9
1.4 Aim of the Study	11
1.5 Research Objectives	11
1.6 Research Questions.....	12
1.7 Scope and Limitation	12
1.8 Intended Contribution to Knowledge.....	13
1.9 Methodology Overview.....	15
1.10 Definition of Terms.....	15
1.11 Structure of the Thesis... ..	16
1.12 Summary	18

CHAPTER TWO

THEORETICAL FRAMEWORK	19
2.1 Introduction.....	19
2.2 Theory and Model	19
2.3 Overview of Related Theoretical Framework on Cyberethics Behaviour	21
2.4 Application of Behavioural Theories in Research in/on Africa as Reflected in some Databases.	23
2.5 Description of the Theory of Planned Behaviour.....	24
2.6 Theory of Planned Behaviour Constructs	26
2.6.1 Attitudes.....	27
2.6.2 Subjective norm.....	28

2.6.3	Perceived behavioural control	29
2.7	Strengths of the Theory of Planned Behaviour	31
2.8	Criticisms of the Theory of Planned Behaviour	31
2.9	Application of the Theory of Planned Behaviour in Cyberethical Studies.....	33
2.10	Justification for Using the Theory of Planned Behaviour	35
2.11	Implication.....	37
2.12	Summary	38

CHAPTER THREE

LITERATURE REVIEW.....	39
3.1 Introduction.....	39
3.2 History of the Internet	41
3.3 The Emergence and Concept of Cyberethics.....	42
3.4 Cybertechnology and Human Behaviour.....	45
3.5 The Influence of Demographic Characteristics on Cyberethics Behaviour among Students.....	47
3.6 Awareness of Cyberethics Behaviour among Undergraduate Students.....	49
3.7 Types of Cyberethics Behaviour among Undergraduate Students.....	53
3.8 Empirical Evidence on the Influence of the Constructs of TPB on Cyberethics Behaviour Intention of Undergraduate Students	62
3.8.1 Influence of attitude on cyberethics behaviour intention.....	63
3.8.2 Influence of subjective norms on cyber behaviour of undergraduate students	64
3.8.3 Influence of perceived behavioural control on behavioural intention towards cyber behaviour	66
3.9 Ethical Issues and Intellectual Property.....	67
3.10 Challenges in Efforts by Undergraduate Students to Act Ethically Correct in Cyberspace	69
3.11 Influence of Cyberethics Policy in Strengthening or Promoting Ethical Conduct in Cyberspace	71
3.12 Ethical Theories and Cyberethics	73
3.13 Gaps in Literature	80
3.14 Implication of Literature Review.....	82
3.15 Summary	84

CHAPTER FOUR

RESEARCH METHODOLOGY	86
4.1 Introduction.....	86
4.2 Theoretical/Paradigmatic Perspective.....	86
4.3 Pragmatism	89

4.3.1	Pragmatic knowledge claims.....	89
4.4.	Research Design.....	91
4.4.1.	Case studies	91
4.4.2	Survey research	92
4.5.	Population of the Study.....	93
4.5.1	Accessible population	94
4.6.	Sampling Procedures and Methods	94
4.6.1	Stratified sampling technique.....	96
4.6.2	Cluster sampling technique	96
4.6.3	Purposive/judgmental sampling	97
4.6.4	Systematic random sampling	99
4.6.5	Sample size.....	100
4.6.6	Sampling frame	101
4.7	Data Collection	104
4.7.1	Questionnaire	104
4.7.2	Interview	107
4.7.3	Pilot study	107
4.8	Validity and Reliability of Instruments.....	108
4.9	Data Analysis	109
4.10	Ethical Consideration	112
4.11	Methodological Challenges Encountered during the Field Investigation	113
4.12	Summary	114

CHAPTER FIVE

	PRESENTATION AND INTERPRETATION OF SURVEY QUESTIONNAIRE FINDINGS ...	115
5.1	Introduction.....	115
5.2	General Background Information of Respondents	116
5.2.1	Distribution of participants by gender	116
5.2.2	Age of respondents	117
5.2.3	Average age of respondents	118
5.2.4	Distribution of students by their year of study	119
5.2.5	Distribution of respondents by cybertechnology skills	120
5.2.6	Distribution of respondents by years of experience using cybertechnology	120
5.2.7.	Distribution of students by average years of use of cybertechnology	121
5.3	Research Question Analysis	124
5.3.1	Relationship between course of study and cyberethics behaviour	125
5.3.2	Relationship between gender and cyberethics behaviour variables.....	126
5.3.3	Distribution of respondents' gender by age.....	129
5.3.4	Distribution of students' gender by cybertechnology skills	130

5.3.5	Distribution of students' years of cybertechnology use by gender	132
5.3.6	Relationship between age of respondents and cyberethics behaviour	133
5.3.7	Relationship between year of study and cyberethics behaviour	135
5.3.8	Relationship between cybertechnology skills and cyberethics misuse	137
5.3.9	Distribution of students' age range by cybertechnology skills.....	138
5.3.10	Relationship between cybertechnology experience and cyberethics misuse.....	139
5.3.11	Distribution of students' age range by years of cybertechnology use	141
5.4	Summary of Regression Results.....	156
5.5	Summary	161

CHAPTER SIX

PRESENTATION AND ANALYSIS OF INTERVIEW DATA.....		165
6.1	Introduction.....	165
6.2	The Findings	168
6.2.1	Level of awareness of cyber behaviour among undergraduate students	171
6.2.2	Types of cyber behaviour of undergraduate students	173
6.2.3	Challenges of students' cyber behaviour on the integrity of the university.....	176
6.2.4	The impact of the use of information technology policy in strengthening or promoting compliance with ethical conduct in cyberspace in the two universities... ..	179
6.3.	Summary	183

CHAPTER SEVEN

DISCUSSION OF THE FINDINGS		185
7.1	Introduction.....	185
7.2	Social Demographic of the Respondents	185
7.3	Respondents' Level of Awareness of Cyberethical Issues	188
7.4	Types of Cyberethics Misuse Behaviours Exhibited by Undergraduate Students at the Two Universities	194
7.5	The Applicability and Impact of Theory of Planned Behaviour on Cyberethics Misbehaviour by Undergraduate Students in the Two Institutions	197
7.6	Identifying the Challenges in Effort by Undergraduate Students to Act Ethically Correct in Cyberspace at the Two Universities	200
7.7	Determining the Impact of Cyberethics Policy in Strengthening or Promoting Cyberethical Behaviour in the Two Universities	203
7.8	Summary	206

CHAPTER EIGHT

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

8.1	Introduction.....	208
8.2	Summary of Findings.....	209
8.2.1	Characteristics of the respondents	209
8.2.2	Awareness level of cyberethics indicators	210
8.2.3	Types of cyberethics misuse behaviour.....	211
8.2.4	Applicability and impact of the Theory of Planned Behaviour (TPB) on cyberethics misuse behaviour.....	212
8.2.5	Challenges faced by undergraduate students in their efforts to act ethically correct in cyberspace	213
8.2.6	Impact of cyberethics policy	214
8.3	Conclusions.....	215
8.4	Theoretical Implication	216
8.5	Originality and Contribution of the Study.....	217
8.6	Recommendations.....	218
8.7	Recommendations for Further Studies.....	222
8.8	Summary	223
	REFERENCES	224
	APPENDIX.....	277

Tables

Table1: Application of behavioural theories in research in/on Africa as reflected in some databases.	24
Table 2: Sampling frame for selection of respondents.....	103
Table 3: Research questions, sources of data and data Analysis.....	111
Table 4: Gender representation of students.....	116
Table 5: Age range of the students.....	117
Table 6: Average age of respondents	118
Table 7: Distribution of students by year of study	119
Table 8: Distribution of students by cybertechnology skills.....	120
Table 9: Distribution of students by years of their use of cybertechnology.....	121
Table 10: Distribution of students by average years of use of cybertechnology.....	122
Table 11: Distribution of respondents by faculties/colleges of study	123
Table 12: Relationship between course of study and cyberethics behaviour	125
Table 13: Relationship between gender and cyberethics behaviour	127
Table 14: Distribution of students' gender by age	129
Table 15: Distribution of students' cybertechnology skills by gender.....	130
Table 16: Distribution of students' years of cybertechnology use by gender	132
Table 17: Relationship between age of respondents and cyberethics behaviour	133
Table 18: Relationship between year of study and cyberethics behaviour.....	135
Table 19: Relationship between cybertechnology skills and cyberethics misuse	137
Table 20 : Distribution of students' age range by cybertechnology skills	139
Table 21: Relationship between cybertechnology experience and cyberethics misuse	140
Table 22 Distribution of students' age range by years of cybertechnology use.....	141
Table 23: Respondents' level of awareness of cyberethics behaviour.....	143
Table 24: Q2: Orientation on use of cybertechnology: the level of awareness of cyberethical behaviour among students in the two universities in Nigeria and South Africa	146
Table 25: Types of cyberethics behaviour among students in the two universities	147
Table 26: Applicability and influence of theory of planned behaviour on undergraduates' cyberethics behaviour	150
Table 27: Influence of theory of planned behaviour on cyberethics misbehaviour of students in SA..	151
Table 28: Influence of each variable on cyberethics behaviour of students.....	151
Table 29: Summary of impacts of theory of planned behaviour on the students' cyber behaviour (N = 192).....	152
Table 30 : Influence of TPB constructs on cyber behaviour of students (N=192).....	152
Table 31: Influence of each variable on the cyberethics behaviour of students in the Nigerian university (N=192).....	153
Table 32: General summary of regression results for the two universities (N=380)	154

Table 33: Influence of TPB constructs on cyber behaviour of students (N=380).....	154
Table 34: Influence of each variable on cyberethics misbehaviour of students in the two universities	155
Table 35: Challenges to students' cyberethical behaviour in Nigeria and South Africa.....	157
Table 36: Interview participants	166
Table 37: Framework of this chapter	169
Table 38: Comments on orientation or specific lesson on ethical use of cybertechnology.....	172
Table 39: Types of cyber behaviour exhibited by undergraduate students	174
Table 40: Comments on challenges of students' cyber behaviour on the integrity of the university .	177
Table 41: Comments regarding policy on ethical use of cybertechnology on campus	180
Table 42: Comments regarding best ways to communicate cyberethics policy.....	181

CHAPTER ONE

INTRODUCTION AND BACKGROUND OF THE STUDY

1.1 Introduction and Conceptualisation

The purpose of this study is to investigate the cyberethical behaviour of undergraduate students of the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria. Current use of cyberspace traffic has brought with it a complex new environment of controversial ethical, social and legal issues. The current growth of 4.7 billion internet users, which is about 57.8% of the world total population (International Telecommunication Union, 2018:12), the rise in the number of cyber technologies and the profound influence of the Internet on human behaviour formed, and the backdrop of cyberethics are critical issues in the present knowledge society (Aiken and Mahon, 2014).

Cybertechnology, as used in this study, consists of a network of computer communication devices, which include but are not limited to smartphones, tablets, personal computer (desktops and laptops) (Tavani, 2011). These networked devices can be connected to the Internet or other privately-owned computer networks (intranet or extranet). Intranet is a private network within an organisation that resembles the Internet. Institutions and organisations use intranet to provide information for their employees. Typical applications include electronic telephone directories, email addresses, employee information and internal job openings. On the other hand, extranet is a private network that connects more than one organisation or institutions. Importantly, institutions use internet technologies to allow students and staff, corporate bodies, government agencies and business partners limited access to their network. The purpose is to increase efficiency and reduce costs, thus enabling users to communicate with each other by creating, editing and sharing information. The Internet, which can be differentiated from intranet and extranet in terms of strength, evolved from the United States Defence Department initiative in the 1960s (Spinello, 2011). Unlike intranet and extranet, the Internet is considered to be a public network, in the sense that much of the information on this network and connection are in the public space and are available to everyone (Tavani, 2013:8).

This invention by military initiative and the emergence of the first computing machine has led to the proliferation of technology use for communication, entertainment and manpower increase. Gaffar, Singh and Thomas (2011) argue that the rapid uptake of cybertechnology around the

world is astounding, especially with the number of new users increasing hourly. This, they claim, is due to the increase in affordable handsets and broadband connectivity. Not surprisingly, scholars contend that cyber technologies are used by individuals, organisations, institutions and governments, as means of socialisation, collaboration, communication and dissemination of information across the world (Chadwick, and Howard, 2010; Lee and McLoughin, 2010). Similarly, others argue that cybertechnology is increasingly becoming central to the learning environment by enhancing communication and collaboration among academics and their peers (Mayisela, 2013:2).

While utilising and harnessing the benefits of cybertechnology of numerous types have brought various ethical issues, many of these issues have focused on the uniqueness of the Internet and its ability to connect members of the academic community to the outside world. Cybertechnology has got to a level where it can offer numerous possibilities. However, because of the possibilities of easy access, ethical concerns have been commonly discussed by researchers in the field of cybertechnology ethics. These include, but are not limited to: access without authorisation (Walden, 2013); hacking into network (Chaabane, Manils, and Kaafar, 2010); illegal copying of licensed software (Jamwal, and Gupta, 2012); downloading inappropriate or obscene materials (Clough, 2015); infringing on software license agreements (MacCord, 2015); knowingly transmitting computer viruses (Kizza, 2015) and inappropriate representation of the university, which violates the established codes of conduct of the institution (Vanclay, Baines, and Taylor, 2013).

Cybertechnology ethical problems within universities have become more prominent and worrisome (Davinson and Sillence, 2010; Eldakak, 2010). One argument by cybertechnology ethicists generally associates an individual's ethical violation to a lack of ethics guidelines in the university setting and in the society in general (Kaufman, 2011:74). Therefore, absence of regulations guiding the use of cybertechnology may create the perception that unethical use of cybertechnology is allowed. Also, extant literature has shown that the astounding increase in speed, space, storage and continuous invention of cheap and affordable cybertechnology devices has now made the collection, search, storage access and distribution of images and information cheaper and faster (Moskowitz, 2017:6). Similarly, the lack of a unified code of ethics in cyberspace makes the prevalence of unethical use, fraud and other violations more recurrent within the academic environment, which calls for a review of these challenges to educational development (Clariana, Badia and Cladellas, 2013: 66).

The social and ethical implications of cybertechnology within the academic environment and beyond demand special attention, resulting in the creation of cybertechnology ethics (Melo and Sousa, 2017; Jamil, Shah and Tariq, 2013). The convergence of computer, the Internet and WWW (cybertechnology) and their uses have led to the new field of research called cyberethics.

The term cybertechnology ethics was chosen because it reflects the current trend in research attention to information and communications technology (ICT). The review of cybertechnology ethics or cyberethics was based on the more established fields of computer and information ethics. Computer and information ethics, as a branch of applied ethics, can be understood as that field of study that analyses social and ethical impacts of ICT (Bynum, 2008:32). The more specific term, cyberethics, is a dynamic field of study that identifies –ethical issues in the use of cybertechnology, the corresponding moral, legal and social implications and the evaluation of the social policies and laws that are framed in response to issues generated by its impact on the society (Tavani, 2013:6). The study of cyberethics, which includes computer ethics, has grown significantly since the early 1980s when Moor (1985) and Johnson (1985) published seminal papers that helped define the field, and ever since the field has grown in strength and recognition among communities of Information Science (IS) scholars. Cyberethics, as a field of applied ethics, is related to information ethics, a more general field which includes computer ethics, media ethics, library ethics and bioinformation ethics (Brey, 2009:1).

Researches have correlated cyberethics to various disciplines and behaviours related to cybercrime, such as software programme piracy, online porn, non-accredited surveillance, identification robbery and privacy violation, hacking/carding/, right/left online extremism, spamming, plagiarism and copyright infringement, fraudulent online banking, cybersquatting and cyber stalking, flaming and trolling, writing and dissemination of viruses (Quigley, 2005; Tavani, 2013). These violations all point to the concept of cyberethical behaviour, as expressed in academic environments.

It has been found that the property of cybertechnology leads to unavoidable ethical problems as a result of policy and conceptual vacuums. Most challenges of these impacts are in the realms of privacy, accuracy, property and accessibility (Moor, 1985; Mason, 1986). In this consideration, unethical cyber behaviour such as computer hacking and digital or internet piracy are the concern of this study.

Recent studies conducted in multiple countries revealed that computer hacking and digital piracy have become prevalent among undergraduate students (Hu, Xu, and Yayla, 2013; Xu, Hu and Zhang, 2013; Thomas and Ahyick, 2010).

Various studies conducted in the university context have examined factors influencing cyberethical behaviour (Alleyne, Soleyn and Harris, 2015; Martz and Shepherd, 2007; Martin and Woodward, 2011; Thomas and Ahyick, 2010). Generally, the results from these studies revealed that students did not regard unethical use of cybertechnology as any form of violation. Lau and Yuen and Park (2013) pointed out that unethical behaviours are typical and prevalent, yet understudied/underexplored among IS researchers in this part of the globe. As such, further attention is needed to address the literature gap.

In this study, the Theory of Planned Behaviour, a well-established social psychology theory for explaining human behaviour, was employed to understand undergraduates' unethical cyber behaviour. This theory has been widely applied in the study of ICT-related unethical or risky behaviour within the higher education and workplace context. Details of the theory and various related studies will be discussed in Chapter Two of this study.

Much of the concern about the use of cybertechnology in its early days was related to the apprehension about the storage and exchange of information in large databases in both private and public domains (Tavani, 2001). In developed countries, the increased value of information and easier access to cybertechnology have raised the concern for personal privacy. Therefore, this has received significant attention from philosophers, anthropologists, sociologists, educationists and academics in law and communication studies (Mason, 1986; Heersmink, Hoven, Eck and Berg, 2011). Consequently, developed and developing countries with heavy cybertechnology usage have made, or are in the process of amending, regulations with respect to privacy, in order to decrease this concern. Britz and Ackerman (2006) explain that the challenge of the current information era is the threat that cybertechnology poses to an individual's right to privacy.

Modern privacy benchmark at the international level originated from the 1948 Universal Declaration of Human Rights. It also established the protection for territorial and communication privacy. Privacy right is also found in various other international instruments. Privacy is at the core of any fledgling democratic system like Nigeria and South Africa. Constitutional provision for the protection of privacy is stipulated in the South African common law in Section 14 of the constitution of South Africa, 1996. Data protection is also an aspect of safeguarding the right to

privacy as guaranteed a legal protection in the constitution of South Africa in the processing and handling of personal information of a data subject by information technology user.. The Protection of Personal Information Act 2013 was signed into law but the provisions are fairly weak, and the risk of litigation has, historically, been low. A person's right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions (De Bruyn, 2014).

In the same vein, right to privacy is provided for in Section 37 of the Nigerian 1999 constitution. It is one fundamental right to dignity that has not received much legal attention. Equally, the Data Protection Act drafted as an instrument to guarantee protection of privacy, relating to the threat brought about by cybertechnology, is also inconsistent with the international legal obligations (Federal Government of Nigeria, 1999).

Accuracy of information is another important ethical issue. Floridi (2010:79) opines that accuracy is the degree to which information in a digital database matches true or accepted values. Considering the amount of information generated every second, the addition of inaccurate information as a result of unethical behaviour regarding cybertechnology use might cause unbearable damage to individuals or institutions. In pursuit of accurate information for nation building and promotion of democratic values, the Independent Communication Authority of South Africa (ICASA) approved the code and mechanisms of the National Association of Broadcasters on content regulations. One of its functions is to monitor the environment and enforce business compliance with rules, regulations and policies. Similarly, the Nigerian government has signed the freedom of information bill into law to enable the citizens have access to accurate and reliable information on social, economic and political issues.

According to Kuzu (2009:06), ethical issues arising from intellectual property are about the most controversial. Intellectual property is the creation of the mind or the intellect with a commercial value which includes, but is not limited to, copyright property, such as literary or artistic work, innovation, design, trading style, artistic work or literary work including computer notation or programmes. Intellectual property is the mainstay of the information industry. The laws of South Africa have identified the following as three types of intellectual property: patents, which protect inventions; trademarks, which protect the unique name or symbol identifying businesses or products; and copyrights, which protect the original works of authors, composers, artists, musicians, film-makers and software developers. Due to their intangible nature, vulnerability to stealing and unethical appropriation, creators of intellectual property are awarded some forms of

rights and protection to prevent other persons from illegal use and appropriation (Spinello, 2011; Adekola and Eze, 2015). Such rights and protection are referred to as Intellectual Property Rights. The governments of South Africa and Nigeria have laws for the protection of intellectual property in their various constitutions.

1.2 Contextual Setting

1.2.1 Law and ethics

Laws are formal written directives that apply to everyone, interpreted by the judicial system and enforced by the police. Law is defined as a legal system that comprises rules and principles set by the ruling authority to govern over the affairs of the community. Ethics are moral guidelines of human behaviour in terms of what is good or bad regarding relationship with self, others and the entire environment (Britz, 2013). It is germane to note that the attributes of law include terms like ‘consistent’, ‘universal’ and ‘enforced’. Ethics, on the other hand, cannot be enforced or compelled but are universal (Kumar, n.d.).

Recognising the ethical issues in the use of cybertechnology, the governments of Nigeria and South Africa have enacted legislations, policies and acts to address cyberethical violations and introduced regulatory measures, public policies, rules and regulations in terms of cyber law and its related terms in the constitutions of the two countries. The two nations have come up with legal frameworks to respond to the increased adoption of information technology or cybertechnology in academic, social and economic life. The main constitutional provisions in South Africa, which are particularly relevant to this study, are contained in the Right to Privacy as entrenched in Sections 14, 16 and 32, respectively. The provision includes the right to privacy, right to freedom of expression and right of access to information. There are also numerous existing policies, bills and act of the Nigerian government that describe activities related to cyberethics in Nigeria, some of which have been enacted (FOI Act, 2011; Cybercrime Bill, 2013) while others are yet to be signed by the relevant ministries or authorities.

In the next section, the available laws, acts and policies that have been enacted in the two countries will be discussed. In doing this, the standard rules governing the use of cybertechnology and conduct of cyber activities in South Africa and Nigeria will be highlighted.

1.2.2 Cyber law in South Africa

The cyber law in South Africa includes the following: promotion of access to information (Act 54 of 2002 G24250 GoN 960), Electronic Communication Amended Act (2014 G37536 GoN 266), The Regulation of Interception of Communication and Provision of Communication-Related Information Amended Act (Act 21 of 2010 G 33839 GoN 1157), Electronic Communications (Act 36 of 2005(ECA) and the Independent Communications Authority of South Africa (Act 13 of 2000(ICASA), Copyright Amended Act (Act 9 of 2002 G23556 GoN 886), Protection of Personal Information (Act 4 of 2013 G 37067), Intellectual Property Rights from Public Financed Research and Development (Act 51 of 2008 G31745 GoN 1402). The aim of this act is to guarantee the right of access to information in paper and electronic formats constitutionally. This act also contains conditions that need to be met for this access either in the public or private sectors. The objective of the Copyright Amended Act (Act 9 of 2002 G23556 GoN 886) is to guard against the unauthorised transmission of copyright work on the Internet and issues of software piracy, infringement of trademarks, as well as invention of patents and domain names.

In recognition of the provision in Section 14 of the 1996 constitution of the Republic of South Africa, which stipulates the right to privacy, the Protection of Personal Information Act (4 of 2013 G 37067) was then enacted to promote the protection of personal information processed by public and private bodies, to provide for the establishment of an information protection regulator, to predict the right of persons regarding unsolicited electronic communications and automated decision making, to predict the issuing of codes of conduct, and to regulate the flow of personal information across the borders of the Republic of South Africa.

1.2.3 Cyberethics policy of the University of Zululand

Higher institutions stress the need for some forms of policies to guide information utilisation and knowledge acquisition and development. Although there are some forms of courses that are embedded with some aspects of cyberethics at the University of Zululand (Unizulu), yet the institution has some policies guiding the conduct of research generally. In line with international and national protocols and legislation that govern the conduct of research and related activities at the university, the University of Zululand's comprehensive Policy and Procedures on Research Ethics, Policy and Procedures on Intellectual Property, Policy and Procedures on Managing and Preventing Acts of Plagiarism, and Research Ethics Guide (University of Zululand, 2014)

stipulate, among others, the university's desire for a principled conduct of research with integrity and respect for the work of others. To ensure that ethical norms and standards are adhered to, researchers conducting research at the University of Zululand are expected to comply with the requirements of the Intellectual Property Right (IPR) Act, 2008, of the Republic of South Africa. The policies include further the nature of data retention and storage of materials with the sole purpose of guiding and assisting researchers and students on ethical principles and code of conduct in research. At Unizulu, one of the first lessons of the first-year orientation class teaches freshmen how to access and use the institution's computer network securely and safely. These policy regulations and awareness are not well publicised among the generality of students, and few students, if any, have been penalised for the violation of ethical conduct. Other measures adopted by the institution include the existence of anti-plagiarism software and hands-on cyber skill for the generality of students during their first-year orientation programme. At the University of Zululand, cyberethics is taught as a core curriculum, within a broader course module in the department of information studies, to all first-year students. There are no specific modules devoted exclusively to cyberethics. The curricula of the department of information studies offers at both undergraduate and postgraduate levels some seemingly related but autonomous courses like information literacy, research methods, introduction to information science and information ethics (Ocholla, 2009).

1.2.4 Cyber law in Nigeria

There are policies, bills and acts of the Nigerian government that describe activities related to cyberethics in the country. Some of them have been enacted while others are yet to be signed into law by the relevant authorities. One of the already-enacted policies is the National ICT Policy of 2012. The objective of this policy is to provide a comprehensive framework for the ICT industry in terms of investment on expansion of networks and services that are accessible at a reasonable cost. It equally aims at facilitating the transition to a knowledge-based economy. The Cybercrime Policy of 2013 is another enacted policy. The major goal of the policy is to provide an efficient and unified legal and regulatory framework for the prohibition, prevention, detection and prosecution of cybercrime in Nigeria. In addition, it aims at promoting cyber security as well as intellectual property and privacy right. The Freedom of Information (FOI)

Act, 2011, was enacted to make public records and information more freely available, provide public access to records and information, protect personal privacy and safeguard the lives of public office holders from adverse consequences of disclosing certain official information without authorisation, as well as other related matters.

It is believed that a study in cyberethics will impact on the societies under study. It is also hoped that knowledge of the laws and ethical guidelines can be further propagated and made useful in the cyberethical world. One of the downsides of most cyber laws is that they are reactive to ethical issues. Stahl and Rogerson (2009) believe that issues and problems often come to light when technologies are developed, and as such new policies should be put in place to identify and tackle such ethical issues before they get out of hand. However, policies and laws on cyberethical issues need to be proactive to address ethical dilemma. Shinde (2013) also asserts that there are drawbacks to cyber laws, as nations still rely on outdated statutes that predate the birth of cyberspace; hence, weak penalties limit deterrence.

1.2.5 Cyberethics policy of the Federal University of Agriculture, Abeokuta

The situation at the Federal University of Agriculture, Abeokuta, is similar to that of the University of Zululand, but also different in terms of direct policy enactment on cybertechnology. Some of the objectives of the policy that are relevant to this study include: to ensure access to efficient and effective use of the institution's cyber infrastructure and to ensure that issues of safety, scope, privacy, copyright and liability are identified and managed in the best interest of the institution (FUNAAB, 2011). The policy, in accordance and compliance with the Nigerian Privacy and Personal Information Protection Act 1998 and the Health Records and Information Policy Act 2002, also ensures that data protection and disposal are done in a socially responsible manner. The limitation of these policies is the non-awareness of their existence by students due to poor publicity of the documents at relevant technological outlets on campus.

1.3 Statement of the Problem

These days, it is notable that universities provide an enabling academic environment for students to use cybertechnology for educational purposes. Rapid developments in cybertechnology have led to the formation of laws and policies, but not all users of these technologies may be fully conscious of or knowledgeable about such laws and policies. The enforcement of these laws and policies is still in its infancy in institutions in Africa. It is necessary to raise the level of awareness in regard to the importance of ethical issues related to cybertechnology. In the last few years, institutions in Africa have established computer use policies, addressing different areas of cybertechnology usage, copyright and other ethical issues. However, what the awareness level of these policies is and how they are enforced and what effects these policies have on undergraduates' cyberethics behaviour related to cyber technological ethical issues within the studied institutions

in South Africa and Nigeria need to be given special attention and emphasised through research. Students in Nigeria and South Africa use information and cyber technologies on a daily basis to perform a broad range of academic activities. There are ethical guidelines governing the use of such technology, and these, to some extent, act as the gatekeeper, preventing ethical violations. However, research indicates a lack of students' understanding of ethical use, knowledge and awareness of cybertechnology ethics, leading to decisions taken without foreknowledge about ethical responsibilities and use (Moor, 2001). Some of these unwholesome behaviours include intellectual property violations, copyright infringement, digital piracy and plagiarism. This new breed of intellectual property issues, provoked by steady commercialism of the Internet and the proliferation of websites, obviously reflects unfair dealing and trespass on ownership right of intellectual property in the information utilisation chain. Software piracy, counterfeiting in films, music, videos, books and pictures and many other vices have become worrisome in recent times (Rujoiu and Rujoiu, 2014; Udo-Akang, 2013). These unethical cyber behaviours have become a common feature among students in the university environment and may have implications for their professional life in the larger corporate society.

There are relatively few research publications on cyberethics in Africa, and the current trend in unethical behaviour in research is relatively new in this part of the world. Not much has been published on the impact of information and communications technology (ICT) on African societies and ethical use (Capurro, 2008). Furthermore, most studies on cyberethics as a concept in literature and ICT, from an ethical point of view, take their perspectives from the western philosophical tradition. A ten-year (2006-2016) structured keyword search by the researcher of relevant peer reviewed articles on cyberethics and related terms, using matching criteria on cyberethics, computer ethics and information ethics on some open access databases of Scopus and Web of Science in the fields of computer science, social science, engineering, arts and humanities, medicine, business management and accounting, produced a total of 137 publications, while the Web of Science produced 160 publications. The search analysis of these publications reveals that none of the research works emanated from Africa.

Universities perform the crucial role of bringing about change in society. Ethical and moral standards of integrity and responsibility cannot be divorced from the context in which this role is carried out. Thus, undergraduate students, as future leaders, cannot afford to neglect acceptable ethical responsibilities which are central to their role as agents of change. It is in the light of this that the researcher feels that there is the need to probe into the menace of unethical cyber behaviour

with a bid to contribute to the existing body of knowledge. In one incidence, highly-placed academic staff members were relieved of their jobs over plagiarism and falsification of data (FUNAAB, 2011). The researcher is also informed by his knowledge, experience and personal observations during his interaction with other academic staff on the issue of ethical violations. In addition, the divergent characteristics of students in the two universities under study serve to emphasise the importance of comparative studies in identifying context-specific and context-general factors that influence students toward ethical violations. Finally, the researcher is led by the desire to contribute to the reduction of the problem of unethical cyber behaviour and motivate students towards strict adherence to ethical guidelines. These, in consequence, would contribute to the existing body of knowledge in the field of cyberethics.

Although cybertechnology ethics continues to be an interesting research subject (Tavani, 2012), Most of the literature has primarily originated from the global Norths, and further empirical evidence on this phenomenon and its determinants from developing countries such as South Africa and Nigeria is warranted. Adebayo and Mabawonku, (2017) posit that more research is needed in order to test demographic variables versus ethics perceptions and education and compare the obtained findings with the findings of the multitude number of researches reported worldwide.

Given the limited empirical evidence on cybertechnology ethics, this research adopts the TPB and other variables to explore the South African and Nigerian students' behaviour towards cybertechnology ethics issues assess the possible impact of a number of individual characteristics (e.g. age, gender, years of education, and cybertechnology experience) on such attitudes. The findings of this research should extend our understanding of the cybertechnology ethics attitudes in these and hopefully and contribute to the growing body of knowledge on global information ethics.

1.4 Aim of the Study

The primary aim of this study is to therefore examine the phenomenon of ethical or unethical cyber behaviour of students' use of cybertechnology, to gain a better understanding of the factors influencing such behaviours and the contexts and conditions in which they manifest.

1.5 Research Objectives

In line with the background to the study, literature review, statement of the problem and motivation for the study, the following are the objectives of this study:

1. To determine the relationship between students' demographic variables and their cyberethics behaviour in the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria;
2. To find out the level of awareness of cyberethics behaviour among students in the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria;
3. To identify the types of cyberethics behaviour exhibited by undergraduate students in the two universities;
4. To investigate the impact of the Theory of Planned Behaviour (TPB) on the cyberethical behavioural intention of undergraduate students in the two universities;
5. To find out the challenges faced by undergraduate students in their efforts to act ethically in cyberspace at the two universities;
6. To determine the impact of cyberethics policy on compliance with ethical conduct in cyberspace in the two institutions.

1.6 Research Questions

Arising from the background to the study, literature review, statement of the problem and motivation for the study, the following research questions are set for this study:

1. What relationships exist between students' demographic variables and their cyberethics behaviour in the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria?
2. What is the level of awareness of cyberethical behaviour among students in the two universities in Nigeria and South Africa?
3. What are the types of cyberethics behaviour exhibited by undergraduate students in the two universities?
4. How does the Theory of Planned Behaviour (TPB) influence the behavioural intention of undergraduate students in the universities in Nigeria and South Africa?
5. What are the challenges to the efforts by undergraduate students to act ethically in cyberspace in the two universities?
6. Does cyberethics policy have impact on compliance with ethical conduct in cyberspace in the two institutions?

1.7 Scope and Limitation

This study was limited to the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria.

Specifically, the focus is on cyberethical behaviour and unethical use of cybertechnology, using the Theory of Planned Behaviour (TPB) as the theoretical framework guiding the study. The study concentrates on undergraduate students in the faculties of Education, Arts, Science and Agriculture, Law, Commerce and Administration at the University of Zululand, on the one hand, and colleges of Management Sciences, Plant Science and Crop Production, Biological Sciences, Physical Sciences, Veterinary Medicine, Animal Science and Livestock Production, Agricultural Management and Rural Development, Environmental Resources Management and Food Science and Ecology at the Federal University of Agriculture, Abeokuta, Nigeria. Although the study acknowledges the existence of other members of the academic community and their cybertechnology usage, however, only undergraduate students are included in the main study. The details of the distribution of the number of students in selected faculties and colleges in each of the studied institutions are well spelt out in the methodology chapter of this thesis. The ICT staff members of the studied institutions were only chosen because of the important role they play in managing the cybertechnology infrastructure of these institutions, and it was assumed they were in a better position to determine violations or otherwise of cyberethics on their campus network.

Both the quantitative and qualitative research methods are used to study natural, social and cultural phenomena in the humanities. Neither of these two methods is intrinsically better than the other; hence, their choice by the researcher is determined by the context, purpose and nature of the research endeavour. This study used a cross-sectional exploratory mixed study. The mixed exploratory design was chosen because it is suited to the systematic discovery of students' attitudes towards cyberethics behaviour. The intent was to discover generalisable attributes that deal with the present condition of undergraduate students' cyberethics behaviour in the studied universities. The adopted design and methods will guide in examining and analysing what is naturally occurring in the studied context and equally help in developing a picture of the prevailing situations. Thus, the survey instruments of questionnaire and structured interview were employed in this study. Upon data collection, descriptive and inferential statistical methods were utilised for data analysis. Descriptive statistics for the survey data included means and frequency distributions. Inferential statistical methods that were suited for the study included correlation, simple regression and multiple regressions.

1.8 Intended Contribution to Knowledge

The adoption of the Theory of Planned Behaviour (TPB) as the underpinning framework is most suited for the study because it includes personal normative and control factors that may influence the intention that determines behaviour in cyberspace and, hence, provides useful contribution to the body of knowledge. The behavioural theory used in this study, Theory of Planned Behaviour (TPB), has been widely used in a range of behavioural intervention studies. However, it has not been widely used or applied in cyberethics studies in Africa, much less in South Africa and Nigeria. The current results enhance the comprehensive of the relationship between cyberethics factors and their effect on undergraduate students' intention towards observing or violating ethics of cyberspace. The study is one of the first studies to evaluate the cyberethical behaviour of undergraduate students from two different comprehensive and specialised universities in Africa.

In addition, the literature on behavioural models, particularly the Theory of Planned Behaviour (TPB), indicates that an increased understanding and awareness of the underlying factors involved in cyberethics behaviour is possible. The outcome of this study indicates that the Theory of Planned Behaviour (TPB) is useful in exploring and determining the underlying assumption of cyberethics behaviour.

The statistical analysis of the data collected using questionnaire enabled the discovery of the kinds of cyberethical behaviour prevalent among undergraduate students who participated in the study. The subsequent interview conducted with staff at the ITS/ICTREC sections of the two institutions enabled the understanding of various cyberethical behaviours and their influencing contextual factors. Thus, it is possible to propose measures for the prevention of cyberethics misuse behaviour. The survey instrument from the study could be used to assess differences in understanding, awareness and perceptions of undergraduate students' knowledge of what constitutes cyberethical behaviours as students' progress through their degree programmes.

The practical value of this study is in its benefit to other researchers who may be attempting to understand South African or Nigerian cybertechnology users' behaviour. It will also help policy makers and relevant educational authorities to get relevant understanding of their students' behaviour in the realm of cyberspace. Future studies on cyberethics in the academic field will also improve the current knowledge on undergraduate students' cyberethics behaviour, which has witnessed a dearth in literature originating from the two countries of South Africa and Nigeria compared to the developed world of Europe and the Americas.

1.9 Methodology Overview

Bellamy (2012) described a method as the set of techniques accepted by most scientists as the appropriate means for collecting, coding, organising and analysing data. This study will adopt a survey research method, which involves the use of multiple data sources from selected categories of staff and students of the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria. Multiple data collection methods (quantitative and qualitative) are deployed to conduct the research, as they are more appropriate methods which allow data to be collected from large samples, due to their relative time- and cost-effectiveness (Gray, 2014).

Both the quantitative and qualitative research methods are used to study natural, social and cultural phenomena in the humanities. Neither of these two methods is intrinsically better than the other; hence their choice by the researcher is determined by the context, purpose and nature of the research endeavour. This study used a cross-sectional exploratory mixed study. The mixed exploratory design was chosen because it is suited to the systematic discovery of individuals' attitudes towards cyberethics behaviour. The intent was to discover generalisable attributes that deal with the present condition of undergraduate students' cyberethics behaviour in the studied universities. The adopted design and methods will guide in examining and analysing what is naturally occurring in the studied context and to equally help in developing a picture of the prevailing situations. Thus, the survey instruments of questionnaire and structured interview were employed in this study. Upon data collection, descriptive and inferential statistical methods were utilised for data analysis. Descriptive statistics for the survey data include means and frequency distributions. Inferential statistical methods that were suited for the study included correlation, simple regression and multiple regressions.

1.10 Definition of Terms

The following terms have specific meaning in the context of this study on cyberethics behaviour:

Attitude: In this study, attitude represents the positive or negative evaluation of students' engagement with digital piracy of music or films and unethical use of cybertechnology. For instance, students who hold positive evaluation of unethical cyber behaviour will likely engage in digital piracy and unethical use of cybertechnology. In contrast, students who hold positive and favourable evaluation of cyberethics behaviour are not likely to engage in unethical cyber behaviour and may view digital piracy as an unfavourable option.

Awareness of cyberethics: Awareness of cyberethics refers to knowledge of and access to information about how the Internet should be used in various contexts. It means an exposure to the rules governing cyberspace from informal or formal source. It encompasses being conversant with the laws governing the use of the Internet and the likely punishments or penalties that accompany the violations of such laws.

Computer and information ethics: In the present essay, the term is understood as that branch of applied ethics which studies and analyses the social and ethical impacts of ICT.

Cyberethics: Cyberethics is based on codes, providing guidelines for proper behaviour on the Internet for the good of the individual and society (Bawa & Marwah, 2011).

Cybertechnology: As used in this study, it consists of a wide range of computing networked communication devices which include, but are not limited to, smartphones, tablets, personal computers (desktops and laptops). These networked devices can be connected to the Internet or other privately-owned computer networks (intranet or extranet).

Ethics: This is a set of rules and principles helping people distinguish right from wrong (Kizza, 2013).

Extranet: This is a private network that connects more than one organisation or institution.

Intranet: This is a private network within an organisation that works like the Internet. Institutions and organisations use the intranet to provide information to their employees. Typical applications include electronic telephone directories, email addresses, employee information and internal job openings.

Normative beliefs or subjective norms: They reflect the perceptions that individuals have about the beliefs of others who they consider important, such as peers, faculty or family members (Harding, 2007). Specifically, in this context, it is the perception that a student has about whether others will approve or disapprove of his or her cyberethics behaviour.

Privacy: Privacy or information privacy is a term in cybertechnology ethics, which implies an interest held by an individual regarding the control and handling of data about themselves.

1.11 Structure of the Thesis

The following chapters are presented in systematic and logical arrangements:

Chapter one: This chapter provides a general introduction and background to the entire study,

as well as a justification for the choice of theoretical framework adopted in the thesis. It includes background to the study, statement of the problem, contribution to the study, research problems/questions, and the research objectives. The research information gathering methods are also provided, as well as the terminology used for the purpose of the thesis. Finally, the chapter concludes with an overview of each chapter of the thesis.

Chapter two: This chapter deals with the theoretical framework. It provides an overview of relevant literature on the theoretical framework chosen for the study. The aim is to provide the readers with a thorough understanding of the existence, value and purpose of attitude theory linked to human behaviour. The purpose of the Theory of Planned Behaviour (TPB) is defined and the constructs of the theory and their functions are outlined. In addition, the strengths, weaknesses and criticisms of the theory and its relevance to the study are equally discussed. Lastly, the chapter ends with the implications and summary.

Chapter three: This chapter presents a critical and exhaustive review of related studies tied to the conceptual variables of the study.

Chapter four: This chapter provides a detailed analysis of the research methodology for the thesis, specifically the methodology used to address the stated problems in the objectives and research questions. This part of the thesis is extensive, as it not only embodies methodological considerations, but also a practical perspective on the phenomenon of cyberethics behaviour.

Chapter five: This chapter discusses the results of the data analysis. Having laid the theoretical groundwork for the actual analysis of the survey, this part presents the findings of this investigation.

Chapter six: This chapter is a discussion of the findings of the study. Through this discussion, the thesis addresses the research questions, as well as examines the practical implications of the findings.

Chapter seven: In the seventh and final part, the study answers the research questions. This is followed by a summary and recommendations, as well as a discussion about the limitations of the study and the implications for future research.

1.12 Summary

The advent of cybertechnology has become an essential tool necessary for effective learning among university students. Students in the universities are expected to use cybertechnology tools to enhance their studies. Extant literature reveals that many students engage in the use of the resources for various unethical purposes. One of the current challenges facing information seekers is how to access and use information without violating any ethical rules. Perhaps nowhere is this challenge more evident than in a university setting, especially when providing cybertechnology resources to a diverse and widespread student population. The possibilities and advantages that cybertechnology affords undergraduate students come with their drawbacks if inappropriately used, regardless of intent.

The background to the research has been discussed in this chapter, and the methodology to be adopted has been elaborated on. The purpose of this research endeavour is to explore, through a cross-national investigation, the cyberethics behaviour of undergraduate students in selected universities in South Africa and Nigeria. The Theory of Planned Behaviour (TPB) as a theoretical lens was adopted to enable a thorough analysis of the cyberethical intentions and attitudes of the participants. Understanding students' cyberethical attitudes and behaviours will inform the development of knowledge and awareness of cyberethics, which will in turn provide management with the tools to help guide ethical conduct and students' moral appreciation of the integrity of academic institutions. Information technology plays an integral part in the world of today, particularly in academic environments. Ethical values in cyberspace are very essential, particularly in maintaining a good relationship between university students and their activities in cyberspace, in order to prevent misuse and ethical breaches. Ethical consideration is also a necessary ingredient for shaping technological usage in order to promote acceptable behaviour. It is indispensable in shaping technology in a socially acceptable and sustainable way (Grunwald, 2000:181).

CHAPTER TWO

THEORETICAL FRAMEWORK

2.1 Introduction

The knowledge of theory is central to the framework of a research study because it is like the spectacle or lens through which various research studies can be linked. A theory shapes and directs the vision of a study. Implicitly, it means that a theory allows the researcher to articulate what is theoretical and what is worth being emphasised (Jonker and Pennink, 2010). Knowledgeable use of theories significantly strengthens the value of investigations (Creswell, 2002). Theories are central to research practice because they are the concepts by which researchers explain their findings. Therefore, research findings that are theoretically linked to other research works will make more substantial contribution to the knowledge fabric of a given discipline than those which are not (Grant and Osanloo, 2014:13). It could then be argued that a research that is not theory-based does not offer a cohesive, meaningful explanation of new discoveries in a subject area. In the same vein, Morrow and Tracey (2006:7), in their book *Lenses on Reading: An Introduction*, note that theoretically disconnected studies have far less opportunity of making meaningful contribution to knowledge in their field of study.

Extant literature has shown the need to separate theoretical framework from literature review. Rocco and Plakhotnik (2009:4) argue that the theoretical framework chapter in research dissertation provides direction for all aspects of the study, from the philosophical ideas to data collection and analysis. Similarly, Grant and Osanloo (2014:13) see theoretical framework as the blueprint for the entire research inquiry. It guides the researcher in the selection of topic, development of research questions and literature review, selection and execution of the methodology and the planning and ordering of the analysis. Therefore, this study will be guided by this trend and will equally discuss some useful literature on the theory that constitutes the framework for this study.

2.2 Theory and Model

In an attempt to address the research objectives and questions of this study, a close look at the following terms is essential: theory, model, conceptual framework and theoretical framework.

Researchers have often used theories and models harmoniously in their studies, as theoretical lens guiding their studies. This is because theories and models help in describing the connections that

exist between variables in the study. There are significant differences in opinion on the definition of theory. Theory has been defined in various ways by social and behavioural scientists. Kerlinger (1980) defines theory as a set of interrelated concepts, definitions and propositions that present a systematic view of phenomena by specifying relations among variables, with the purpose of explaining and predicting phenomenon. Likewise, Coreil (2010:69) sees theory as a set of interrelated concepts, constructs and propositions that present a systematic view of a domain of study for the purpose of explaining and predicting phenomena. In other words, theory is a concept that summarises and organises, providing tentative explanations for phenomena and equally providing bases for making predictions.

Although there are differing opinions as to what constitutes a theory, a comparison of the diverse opinions on what constitute the qualities of a good theory is important. Mintzberg (2017:179) claims that a good theory should be functional, strong, parsimonious and valid. Wacker (1998) also opines that the operationalisation of the definition of theory should directly be tied to the necessary components of theory. According to Walker and Sinclair (1998), a theory is composed of four components: definitions, a domain of applicability, a set of relationships of variables, and specific predictions or factual claims. Littlejohn, Stephen and Foss (2010:29) argue that a good theory must be stated explicitly with the aim of formulating a logically consistent and mutually interdependent body of knowledge. They go further to describe the four functions of a theory as descriptive, delimiting, generative and integrative. Based on the description by Littlejohn, Stephen and Foss, Thompson (2017) reacted that for a theory to have scientific value, it must go beyond the simple propositional level. This implies that a theory in a research study is the framework that holds science together and enables the researcher to build on the works of others.

In many fields of study, including information studies, the terms model and theory are sometimes used interchangeably. However, having the terms refer to similar things is problematic (Caputi, Hunter and Tan, 2009:498). Theories, as used in many researches, are abstract. They are used in explaining phenomena so as to enable predictions to be made. On the other hand, the term model is narrower in scope. According to Coreil (2010), and Caputi, Hunter and Tan (2009), a model is an exploratory device for organising the components of a domain of phenomena to show relationships between the parts and the outcome of interest. They are analogies that assist the researcher in explaining and conveying the central principles or ideas of a theory. Using symbolic diagrams as a model is a schematic representation of ideas and the specific relationship that exists among phenomena (Tarkang and Zotor, 2015:2). A model is also seen as a description of an

analogy that helps researchers to understand something usually unseen or complex (Graziano and Raulin, 2010:3). This seems to imply that constructing and using a model in research helps behavioural scientists to organise knowledge and hypothesis about the reality represented by the model. Importantly, models are not theories; they rather assist in explaining a theory. Hence, they do not replace theory (Valentine and DuBois, 2005, in Caputi, Hunter and Tan, 2009:15).

Ranganatham, Krishnaswami and Anand (2010) describe a conceptual framework as a simplified systematic conceptual structure of interrelated elements of a body of knowledge in some schematic form, such as a narrative statement or mathematical equation. Similarly, Imenda (2014:189) defines conceptual framework as the end result of bringing together a number of related concepts to predict or explain a given event or give a broader understanding of the phenomenon of interest of a research problem. This evidence suggests that theoretical framework provides assumptions, schematic concepts and forms of explanation in scholarly research. Theoretical framework refers to the theory that a researcher chooses to guide his research (Imenda, 2014:187). Rocco and Plakhotnik (2009:4) affirm that the scaffolding frame of any research structure is the theoretical framework.

There is no doubt that utilising a theoretical framework is central to a research. It serves as the structure and support for the rationale of the study, the problem statement, the purpose, the significance and the research questions. Theoretical framework provides a grounding base or an anchor for the literature review and, most importantly, the methods and analysis. Lysaght (2011:570) highlights the necessity of identifying one's theoretical framework for a dissertation study. Drawing inference from the foregoing, a theoretical framework is the synthesis of existing related theories and concepts in a research study, without which the structure and vision for a study is unclear - much like a house that cannot be constructed without a blueprint (Grant and Osanloo, 2014:12).

2.3 Overview of Related Theoretical Framework on Cyberethics Behaviour

Different theories and models exist in the literature regarding the field of cybertechnology ethics, but only a few of them are being used in publications by researchers and authors. Theories or models that are often used in a field of study shape and inform the scope of practice and equally determine the socialisation and training of its experts and practitioners. Studies evidence and a number of empirical investigations have indicated that no single theory or conceptual framework dominates in the studies on cybertechnology ethics and education (Schepers et al, 2014; Glanz and

Bishop, 2010). However, extant literature published in the past two decades have shown the most adopted theories in cyberethics behaviour research. It is essential to note that the process of grounded theory and substantive theory produces four primary constructs: (a) heuristics (expansion of the existing body of knowledge, discovery and problem solving), (b) description, (c) delimitation, (d) parsimonious (Udo-Akang, 2012:91).

Different theories exist in the literature regarding cyberethics behaviour. They are grouped under ethical decision theory or model and behaviour adoption theories:

1. Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975)
2. Theory of Planned Behaviour (TPB) (Ajzen, 1985)
3. Technology Acceptance Model (TAM) (Davis, 1993)
4. Combined-TAM-TPB (Taylor and Todd, 1995)
5. Model of PC Utilisation (MPCU) (Thompson et al., 1991)
6. Motivational Model (MM) (Davis et al., 1992)
7. Social Cognitive Theory (SCT) (Bandura, 1991)
8. Moral Intensity Model (Jones, 1991)
9. General Theory of Marketing Ethics (Hunt and Vitell, 2006)
10. Self-Control General Theory of Crime (Gottfredson and Hirschi, 1990)

The models and theories above are classified as behavioural intention models and are being adopted in information and cybertechnology ethics-related studies. The models and theories focus on behavioural intention as an important determinant of technology usage (Kufafka, Johnson, Linfante and Allegrante, 2003). The Theory of Reasoned Action (TRA) and Technology Acceptance Model (TAM) are included in this list because these models explain why people behave the way they do in relation to cybertechnology usage. For the purpose of this study, the Theory of Planned Behaviour (TPB) will be used as an intervening theory to investigate the cyberethics behaviour of undergraduate students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria.

Theoretical approaches to cyberethical studies that have relied on social psychology models of

behaviour change seek to identify determinants and pathways of influence of cyberethics behaviours, such as ethical and unethical use of cybertechnology (Coreil, 2010). In a related development, Harding, Mayhew, Finelli and Carpenter (2007:256) suggest a robust theoretical framework and intervention to improve the understanding of the underlying psychological mechanisms that are involved in students' ethical decision-making. Related selected key constructs/variables that have received particular attention in the field of cybertechnology ethical theory usage include facilitating conditions, performance expectancy, effort expectancy, social influence, experience, attitude, subjective norms, intention, perceived behavioural control, self-efficacy and outcome expectancy.

2.4 Application of Behavioural Theories in Research in/on Africa as Reflected in Some Databases

This study completed a review of extant literature on cyberethics and behavioural theories. The review was confined to empirical research published between 2007 and 2017, generally on the Theory of Planned Behaviour (TPB). Electronic databases such as SCOPUS, Web of Science, Google scholar, IEEE, Ebsco Host and Sabinet e-publication had been searched to determine the number of articles which have used the TPB on issues in Africa and on Africa from different nations. The justification for searching those unique databases is primarily based on the statement by Sampson, McGowan, Cogo, Grimshaw, Moher and Lefebvre (2009) that the electronic databases in a study must incorporate a vast number of theoretically applicable papers, reviews and reports of grey literature which are peer reviewed. The searches were performed using established procedures set out in literature (Randolph, 2009). The review equally adopted the keyword search and relevant peer reviewed articles along matching criteria on the issues of cyberethics, as well as the theories and models highlighted in Table 1. Other search combinations have been applied to retrieve applicable literature from electronic databases, including material on concepts of Planned Behaviour and Cyberethics, TPB and Computer Ethics, Planned Behaviour and Net Ethics, and Cybertechnology Behaviour and Reasoned Action, among others. Studies have been included in this review based on the criteria of title, abstract, key phrases, completeness and publication in the English language (Aderibigbe and Ocholla, 2019).

Table 1: Application of Behavioural Theories in Research in/on Africa as Reflected in Some Databases

Theories	Ebsco	Scopus	WOS	GS	IEEE	Sabinet e-publication
TRA	53	1	1	24	49	1
TAM	44	16	1	21	642	0
TPB	87	11	4	52	1	1
MPCU	0	2	46	2	56	0
MM	6	13	0	3	112	0
SCT	300	7	0	16	113	0
MIT	5	1	190	3	56	0
GTME	24	5	31	77	56	0
SCGTC	26	2	491	0	54	0

The above results are from all fields, including full text containing the following theories: Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), Model of Personal Computer Utilization (MPCU), Motivational Model or Theory (MM), Social Cognitive Theory (SCT), Moral Intensity Model (MIM), General Theory of Marketing Ethics (GTME) and Self Control General Theory of Crime (SCGTC). The content contains research publications from 2008-01-01 and 2017-12-01 on the major database in the field of information studies. **The findings presented in the table show a growing acceptance and use of TPB in scientific research investigation to predict human behaviour and hence, justify the choice of the TPB for the study**

2.5 Description of the Theory of Planned Behaviour

The theoretical framework for this current study is the Theory of Planned Behaviour (TPB). Social, psychological and knowledge factors have been shown to influence an individual's cyberethical decision. Social cognitive approaches to understanding the reasoning behind cyberethics behaviours have frequently used the Theory of Planned Behaviour. According to the theory, the stronger the subjective norm, the stronger the intention to perform a targeted behaviour (Ajzen, 2011). This implies that individuals experience social pressure from their referents not to engage in a targeted behaviour. This may compel them to desist from engaging in the behaviour.

The Theory of Planned Behaviour traces its origin to the expectancy-value theory (EVT), which evolved into the Theory of Reasoned Action (TRA) and later into the Theory of Planned Behaviour. The popularity and acceptance of the Theory of Planned Behaviour by researchers is

based on the amount of variance explained in behavioural intention and behaviour (Ajzen, 2011:1). A review of 185 studies applying the theory provided the evidence that it accounted for an average of 27 per cent variance in actual behaviour and 39 per cent in behavioural intentions (Armitage and Conner, 2001).

The Theory of Planned Behaviour (Ajzen, 1985, 1991) is an extension of the theory of reasoned action (Ajzen and Fishbein, 1980). The theory of reasoned action assumes that attitude and subjective norms are the determinants of the individual's intentions to carry out a given behaviour. In other words, the intention to perform behaviour correlates with actual behaviour. This theory has provided a strong support for determining volitional behaviour and has been used by researchers in various fields of human endeavour to understand the social cognitive processes of human behavioural decision making.

The addition of perceived behavioural control (PBC) to the theory of reasoned action (TRA) brought about the Theory of Planned Behaviour (TPB) (Ajzen, 1991). The Theory of Planned Behaviour assumes that behavioural intention is the strongest determinant of actual behaviour, while the direct determinants of individual behavioural intentions are attitudes, subjective norms and perceived behavioural control (PBC) (Ajzen, 1991). The Theory of Planned Behaviour (Ajzen, 1991) and its predecessor, the theory of reasoned action (Ajzen and Fishbein, 1980), have been used extensively in research on a wide range of social and human behavioural studies, particularly those associated with the ethical use of cybertechnology (Attuquayefio and Addo, 2014; Goles, et al., 2008; Taylor and Todd, 1995), digital piracy (Yoon, 2010; Liao, Lin and Lin, 2010), unethical behaviour (Chatterjee, Sarker and Valacich, 2015), perception of cybertechnology ethics (Chiang and Lee, 2011), and academic dishonesty (Harding, Mayhew, Finelli and Carpenter, 2010).

In practice, researchers have generally considered the Theory of Planned Behaviour as a choice for explaining behaviours where ethical considerations are an issue. Some have sought to add variables or constructs to the Theory of Planned Behaviour: for instance, ethical predispositions (d'Astous, et al, 2005), moral obligation and aspects of law (Gole, et al, 2008), deterrence effects (Kwong and Lee, 2002), and to synthesise the Theory of Planned Behaviour with other models (Taylor and Todd, 1995; Shemroske, 2011; Chan, 2015).

Behavioural intention is seen as the readiness or an indication to perform a given behaviour (Ajzen and Fishbein, 2005). It is equally considered as the immediate antecedent of behaviour. In other words, intention corresponds to an individual's estimate of the likelihood that a specific behaviour

will be performed within a certain timeline. Intention is singled out as the most proximate determinant of behaviour because cyberethics-related actions are usually adopted in a conscious or planned manner (Ajzen, 1985). Individual intention to perform the target behaviour is strengthened by the level of control the individual has over the performance of the target behaviour (Ajzen, 2002). In other words, if the individual holds a strong intention to engage in the target behaviour, then the likelihood of the behaviour being carried out is increased.

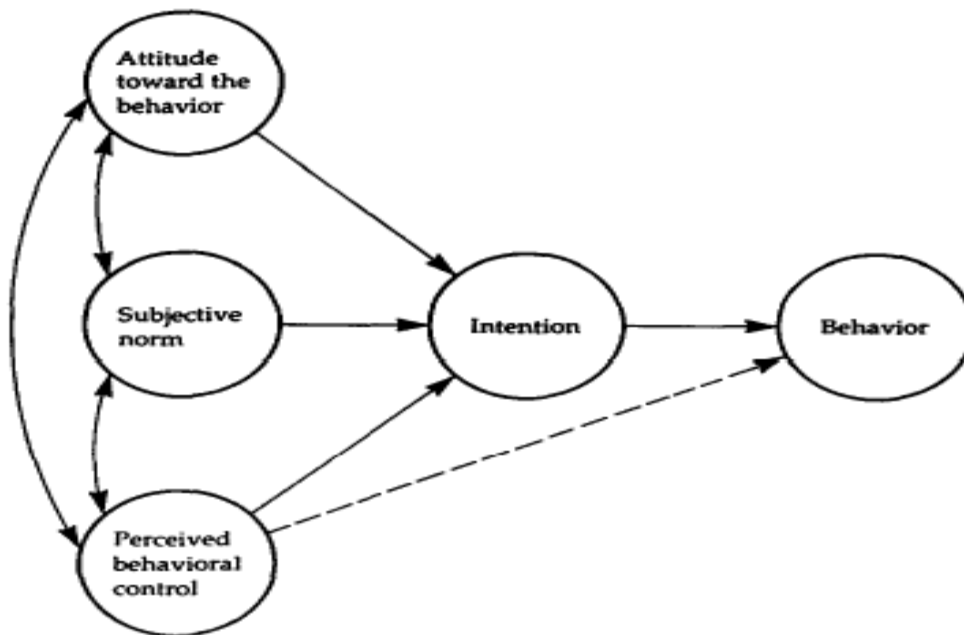


Figure 1: Theory of Planned Behaviour (Ajzen, 1991)

Figure 1 shows that there is a significant relationship between each of the IVs (attitude toward behaviour, subjective norms, and perceived behavioural control) and behavioural intention. Also, behavioural intention is also shown to influence actual behaviour of interest.

2.6. Theory of Planned Behaviour Constructs

Several theories and models - such as social cognitive theory, privacy, accuracy, property and accessibility (PAPA), self-determination theory, protection motivation theory, deterrent theory and Theory of Planned Behaviour (TPB) - have been adopted in studies over the past decades to improve understanding of the antecedents of engaging in questionable behaviour. Among these, the Theory of Planned Behaviour is a prominent model that has been proven to be effective, parsimonious and versatile in examining the antecedents of cyberethics behaviour among students. According to the Theory of Planned Behaviour, behavioural intention is influenced by three factors: attitude, subjective norms and perceived behavioural control (PBC) (Ajzen, 1991). These

factors all work together to influence students' intention to engage in digital piracy and unethical use of cybertechnology.

2.6.1. Attitudes

Attitude towards behaviour is one of the factors or predictors of behavioural intention, and one of the two initial constructs from the theory of reasoned action. Attitude towards behaviour is the degree to which an individual's performance of a behaviour is positively or negatively valued.

Individual attitude differs from belief because it reflects some disposition toward the object of attention. Consequently, an individual's attitude toward cyberethics behaviour may range from negative to positive on a continuum. Attitude, as with other constructs and determinants of intention in the Theory of Planned Behaviour, is influenced by a set of beliefs. Attitudes towards a certain behaviour are determined by the individual's evaluation of the behaviour and the magnitude of engaging in that particular behaviour. The theory assumes that if one recognises the outcomes of a behaviour to be positive and ascribes a high value to such consequences, then his or her attitude towards the behaviour is favourable (Ajzen, 1991:183). This in turn is thought to influence the individual's intention to perform the given behaviour and, consequently, his or her decision to engage in the behaviour (Ajzen, 1991). In general, the more positive the attitude, the stronger the intention to perform or carry out a behaviour would be (Armitage and Conner, 2001). Intentions, in the Theory of Planned Behaviour, are the antecedents of behaviour (Ajzen, 1991, 2002). According to Ajzen (2006:1), given a sufficient degree of actual control over the behaviour, people are expected to carry out intentions when the opportunity arises. In other words, when benefits are perceived to outweigh the cost of performing the action (that is, when attitudes and social norms regarding digital piracy and unethical use are favourable and perceived behavioural control is high) digital piracy and unethical use will likely occur.

The expectancy-valued model of attitude (Ajzen and Fishbein, 2005) conceptualises beliefs as antecedents of attitude. Belief, as an influence on attitude, is defined as the subjective probability that an object has a certain attribute. Therefore, attitude towards a given behaviour and beliefs become behavioural beliefs, as they are related to a specific behaviour. Although attitude can influence a person's intention and actual behaviour, studies have shown that the correlation between attitude and behaviour is often weak (Ajzen and Fishbein, 1980; Echebarria-Echabe, 2013; Kollmuss and Agyeman, 2002). Other survey research works that elicit responses on generalised attitudes faintly predict specific behaviours (Myers, 1999). Studies have also shown

that the strength of the correlation between attitude and behaviour improves with greater specificity (Henderson-Redmond, Guindon and Morgan, 2016). For example, specific attitudes to recycling have been shown to correlate with recycling behaviour (Vining and Ebreo, 1990). Specific attitudes toward recycling also correlated with recycling intention (Taylor and Todd, 1995).

2.6.2. Subjective norm

Subjective norm (SN) is a construct conceptualised as the social pressure or perceived social pressure to perform or not to perform a given behaviour (Ajzen and Fishbein, 2005). Subjective norms refer to people's perceptions of how their reference group or significant others (those they think about when assessing what is normal and socially approved) think or feel about the behaviour. The concept was first formulated in the initial formulation of the reason action approach as social norm and defined as the individual's perception that most people important to them think they should or should not perform a specific behaviour (Ajzen, 1991). If an individual believes a behaviour to be considered acceptable by his or her social group, the individual is more likely to report intention to perform the said behaviour (Ajzen, 1991). It is assumed that subjective norm is determined by the total set of accessible normative beliefs concerning the expectations of important referents: that is, whether important referent individuals approve or disapprove of performing the behaviour weighted by the person's motivation to comply with those referents. For instance, a person who believes that certain referents think that he or she should perform a given behaviour, and who is motivated to meet their expectations, will hold a positive subjective norm. Conversely, a person who believes these referents think that he or she should not perform the behaviour will have a negative subjective norm, and a person who is less motivated to comply with those referents will have a relatively neutral subjective norm (Ajzen, 2006).

Similarly, applying the social norms theory, Berkowitz (2005) found out that peers had an influence on young adults' involvement in unethical behaviour. Equally, based on the social learning theory (Bandura, 1986), it is postulated that humans learn by observing their peers. Studies have also shown the relationship between differential association and cyberethics behaviour in areas like computer crimes (Holt, Bossler and May, 2012). From the foregoing, it can be inferred that peer influence is an environmental determinant of both personal factors and behaviours.

The role of subjective norms in cybertechnology and related studies is ambiguous and to date only weak correlations have been established between behaviour and subjective norms (Taylor and Todd, 1995). However, Armitage and Conner (2001) suggest that this issue is most likely to be

methodological and they state that the few studies which measured subjective norms appropriately have actually illustrated their reasonably strong relationship with behaviour.

2.6.3. Perceived behavioural control

Perceived behavioural control (PBC), an addition to the previous model of the Theory of Reasoned Action (TRA), is the third construct in the Theory of Planned Behaviour (TPB). Perceived behavioural control is seen as the ability or the degree to which an individual can wilfully engage in a particular behaviour. Students will intend to perform cyberethics behaviour when they evaluate it positively, when they experience social pressure to perform it, and when they believe that they have the means and opportunity to do so (Ajzen, 2005). It is regarded as synonymous with Bandura's concept of self-efficacy or confidence in one's own ability (Ajzen, 1998; Bandura, 1998). It is also a reflection of the beliefs of the availability of resources and opportunities in order to perform the behaviour (Ajzen, 1991, 2005; Taylor and Todd, 1995). In other words, it is linked to how easy/convenient or difficult/inconvenient it is to perform a certain behaviour. The antecedents of perceived behavioural control are control beliefs, which are based on the perception that one has or does not have the ability to carry out the behaviour (Ajzen and Fishbein, 2005).

While control beliefs influence students' perceptions of behavioural control, perceived behavioural control (Ajzen, 2006) refers to resources that impede engagement in the behaviour (Ajzen, 2005). Strong behavioural control is characterised by a belief in one's ability to successfully accomplish a desired task (such as digital piracy and unethical use of cybertechnology) (Ajzen, 2006). Based on this study, students who have high motivation for unethical behaviour are more likely to engage in digital piracy and are more likely to believe that they can engage in digital piracy and unethical cybertechnology use and get away with it. Conversely, those who express strong feelings of control over their cyber behaviour are less likely to engage in digital piracy and unethical cybertechnology use.

Perceived behavioural control is based on students' past experiences with digital piracy and unethical use and their perceptions of their ability to control factors in their environment that either facilitate or inhibit their ability to perform unethical cyber behaviour. In general terms, the more favourable a student's attitudes are toward digital piracy and other anti-social behaviours, the stronger his or her perceptions are that norms support cyber behaviour violations, and the stronger his or her perceptions are that he or she can control the outcome of their cyber behaviour, the more likely he or she will be to engage in digital piracy and unethical cybertechnology use (Yoon,

2011:407).

Perceived behavioural control comprises two main aspects. First, it depends on the degree to which individuals intellectualise themselves as suitably competent, self-controlled and able to perform some action, called internal control, which overlaps with the concept of self-efficacy (Ajzen, 1991:186). Second, perceived behavioural control depends on the extent to which individuals feel that other factors, such as the cooperation of colleagues, resources or time, could prevent or facilitate the behaviour, called external control (Jawahar et al., 2012). In other words, perceived behavioural control is determined by:

- Control beliefs: The inspiration to behave in a certain way, inclined by the perception of how hard the behaviour is likely to be;
- Perceived power: The incentive to behave in a certain manner, inclined by the perception of how positive that behaviour is likely to be (Ajzen, 2002:667).

Perceived behavioural control (PBC) is important in explaining people's behaviour, especially when they do not have whole control due to situational factors (Chiou, 1998). Situational factors such as free access to university Wi-Fi, as well other internal factors, including their knowledge of how to use cybertechnology, will determine the cyberethics behaviour of students and their perceived behavioural control. A high perceived behavioural control is linked with behavioural intention and subsequent execution of the behaviour when the perceptions of control accurately reflect actual control (Ajzen, 1991; Armitage and Conner, 2001). In addition, intention to perform an action does not always end in the performance of the behaviour. Perceived behavioural control is relatively, but not totally, related to actual behavioural control (Armitage and Conner, 2001), which in turn affects the extent to which intentions are linked with the corresponding behaviour. Perceived and actual behavioural control can sometimes differ, such as when individuals are unaware of factors that can hinder or facilitate the intended behaviour.

2.7 Strengths of the Theory of Planned Behaviour

One of the major strengths of the Theory of Planned Behaviour is that it is widely applicable to a variety of behaviours in different contexts, including such diverse areas as health, communication, environmental concern, risk communication, mass transit use and technology adoption. It is also easy to understand and, subsequently, has been used by hundreds of researchers (Knabe, 2012). While the sense of understanding of each theory primarily lies in each scientist's own mind, previous use of a theory is a strong indicator of its comprehensibility and utility (Reynolds, 1971).

In broad terms, the theory is well-supported with empirical evidence. Intentions to perform behaviours of different kinds can be predicted with high accuracy (Ajzen, 1991).

The Theory of Planned Behaviour is also parsimonious. This is an important characteristic because the simplicity of a theory is a quality associated with strength and utility of theories (Zuidema, 2007). In other words, the more times a theory is used and understood, the more it is accepted by the scientific community. In the case of the Theory of Planned Behaviour, the use has increased significantly in the last decade, with more than 1,000 published studies utilising the theory (Nguyen, Nham, and Hoang, 2019). It is one of the most successful frameworks for studying determinants of cyberethics behaviour because it accounts for a substantial amount of variance in intention and behaviour. Social cognitive approaches to understanding the reasoning behind cyberethics behaviour have often used the Theory of Planned Behaviour. The theory has been a dominant model and framework that has been used to guide research on health-related behaviour for the past three decades (Sniehotta, Pesseau, and Araújo-Soares, 2014). The concepts of the theory are precise, and the theory can be flexible when applied in non-western countries or environments. This is due to the fact that some of its constructs are global and, therefore, could be used to determine the cyberethics behaviour of students in academic environments, especially in universities in South Africa and Nigeria.

2.8 Criticisms of the Theory of Planned Behaviour

Researchers have criticised the model. Although the framework has provided factors that may influence an individual's intention to engage in some behaviours, a review of 237 independent prospective tests found that the Theory of Planned Behaviour accounted for 19.3% of the variability in behaviour, with intention being the strongest determinant at 44.3% (McEachan, Conner, Taylor and Lawton, 2011:125). The study further shows that the Theory of Planned Behaviour was considerably less predictive of behaviour when studies adopted a longitudinal, rather than a correlational, design, when the studied population was not university students, and when outcome measures were taken objectively rather than as a self-report.

Reasons for cyberethical violations are wide and complex. Social, psychological and knowledge factors have been shown to influence an individual's decision on digital piracy, including unethical use of cybertechnology. Other authors assert that experimental tests of the theory have been rare and those that have been conducted have not supported the theory's assumption (Sniehotta, Pesseau and Araujo-Soares, 2014:2). Similarly, the theory has been criticised for its exclusive focus on rational reasoning, excluding unconscious influences on behaviour (Sheeran, Gollwitzer

and Bargh, 2013:460), and the role of emotions beyond anticipated affective outcomes (Conner, Godin, Sheeran and Germain, 2013). Likewise, the static, explanatory nature of the Theory of Planned Behaviour does not help to understand the evidenced effects of behaviour on cognitions and future behaviour (McEachan et al., 2011; Sutton, 1994:76).

The subjective norm construct was found to be a weak determinant of intention. This was partly attributed to poor measurement and the need for the expansion of the normative component. Accordingly, these components do not explain all the variance in intentions and behaviours. Other components or factors have been proposed. For example, in the domain of honesty, a measure of moral obligations was recommended as another potential determinant of intentions to act duplicitously (Beck and Ajzen, 1991; Conner, Smith and McMillan, 2003).

McEachan et al. (2011) reviewed over 200 studies that used the Theory of Planned Behaviour to prospectively determine health-related behaviours. The review found that intention and perceived behavioural control accounted for 19% of the variance in behaviour and that attitude, subjective norms and perceived behavioural control accounted for 44% of the variance in intention. Other focus of the theory's criticism questioned its limited predictive validity, especially the problem of inclined abstainers, who are individuals who form an intention and subsequently fail to act (Orbell and Sheeran, 1998).

Ajzen (2015:133) reacted to these criticisms by noting that the Theory of Planned Behaviour is not a theory of behaviour change. Rather it is meant to help explain and predict people's intention and behaviour. It has also been argued that the focus of the criticism of the theory is intention. In the Theory of Planned Behaviour, intentions are viewed as behavioural plans that are in conjunction with appropriate opportunities and resources that enable attainment of a behavioural goal (Ajzen, 1996). On the contrary, intentions do not always lead to the successful enactment of behaviour (Conner and Armitage, 1998). The results of meta-analyses of the Theory of Planned Behaviour indicate that intentions and perceived behaviour control (PBC) account for only 49% of behaviour (Knabe, 2012).

2.9 Applications of the Theory of Planned Behaviour in Cyberethical Studies

Applications of the Theory of Planned Behaviour are various and large, as testified by the large number of citations reported in Ajzen (2011:1113). He claims that from 22 citations in 1985, it had grown to a stable total of 4550 by 2010. However, the theory is not only supported by extensive empirical evidence, but also by relevant meta-analyses that synthesise the evidence. In fact, several

meta-analyses and systematic reviews consistently support the utility of the theory across conditions. Thus, empirical evidence from various meta-analyses give credence to the determinants of cyberethics behaviour and, thus, suggest possible ways and means for improving ethical use of cybertechnology in order to prevent unethical cyber behaviour.

Studies over the past two decades have provided important information on the Theory of Planned Behaviour as a framework for explaining and predicting cyberethics behaviour, particularly the determinant factors of human behaviour in cybertechnology. The Theory of Planned Behaviour has often been adopted as a choice in studies of user intentions with respect to technology (Venkatesh et al., 2003) and cyberethical violations by users, especially by undergraduate students in academic environments, particularly the perceived factors that influence unethical usage among undergraduate students. Al-Jabri and Abdul-Gader (1997), Al-Rafee and Cronan (2006) and Goles et al. (2008) applied the Theory of Planned Behaviour as a base theory to explain the behaviour to commit digital piracy.

Kisamore et al. (2010) conducted a study in Oklahoma using the Theory of Planned Behaviour to predict academic misconduct intentions and behaviour. Using technology, they studied the cheating intentions and behaviour of a sample of 241 business undergraduates and discovered that the Theory of Planned Behaviour accounted for 21% of the variance in cheating intentions and 36% of cheating behaviour. The findings of their study show that the Theory of Planned Behaviour model is a valuable tool for determining cheating behaviour and could enhance further research on cybertechnology misconduct.

On the other hand, Martin et al. (2010) conducted a survey on 80 college students, using the Theory of Planned Behaviour to survey the factors that influence online gambling behaviour and frequency. The results of their study supported the efficacy of using this theory to clarify gambling behaviour in the studied population. They found that perceived behavioural control and subjective norms determine past gambling, and that subjective norms, attitudes and perceived behavioural control predicted the frequency of gambling behaviours. Similarly, Baker and White (2010) conducted a study to determine adolescence behaviour in social networking. Questionnaire was administered to 160 students. The study supported the components of the Theory of Planned Behaviour - attitude, perceived behavioural control and group norms - in predicting intentions to use networking sites.

Some researchers have also found that ethical considerations have some effect on a user's intention to share files. For instance, Chiou, Huang and Lee (2005) included ethical decision making within

the constructs of the Theory of Planned Behaviour. Gopal, Bhattacharjee, Agrawal and Wagner (2004) found out that ethical predispositions had a significant relationship with unethical software piracy behaviour in both the USA and India. They concluded in their study that other factors such as deterrence, legal actions and education were not likely effective in reducing music piracy. Cronan and Al Rafee (2008) examined the factors that influence the intention to pirate software and media, using the original constructs in TPB. The study's findings show that past behaviour, moral obligations, attitude, and perceived behavioural control explained 71 per cent of the intention in cyber piracy.

In addition, Chang and Lee (2011) applied the Theory of Planned Behaviour in a study to investigate students' ethical behaviour regarding cybertechnology, with emphasis on their observance of rules pertaining to cyberspace use and ethical attitudes. Likewise, Peace, Galleta and Thong (2003) based their study on Ajzen's (1991) Theory of Planned Behaviour. They examined intention to pirate software and the roles that ethical attitudes of users play in the utilisation of cybertechnology. In another study, Robertson, McNeill, Green and Roberts (2012) used the Theory of Planned Behaviour to examine the relationship between illegal downloads, personal ethical attitudes and other engagements in illegal behaviour. Their study equally sought to identify why existing deterrence methods could not prevent continued unethical cyber attitudes by users.

Lee, Cerreto and Lee (2010) used the theory to study teachers' decisions to create and deliver lessons using computer technology. Moss, O'Connor and White (2010) used it to examine students' intentions to use podcasting as a learning tool in a college course. In the same vein, Alleyne, Soleyn and Harris (2015) used the Theory of Planned Behaviour to investigate accounting students' intentions to engage in software and music piracy. Their findings revealed that attitudes, subjective norms, perceived behavioural control and moral obligation significantly influence intentions to engage in software and music piracy. Equally related to this is the study conducted by Stylianou, Winter, Niu, Giacalone and Campbell (2012). They used the Theory of Planned Behaviour to study intellectual property and unethical cybertechnology practices. Their findings revealed that gender and computer expertise interact with Machiavellianism to influence individual behavioural intention of reporting unethical cybertechnology practice. In another study, Chan and Wong (2015) applied the Theory of Planned Behaviour to understand adolescents' unethical online behaviour, using 757 students in Hong Kong. The study revealed that the Theory of Planned Behaviour accounted for 54.8% and 48.0% of the variances in plagiarism and unethical

cybertechnology use, respectively. The findings of the study also confirmed the utility of the Theory of Planned Behaviour as a valuable model for determining unethical cyberethics behaviour.

These past studies reflect successful applications of the Theory of Planned Behaviour and reinforce its utility for research involving cyberethics behaviour. Furthermore, evidence provided by these reviewed studies, including meta-analytic reviews and other relevant studies, shows that the Theory of Planned Behaviour is an appropriate and reliable theoretical framework (Webb and Sheeran, 2006; Armitage and Conner, 2001). Thus, this review has focused on the Theory of Planned Behaviour because it is shown to be a useful and highly significant cognitive framework that has been used to determine and explain the extent to which undergraduate students' attitudes, subjective norms and perceived behavioural control influence their cyberethics behaviour (Chatterjee, Sarker and Valacich, 2015; Chan, 2015). Therefore, these studies and other similar theoretical frameworks were reviewed to provide insight into, and direction on, the applicability of the Theory of Planned Behaviour to the current investigation.

2.10 Justification for Using the Theory of Planned Behaviour

The Theory of Planned Behaviour was used in this study to determine which of its constructs determine undergraduate students' behavioural attitudes towards cybertechnology. The Theory of Planned Behaviour has been applied to a wide range of behaviours in order to better understand which individuals behave in which way. It has been equally adjudged one of the best-supported socio-psychological theories with respect to predicting human behaviour (Sommer, 2011) and as one of the most influential social behavioural and cognitive decision-making theories.

Several reasons abound as justification for the choice of the Theory of Planned Behaviour for this study. There is a convergence of opinion on the Theory of Planned Behaviour as a useful theory on which to base interventions in cyberethics behaviour. First, the theory postulates clear constructs through which the influence on behaviour can be determined and studied. Second, meta-analytic reviews of correlational studies, using the Theory of Planned Behaviour, have provided empirical support in terms of its capacity to determine and investigate many behaviours (Armitage and Conner, 2001; Conner and Sparks, 2005), including unethical cyber behaviour (Liao, Luo, Gurung and Li, 2009). Third, the Theory of Planned Behaviour is one of the most common social cognition models utilised in information studies research (Godin, Conner and Sheeran, 2005; Johnson, French, Bonetti and Johnson, 2004; Ogden, 2003).

Prior to the emergence of the Theory of Planned Behaviour, researchers have used the theory of

reasoned action as a model to examine users' behaviours. However, the inclusion of the perceived behavioural control construct to the theory of reasoned action led to the robustness of the theory and the postulation of the Theory of Planned Behaviour. The theory is a well-established social psychology theory that has been employed to explain many human behaviour-related phenomena. It stipulates that the psychological process to act or put up some behaviour is stimulated by intention, which in turn is influenced by some underlying beliefs (Ajzen, 1985, 1991; 2005). The determinant factors of intention are the user's attitude towards the behaviour, the subjective norm and the perceived behaviour control. The Theory of Planned Behaviour has been used, and is well-established, in social science, information science and technology, and literature to explain and predict user behavioural intentions (Mykytyn and Harrison, 1993).

The Theory of Planned Behaviour is one of the dominant theories of attitude-behaviour relations (Armitage and Christian, 2004). It can be used to determine undergraduates' cyberethics behavioural beliefs, normative beliefs and perceived control of performing the target behaviour (digital piracy and unethical use). Specifically, if a student holds a positive attitude towards the violation of ethical use of cybertechnology, if there are positive expectations from important referents that he or she should comply, and if the individual perceives having full control of performing the intended behaviour, then it is very likely that he or she will perform digital piracy and unethical use of cybertechnology. Conversely, if the outcome of the performance of this target behaviour is viewed unfavourably or negatively, and if the student believes that the social pressures from important others is for him or her to not comply, and if there are no perceived barriers to non-compliance, then non-compliance behaviour is very likely to occur.

2.11 Implication

The reviewed literature on the Theory of Planned Behaviour as adopted in this study shows that, globally, ethical behaviour continues to be a very important theme among various disciplines. Unethical use of cybertechnology among undergraduate students is prevalent, and from literature, seems to be on the rise. To investigate this phenomenon, the study adopted a theory- based framework to gain insights into young adults' ethical reasoning and actual ethical behaviour in the use of technology and to equally come up with an intervention to stem the tide of unethical behaviour. Research has indicated that unethical behaviour in schools is related to unethical cyberethical attitude at work (Molnar, Kletke and Chongwatpol, 2008). A better understanding of the factors that influence ethical or unethical behaviours may be an approach to positively influencing ethical behaviour. Arising from various studies cited in the foregoing, knowing what influences individuals to act unethically would be a more advantageous perspective. This is especially important because studies have suggested that individuals do not perceive digital piracy and other cyberethics behaviour as a crime or as inappropriate behaviour (Yoon, 2010; Chang, 1998).

This review has added to the cyberethics behaviour literature through the development of a behavioural process model and determining the suitability of its application in developing countries where unethical cyber behaviour is noticeable. Empirical data presented in this study corroborate the findings of Ajzen's (1985, 1991) Theory of Planned Behaviour for the prediction of cyber behaviour and could also suggest possible ethical usage of cybertechnology within the academic environment. With the goal of curbing unethical cyber behaviour, the implication of the study for institutions is apparent. It is important as a guide on the formulation of curriculum interventions and policies. These will address and focus resources and energy on improving students' knowledge of ethical decision-making and behaviour in the cyberspace. Specifically, it is important to include the critical knowledge of information ethics in the teaching curriculum of students, considering that institutions' function regarding cybertechnology ethics education is more important than another organisation's function. Some studies have noted the limited effects of law and the protection policy of institutions, as they hardly provide ethical attitudes and a sense of responsibility to their cybertechnology users (Stylianou, Winter, Niu, Giacalone and Campbell, 2012).

Given the rapidly changing nature and complexity of cybertechnology, which the universities depend on for knowledge acquisition and sharing, it is imperative for university managements to review their policies on the use of internet resources on a regular basis to ensure that those policies are not outdated. It is perhaps more important to explore whether these policies set the right tone for their institutions' culture and whether they adequately deal with how individuals within the community engage in cybertechnology ethical issues when they arise. The knowledge of related risks and ethical issues through cybertechnology ethics will help students to understand different points of view and allow them to make better and knowledgeable decisions regarding information technology usage (Acilar and Aydemir, 2010). This ethical usage knowledge may help students to consider their options in a safe environment and open their minds to different possibilities and choices (Thomas and Ahyick, 2010).

The principal theoretical implication of this study is that, while it is not enough to declare that unethical cyber behaviour is against the institution's code of conduct and acceptable use, undergraduate students, as individuals, need to contend with what ethical and acceptable behaviour actually means in today's digital world. University managements need to initiate more forums where nuances of opinions can be shared among stakeholders on what constitutes cyberethics behaviour, how to behave in the cyberspace, why intellectual property rights are important, how archaic laws might be changed for more robust and useful ones, and how creativity can be encouraged and blended with property rights, without legal and ethical infringements.

2.12 Summary

The chapter discussed concepts of theoretical framework, theory and models, and showed how they collectively fall within the context of cyberethics. Different theories and models were highlighted to demonstrate the pattern of their link to cyberethical behaviour, with the Theory of Planned Behaviour being the favoured and therefore adopted for this study. The relationship between the Theory of Planned Behaviour and cyberethics through various forms of their application in several studies has been shown, specifically how the constructs within the theory could determine the cyberethical behaviour of cybertechnology users and other contextual factors.

The next chapter presents a literature review of the study.

CHAPTER THREE

LITERATURE REVIEW

3.1 Introduction

Literature review in thesis and research studies involves the selection and use of published and unpublished documents containing information, ideas, data and evidence written from different viewpoints. The essence is to fulfil the aims expressed by the researcher on the nature of the topic being investigated (Hart, 2018; Ridley, 2008). Fink (2010:3) established that literature review is a systematic and explicit method for identifying and evaluating existing gaps in a body of knowledge. In other words, it determines the current state of a research problem and the scientific discussions regarding that field of knowledge. Literature review provides insights into previous works conducted through the methodological, analytical and synthesised quality of literature sourced. It also gives a picture of the state of knowledge and other questions that could be asked in the topic area, by allowing a firm foundation to the research topic and choice of research methodology applied (Levy and Ellis, 2006; Chiasson, Germonprez and Mathiassen, 2009).

Similarly, Okoli and Schabram, (2010:2) note that reviewing existing documents is another evidence in relation to the topic under investigation. All these serve as vital steps towards the accomplishment of research. There are numerous sources that assist in this process, such as official statistics, survey data, self-report studies and other secondary sources used by researchers. However, the task of a novice researcher is made difficult due to limitations of the aforementioned sources, as well as the lack of an existing operational definition of cyberethics behaviour or cyberethics itself. Cyber ethicists also face the momentous task of determining the level of ethical violations in the cyber domain when data from differing sources show contradicting trends and patterns. A good number of factors have been attributed to cyberethical intentions and cyber behaviour of adolescents and young adults in cyberspace. Recently, there has been a wide interest in determining some of the factors influencing cyber behaviour. In this section, focus is on some of the antecedents of cyber behaviour of undergraduate students and issues related to the ethical and responsible use of cyber technology in the educational environment.

The two prominent theories of ethics that inform ethical decision making, and which have received cyber ethicists' attention in literature, are deontology and teleology (Basse, 2012). Deontological

theory of ethics is an approach to ethical decision making that takes pleasure in rich historic traditions, going back to theorists such as Socrates and, more recently, to the work of Kant. Deontology is about the concept of universal truths and principles which need to be adhered to regardless of any situation (MacKinnon and Fiala, 2014). Categorical imperative by Kant states that an individual confronted with an issue ought to have the ability to react consistently and in conformity with their ethical principles as well as feel comfortable with the choice being made (Plaisance, 2007). According to Wood (2007), following from the philosophical tradition of Jeremy Bentham and John Stuart Mill on utilitarianism, ethical decisions are made in view of anticipated results, which remove the universality of choices. Therefore, deontology views the means as more important than the end, whilst for teleology it is the end that justifies the means.

Societal perspective of these theories helps in the formulation and employment of various tools that could be used to control cyberethics behaviour. From the legal angle, command and control instruments like laws, code of conduct and acceptable policy play key roles. Breaking the law, from the view of deontologists, will contravene their view of ethics, and as such, they abide and comply with legislation regardless of its value (Spangenberg, 2016:34). Yet, consequences of the violations of the law or regulations are what a teleologist weighs against the benefits of breaking the law. If a student seems to apply a teleological view to an ethical dilemma, it follows that legislation can only expect to be efficient if stringent consequences or penalties that make the outlawed behaviour not worthwhile are applied; hence the need to study how ethical behaviour and decisions are made within the realm of cybertechnology use. Generally, the boundaries of tolerable and deplorable cyber behaviour are defined by government establishments, who develop regulations around specific unlawful cyberspace behaviours, and businesses which detail inappropriate actions in their terms of service agreements (Oakley and Salam, 2012:1). Past research has shown that even with detailed guidelines, users within the institution continue to cause breaches in security (Harris, 2012) and these actions are greatly influenced by the behaviours of their students and staff (Gallivan, Spitler and Koufaris, 2005). There are several views on the legal, moral and technological strategies used by institutions to reduce unethical cyber behaviour. Surveillance systems and continuous monitoring are being adopted by institutions around the globe to monitor cyber footprint of cybertechnology use (Zetter, 2007; Schulman, 2001). Adoption of policies is another method used by institutions to deter misuse (Young, and Case 2004).

To deter students from unethical use of cybertechnology, it is necessary to identify the factors influencing such activities. Further, the role played by policies and other policing factors in deterring misuse and their effectiveness should be explored to formulate strategies to be recommended to the management of institutions. Studies have shown that people choose to trade some aspects of personal freedom for social order (Staub, 2013; Andrews and Withey, 2012). This view was also shared by Jean Jacques Rousseau, who explained the social contract, or principles of political right. The rules members of a society make to balance their individual rights to freedom against the needs of the society are called laws. Laws are rulings that command or forbid certain behaviours. They are drawn from ethics, which have to do with socially acceptable behaviours. The significant difference between laws and ethics is that laws carry the authority of a governing body, while ethics do not. Ethics, in turn, are based on cultural mores: the fixed moral attitudes or customs of a group. Some ethical standards are universal. For example, murder, theft, assault and arson are actions that deviate from ethical and legal codes throughout the world (Sumner, 2013; Singer, 2011). Some research projects that focus on the phenomenon of cyberethics have included the exploration of the emerging practices in cyber law, dealing with intellectual property rights in cyberspace (Shinde, 2013; Moorthy and Ramaiah, 2014). While ethics should not be confused with law, the issue involving the regulation of social responsibility demands a discussion of law. Hence, cyberethics could also include the right of the users of cybertechnology to engage in free and unrestricted access and use of cybertechnology as long as their use is not harmful to themselves and others.

3.2 History of the Internet

In its current form, the Internet is primarily a source of communication, information and entertainment, but increasingly, also, a vehicle for unethical behaviour (Tavani, 2013:7). An understanding of the factors responsible for unethical behaviour on the World Wide Web is particularly relevant in the context of predictions made regarding the educational environment in users' quest to meet their information needs, education, entertainment and other sundry social inclusion.

3.3 The Emergence and Concept of Cyberethics

Norbert Wiener, a college philosopher and scientist who taught mathematics and engineering, created a new course of ethics using new evolutions in science and philosophy, which would later

be called cybertechnology ethics or information ethics (Bynum, 2011:24). Wiener's interests in the potential influence of cybertechnology in World War II enabled him to establish applied science which he named cybernetics. Bynum (2011) believed Wiener had the opportunity to propose social and ethical behaviour of cybernetics integrated with electronic cybertechnology. He believed that in the coming years, the world would undergo a second industrial revolution - an automatic age with "enormous potential for good and for evil promoting new ethical challenges and opportunities".

Wiener wrote the two books that would lay the foundation for cybertechnology and information ethics in 1950 titled *The Human Use of Human Beings*. This established him as the founder of cybertechnology ethics and provided a detailed cybertechnology ethics foundation which continues till date (Bynum, 2011:20). The book defined the incorporation of cybertechnology into society that will usher in the rebuilding of society. Specifically, he describes three major ethical principles by which people should live: equality, freedom and benevolence. He regarded this as the "second industrial revolution" which would potentially change every significant aspect of life (Bynum, 2011). Apparently, the cybertechnology revolution will involve a variety of roles and responsibilities. According to Bynum (2011), employees are going to be forced to adapt to changes in the workplace. Unique laws and guidelines will be formed by government, while the private sector will establish new policies and practices. Professional organisations will develop different rules of conduct for their associates. Sociologists and psychologists will examine and apply new social and psychological trends, and philosophers may reconsider old social and ethical concepts. Bynum (2011:13) indicated that in the 1960s, significant social and moral implications of cybertechnology had already emerged as a major problem, and cybertechnology-associated ethical challenges had begun to develop. In the early 1990s, a different emphasis within cybertechnology ethics was advanced by Donald Gotterbarn, who believed that cybertechnology ethics is recommended as professional ethics dedicated to the advancement and achievement of standards of good practice and codes of conduct for computing professionals. Gotterbarn (1991) stated:

There is little attention paid to the domain of undergraduate ethics and the values that guide the day-to-day activities of computing experience in their role as future professional. By future professional I mean

anyone involved in the design and development of computer artefacts. ... The ethical decisions made during the development of these artefacts have a direct relationship to many the issues discussed under the broader concept of computer ethics.

Cyberethics a particular kind of technological applied ethics has emerged as an area of ethical concern. Froehlich (2005) described cyberethics as ethical issues related to the cyberspace or internet. Expert systems, synthetic intelligence and the ability of robots to reason are all topics inside the discipline of cyberethics. Froehlich (2005) identified numerous vital works associated with these particular fields: James Boyle's *Shamans, Software and Spleens: Law and the Construction of the Information Society*; Lawrence Lessig's *Code and Other Laws of Cyberspace*; and Richard A. Spinello's *Cyber Ethics: Morality and Law in Cyberspace*. Thomas, Singh and Gafar (2011) argue that the rapid uptake of cybertechnology around the world is astounding, especially with the number of new users increasing daily. The situation, others claim, is due to the increase in affordable handsets and broadband connectivity which is driving the fast penetration of the technologies (Mutula, 2013:45). Not surprising, scholars contend that cyber technologies are used by individuals, organisations, institutions and governments as a means of socialisation, collaboration, communication and dissemination of information across the world (Lee and McLoughin, 2010). Similarly, others argue that cybertechnology is increasingly becoming central to the learning environment by enhancing communication and collaboration among academics and their peers (Narayan and Baglow, 2010).

There is a lot of focus on the benefits of cybertechnology and the uniqueness of the Internet in terms of its ability to connect members of the academic community to the outside world. Much of the concern about the use of cybertechnology in its early days was related to apprehension about the storage and exchange of information in large databases in both private and public domains (Tavani, 2001). In developed countries, increase in the value of information and easier accessibility of cybertechnology have raised concerns about personal privacy. This has received significant attention from philosophers, anthropologists, sociologists, educationists and academics in law and communication studies (Mason, 1986; Heersmink, van den Hoven, van Eck and van den Berg, 2011). Consequently, developed and developing countries of the world with high cybertechnology

usage have made laws or are in the process of amending regulations with respect to privacy in order to decrease these fears and concerns. Ackerman and Britz (2006) explain that the challenge of the current information era is the threat that cybertechnology poses to an individual's right to privacy.

The definitions of cyberethics, cybertechnology ethics, internet ethics, as well as other related terms vary in the literature. This terminological confusion was underscored by Onyancha (2015) in his study to identify the similarities and differences that exist among the three stated concepts. He affirms that the concepts pose a challenge for educators and indexers of published literature and educators who work in the field. For Moor (1995:266), cybertechnology ethics refers to the examination of the nature and societal effects of cybertechnology, technologic information and the corresponding system and application of policies for the ethical use of such technology. Moor anchored his definition on the perception of the situations where cybertechnology is essentially involved, thus creating a situation of overlap in the field and unethical use of technology.

A further definition is given by Froehlick (2005) who describes cyberethics as a branch of cybertechnology ethics that is concerned with ethical issues related to the Internet or cyberspace. He adds that the issues discussed in the field include artificial intelligence, expert systems and the ability of robots to reason. Yamano (2006:2) uses the term cyberethics as an ethical guidance upon which individuals rely. In other words, she defined it as the guidelines or framework upon which students will base their ethical and moral decision-making. The definition by Tavani (2013) is the most precise operational perception of the term cyberethics. He viewed it as the field of applied ethics that examines moral, legal and social issues involving cybertechnology.

Cyberethics examines the influence of cybertechnology on our social, legal and ethical systems, and it evaluates the social policies and legal guidelines that have been framed in response to issues generated by way of its development and use. Consecutively, cybertechnology refers to a wide range of computing and communication devices, from stand-alone cybertechnology systems to connected or networked computing and communication technologies. These clustered or networked technologies, however, need not be confined to devices such as smartphones, iPods, tablets, personal cybertechnology systems (desktops and laptops) and large mainframe cyber technologies (Tavani, 2013).

With the arrival of the Web, disputes over personal privacy, property, security, accuracy, ease of

access, censorship, filtering and others have occurred and have been widely studied by researchers in the field of cyberethics. Scholarly literature in the field of applied ethics has witnessed various researchers placing their studies under various titles: cybertechnology ethics, internet ethics, information ethics, and so on (Sharma, Mittal and Verma, 2015:141). Each of these applied ethics shares roots and relationship with the others, and with an extensive variety of fields such as engineering ethics and business ethics.

3.4 Cybertechnology and Human Behaviour

Human behaviour is classified into two worlds that exist separately, but which are interrelated: real-world behaviour and cyber behaviour. While the real world is a phenomenon that has existed with humans from the first day of human history, cyberspace came about only a few decades ago after the Internet was invented. According to Yan (2012), cyber behaviour is simply a hybrid of two words and entities - cyberspace and human behaviour - referred to as human behaviour in cyberspace. Similarly, Goritz, Singh and Voggeser (2012) describe cyber behaviour as any physical, social or mental activity that human beings engage in while interacting with the Internet within cyberspace. The term cyber behaviour refers to the pattern of behaviour that users display when employing different cyber technologies for various purposes. Hence, it is understood as the pattern of use of new media technologies, focusing in cyberspace. It includes the study of what people use the Internet for, how they use it, how often they use it and its various applications (Brandtzæg, 2010). Based on the foregoing, human activities that involve physical, social or mental engagement in connecting to and interacting in cyberspace could broadly be referred to as cyber behaviour.

Although it has been studied for over 20 years by a variety of researchers in multiple disciplines, there is still considerable debate over the impact of cyberspace and cybertechnology on human behaviour. The debate may partially be attributed to the constantly-evolving nature of cyber technologies and their use in the performance of everyday professional, academic and personal activities by members of the academic community. Accordingly, cyberethical standard is still evolving for cybertechnology due to the ease of access to copyright software, music and other digital materials. In recent years, some authors have stated that ethical or unethical behaviour takes place as a result of ethical dilemma (Mihelic, Lipicnik and Tekavci, 2010; Monahan, 2012; Disoloane, 2012).

Some factors are theorised as influencing behaviour directly, while other factors influence through mediating variables. Venkatesh et al. (2003) sum up the conceptual framework of intention-based models as follows: intention to use and actual usage are impacted by people's reaction to using cybertechnology; intention to use influences behaviour. However, actual usage, in turn, influences how people will react to cybertechnology in the future. Researchers such as Riemenschneider, Harrison and Mykytyn (2003) have pointed out that the TAM, TRA and TPB, which preceded the TRA, are well established intention models grounded in a large body of research.

It must be noted that understanding students' cyber behaviour is critical to understanding and analysing the factors that influence their cyberethics behaviour and the eventual analysis of the phenomenon of cyberethics within the academic environment. Gotterbarn had first argued for reasons why the field of cyberethics should be a primary concern of computer professionals. He observed that most ethical issues involving computers directly affect the computing profession. However, events in the last decade have shown two major factors that have shifted opinion from this direction. First is the emergence of the Internet and its accessibility by ordinary people. This has led to the emergence of more complex, broader cyberethical issues and behaviour. Secondly, most users of cybertechnology currently use it either for work, entertainment, recreation, education or other sundry purposes, and they are not professionals. Therefore, the conception of the field of cyberethics at present is broader than that proposed by Gotterbarn.

Many studies have been undertaken, which draw on moral theoretical concepts on the behaviour of cybertechnology among young adults within the university environment. Some authors (Vallor, 2010; Calvani, Fini, Ranieri & Picci, 2012; Plaisance, 2013) have called for a consideration of the moral dimensions of cybertechnology; yet others (Capurro, 2008) have sought to advance some universal ethical principles for the use of cybertechnology. Just like other technological inventions and innovations throughout human history, some of the literature consider that cybertechnology tends to have both positive and negative impacts on society, and equally tends to raise moral and ethical questions (Stahl, Eden & Jirotko, 2013; Von Schomberg, 2012).

3.5 The Influence of Demographic Characteristics on Cyberethics Behaviour among Students

Demographic factors are sometimes adopted as units of measurement to examine the level of their various influences on a phenomenon of study. It is common practice among behavioural scientists

to refer to them as personal characteristics (Tella and Mutula, 2008). Studies have listed some forms of demographic variables to include, but not limited to, age, gender and religion (Lau, Yuen and Park, 2013). Studies of ethical decision-making in the realm of cyberspace are generally determined and searched for from two directions: either examining demographic and personality styles of cybertechnology users who judge a particular behaviour as unethical or examining the process of ethical decision-making to identify beliefs and attitudes which lead to cybertechnology misuse behaviour (Haines and Leonard, 2007). Others have observed that research on demographic variables as the determinants of cybertechnology ethics of undergraduate students may enrich the body of knowledge concerning the teaching and learning of moral and ethical education (Lau and Yuen, 2014). Despite the observed importance, previous studies have failed to consider or have given less attention to this phenomenon in the context of cyberethics education and eventual behaviour of undergraduate students in institutions in developing economies.

To determine the influence of demographic characteristics on internet ethics of their respondents, Williamson et al (2010) examined age, gender, college major, number of hours per weekend and self-rating of their respondents' expertise on cybertechnology to determine their ethical or unethical use of devices on the university cyberspace. In a related study, Shemroske (2011) identified the various demographic variables that may influence the ethical use of cybertechnology. These include age, gender, experience with computer, experience with sharing of software and work experience. In addition, it is understood in current literature that there is some consensus on the attitudinal description of undergraduate students as having the demographic tendencies and attitudinal factors for cyberethics behaviour (Upshaw and Babin, 2010; Chiang and Lee, 2011). For instance, demographic norm depicts how males, younger adults and students with faster internet connection are more likely to engage in cyberethics behaviour (Goel, Kaur and Vaidya, 2012). Kini, Rominger and Viayaraman (2000:70) note that unethical behaviours in the use of the computer are not affected by students' experiences with computers but greatly affected by social demographic variables such as age. Similarly, studies have equally established that female students are more aware of various unethical behaviours in the use of cybertechnology than their male counterparts (Domeova and Jindrova, 2013; Hu and Lei, 2015).

In an earlier research, Hayes and Introna (2005:229) noted that many university students attribute unethical cybertechnology behaviour to diverse complex and cultural backgrounds. Thus,

decision-making by undergraduates and young adults in cyberspace within the university environment may be determined by age, gender and other demographic variables. Similarly, in another study conducted in Thailand, it was shown that undergraduate demographic variables, such as age, gender, experience and skills in the use of cybertechnology, correlate significantly with cyberethics behaviour (Kini et al, 2000).

Sargolzaei and Nikbakht (2017) reported that in some cases, gender has a significant impact on the ethics of information technology, which can be due to local traditions, beliefs and cultural factors in specifically Islamic countries. From a traditional and cultural point of view, women are expected to have different values than men; therefore, they have different moral behaviour, in different conditions, compared to men. As reported by Sidani (2005) and Sidani, Zbib, Rawwas and Moussawer (2009), women are expected to follow cultural and family values and obey tough constraints.

Odo and Odo (2015) in their study reported that gender, age and institution type have significant influences on the level at which students will get involved in cyberethics behaviour. They also found that female students are less prone to involvement in cybercrime compared to their male counterparts. Also, the age of the students and level of study, to an extent, will influence the willingness and propensity to involve in cybercrime. They recommended that youths are the leaders of tomorrow and should be given proper education to be able to channel their energies towards more profitable ventures, and that as a matter of urgency, government and other related stakeholders and key players in the Nigerian economy should try and create more job opportunities for young graduates in order to alleviate their involvement in negative societal behaviour.

Consequently, to add richness to the current understanding of literature in the context of this study, this study also examines the influence and interplay of some demographic variables and cyberethics.

3.6 Awareness of Cyberethics Behaviour among Undergraduate Students

Studies have shown that 50 to 70% of the overall unethical use of cybertechnology in institutions results either directly or indirectly from misuse, and ranges from naivety to intentional ethical violations (Ernst and Young, 2004; Siponen and Vance, 2010). Therefore, improving cyberethical awareness is a necessity for improved ethical conduct in the use of cybertechnology within

academic institutions.

It is necessary here to clarify exactly what is meant by awareness in the context of cyberethics behaviour. For Dinev and Hu (2007), awareness means the extent to which a target population is conscious of an innovation and formulates a general perception of what it entails. Awareness is an antecedent for the attitude formation stage of cyberethical intention and behaviour. In the framework and context of this study, this would mean that awareness is an antecedent of attitudes and behavioural intentions. Clearly, based on the classification of cyber technologies, awareness in cyberethics behaviour is developed from the perspective of Butterfield, Trevino and Weaver (2000: 982) who view it as an individual's recognition that his/her potential decision or action could affect the interest, welfare or expectations of self or others in a fashion that may conflict with one or more ethical standards. Here, awareness is seen as the ability to be alert to scenarios that pose a potential ethical dilemma in cyberspace and cybertechnology use. Similarly, awareness as a concept is seen as a main driver of behaviour in students' cyberethical intentions (Dwivedi, 2009).

Diverse studies have shown awareness to be an important direct and indirect determinant of cyberethics behaviour. For example, Galvez and Guzman (2009) identified awareness as one of the shaping factors of behaviour and conclude that the higher the cyberethics awareness, the higher the cyberethics behaviour practice. Dinev and Hu (2007) found that individuals' awareness about potential consequences and negative implications of cyber technologies is a determining factor in the intention to make use of protective information technologies. Relating to the general deterrence theory, D'Arcy, Hovav and Galletta (2009) showed that a high level of users' awareness of institutions' countermeasures, such as security education training awareness (SETA) programmes, computer surveillance and cyberethics policies reduce unethical cybertechnology intention. North, George and North (2007) used 465 volunteers in their study to investigate cybertechnology security and awareness at black colleges and universities. The study reports a lack of awareness of cybertechnology security and violations of code of ethics. The study further suggests a need for cyberethics education and awareness training for cybertechnology users.

The steady growth and reliance on cybertechnology and innovations within academic institutions make the oversight of technology far more complex, political and disruptive than in the past (Falconi, 2014). In view of the accompanying behaviour in cyberspace, due to growing increase

and reliance on cybertechnology innovations and the Internet, certain measures have been adopted by many developing nations. One of these measures is the awareness and education initiatives. This was informed by the fact that lack of knowledge is perceived as a factor that facilitates unethical cyber behaviour (Thomson, von Solms and Louw, 2006). Kortjan and von Solms (2012) note that cyberethics awareness and education is a prerequisite for ethical implementation in cyberspace. They, however, observe that the initiative for ethical cyber behaviour through education and awareness is offered by academic institutions in South Africa. Igwe and Ibegwam (2014) note that many students in Nigerian universities are aware of various cyberethical violations like plagiarism, copyright violations, computer hacking, misinformation, online gambling and various internet addictions.

Ngoqo and Flowerday (2014) consider awareness and knowledge as two important factors of cybertechnology behaviour intentions of students in higher institutions in South Africa. Their result shows a moderate positive correlation between the level of awareness and behavioural intent. This implies that there is a need for every student in an academic environment to be aware of cyberethics behaviour as a guide to ethical cybertechnology use. It can also be said that there is need for ethical use of information technology in order to prevent violation of use. It is only when they are aware of the negative cyberethics behaviours that students will be able to use the resources legally. Lysonski and Durvasula (2008) have also noted that lack of awareness of the social costs of downloading information and its consequences in terms of the impact on copyright ownership may increase users' inclination to participate in unethical cyber behaviour. In addition, Tadele (2013) also affirms this position in his study that students do not believe that cyberethics behaviour could result in monetary loss to some people. The University of North Carolina (2014) reported that many students in the university face various ethical problems, including plagiarism and software piracy.

Adetimirin (2017) conducted a study in two public universities in Nigeria on the level of awareness of cyberethics. The findings revealed that the level of awareness of cyberethics in Nigerian universities varied. In one university, the level of awareness was higher than the other. Other researchers have found a strong correlation between unethical cyber behaviour of students while in the academic environment and later in their future professional lives (Anitsal, Anitsal and Elmore, 2009; Martin, Rao and Sloan, 2009). Summing up this assertion, Kidwell and Kent (2008)

observe that what is learnt by students as ethical behaviour in cyberspace during their academic pursuit may well inform their professional expectations of acceptable digital behaviour in their professional lives; hence it could be said that if there is unethical perception and behaviour towards cybertechnology in the academic environment, when a student begins a professional life, it will probably be difficult for them to form an ethical attitude towards the use of cybertechnology.

Dadzie (2011) argues that the level of education of students is a major factor that determines their level of awareness of various cyberethics behaviour when using the computer. This implies that university students that are in their first year may not know the negative implications of what they are doing, particularly as it relates to issues of plagiarism, computer crime and abuse of social networks, compared to those in the final stage of their studies.

Poor awareness of unethical behaviours in the use of cybertechnology in academic institutions is considered a serious issue that may be counterproductive to educational development (Szabo and Underwood, 2004). Gan and Koh (2006) conducted an academic survey in Singapore, where many students admitted that they were not aware that software piracy is a crime. Likewise, Akbulut et al (2008) conducted a study in Turkey, where the university students admitted that they were not aware of unethical computer behaviour, although many of them used the Internet to engage in various unethical behaviours such as fraud, plagiarism and falsification. Ni, Yan, Chen and Liu (2009) observed that undergraduate students who took courses in information ethics developed better skills about computer usage, which permitted them to know the dos and don'ts of computer usage. Similarly, some organisations have adopted policies and trainings to create awareness on ethical use of cybertechnology. Human resource policies and trainings are developed to create awareness on ethical and proper use of cybertechnology (Mohamed, Shahriza, Abdul Karim and Hussein, 2012). Furthermore, authors observed a negative correlation (correlational coefficient – 0.611) between the level of awareness of acceptable use policy and the level of misuse, suggesting that awareness reduces misuse (Liyanagunawardena and Samarasinghe, 2008). This indicates that students offering five- or six-year courses may be more aware of cyberethics issues than students in the lower academic cadres. Woodward, Martin and Imboden (2011) expand and validate Mason (1986) PAPA framework to explore and determine its continued influence on the study of ethical issues involving cybertechnology among professionals and students. Their study revealed a valid refinement of the issue of cybertechnology misuse, thereby informing those studying cyberethics

to examine the influence of the framework in refinement and expand cyberethics- related pedagogies. Tahat, Eliaa, Sawalha and Al-Shaikh (2014) observed in their comparative study of ethical orientation among university students in the Middle East and the US that there is no significant difference between the two samples. The findings revealed a general awareness of ethical issues and the dangers associated with cybertechnology by many students in the two countries.

The inclusion of orientation as a determinant of cyberethical awareness has also been suggested by some authors. For instance, Bairaktarova and Woodcock (2017) affirm the influence of orientation on engineering students' ethical awareness and behaviour. It was reported in their studies that one of the motivational variables that help in the formation of students' ethical decisions is in their institutions' instructions that help students to interpret interpersonal cues to detect ethical dilemmas, with a core focus on the values of achieving professional ethics and responsibilities.

All the foregoing discussions indicate a general theme of ethical awareness in some cases, and its lack thereof in other cases, within academic institutions. Given the importance of ethics in the use of cybertechnology, educational institutions have introduced ethics into many courses at both undergraduate and postgraduate levels. A typical management information systems (MIS) course often contains a module on cybertechnology ethics. Nevertheless, universities are commonly affected by incidents of cyberethical violations such as inappropriate access, copyright infringement and illegal downloads. Despite the volumes of studies on this phenomenon, there are very few publications on the topic in Africa. Therefore, evidence on this phenomenon in the context of Africa, which the findings from this study will divulge, will be valuable.

3.7 Types of Cyberethics Behaviour among Undergraduate Students

The extensive and rapid advancement in the application and use of cybertechnology around the world has also prompted opportunities for abuse and discussions in the field of IS on the growing grey areas about ethical and unethical uses of cybertechnology. An alarming statistics in a study revealed an estimated 2.5 million incidents of cybercrime, including hacking and spreading of viruses (Office for National Statistics, 2018). Meanwhile, a national study reported in Times Live (2017) claimed that cybertechnology users in South Africa are at particular risk of being hacked due to poor digital literacy. Cybercrime is on a high increase, not only in the developing world but

also the developed world (Hamsi et al, 2015). Obar et al (2012) attribute this to the fact that many students and young people use social media to communicate with one another every day. In a related study, the Digital Civility Index report on 23 countries conducted by Microsoft in 2017 to examine the extent of unethical behaviour in cyberspace indicated that South Africa ranked 22nd and 8% (47%) above the global average of 39% (African Technology and Media Holdings, 2018).

A considerable amount of literature has been published on cyberethics in North America and Europe, and these studies have identified a variety of unethical or questionable cyber practices, some of which will be highlighted in this section of the study. For instance, the use of pirated software and intellectual and copyright property violations are common phenomena in universities (Peslak, 2008). Researchers like Siponen and Vartiainen (2007) and Cilliers (2017) have found that young adults viewed making copies of protected items on the Internet as socially and morally acceptable.

Folorunso, Vincent, Adekoyo and Ogunde (2010) conducted a study at the University of Agriculture, Abeokuta, Ogun State, Nigeria, on the diffusion of innovation in social networking sites among university students. One of the major findings of the study shows that the respondents had attempted to try social networking sites before adopting their use. Thus, the users of the sites often examine them, and probably know the gratifications they could derive from the media, before accepting to use any of them.

Criminal activities within cyberspace are now on a global scale. Halder, Jaishankar, Periyar, and Sivakumar (2011) view cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as the Internet (chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

According to Pahuja (2011), cybercrimes means a lot of things. It could be hackers vandalising a site, viewing confidential information, stealing trade secrets or intellectual property with the use of Internet. It can also include denial of services and virus attacks, preventing regular traffic from reaching the site. According to Pahuja, crimes, such as frauds and forgery, are traditional and handled by statutes such as the Indian Penal Code or State Level Legislatures (SLL). However, the abuse of the computer and related electronic media has given birth to a set of new crimes with

some peculiar features. A simple definition of these crimes would be *“unlawful acts wherein the equipment transforming the information, be it a computer or a mobile, is either a tool or a target or both* (Rathinasabapathy and Rajendran, 2007) .

All over the world today, so many people have embraced cybercrime as a means of livelihood at the expense of the physical and mental wellbeing of others. Tade and Aliyu (2011) affirmed that many have become rich through cybercrimes while some others have been caught by the law. Cybercrimes are not limited to the few types that are known to users of the Internet, but they are ever-evolving with new strategies, thus throwing up new challenges to crack them down. Below is a compiled list, updated from various studies (Aggarwal, 2015; Pahuja, 2011).

- Cyber piracy (software piracy: music and film downloading);
- Cybersex (online porn) or pornography;
- Privacy violation;
- Disseminating fake news;
- Cybercrime.

Harm that could be inflicted on individuals in cyberspace include harassment via emails, stalking, bullying, dissemination of obscene materials, defamation, hacking, cracking, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, forgery and phishing. Similarly, there are cybercrimes and cyber misconducts done to harm the property of an individual or organisation. They include intellectual property crimes, cybersquatting, cyber vandalism, computer hacking, computer forgery, transmitting of viruses and malicious software, cyber trespass, Internet time theft, theft of funds via online transactions, amongst others.

Cybercrimes against government include cyber warfare, cyber terrorism, cyber espionage and distribution of pirated software. Cybercrimes that are highly threatening issues at societal level include child pornography, cyber trafficking, online gambling and financial crimes. According to Livingstone and Haddon (2008), adolescents are exposed to the following four categories of negative online behaviour:

- i. **Content risks:** This involves being confronted with sensual/violent/racist/hate material, pornography and challenging content (e.g. suicide, anorexia, drugs, etc.). Many teenagers pointed out that they search for inappropriate contents, talk about sensitive topics, read about

and see Internet postings on these issues (Livingstone and Haddon, 2008). Also Mathieu et al (2012) observed that the Internet might affect young users when they search for harmful contents, as they will be exposed to violent images and contents, and there is a danger that they will act on what they have seen. Internet addiction increases the risk of self-harm, depression and suicide. The harm extends to the use of drugs too, and researchers have found that young people use instant messaging to discuss drug issues. Wolak, Mitchell and Finkelhor (2007) revealed that risky Internet behaviour could expose users to pornography, without seeking or expecting such pictures when they are searching online, opening websites or pop-up links. Miller and Record (2013) also reiterated that access to the Internet exposes youths to uncensored pornography. Some teenagers can become involved in online harassment by sending unethical photos of people to others without their knowledge.

- ii. **Contact risks:** This involves contact with foreigners, cyber-bullying, online harassment, etc. Mitchell, Finkelhor and Wolak (2007) observed that the Internet provides teenagers with much information, but it can also expose them to greater risks and dangers. They can face dangerous people online, a variety of sensitive material, and they could become victims of harassment and bullying. Online harassment is attacking or offensive online contents that are inflicted on teenagers and seen by others. In their study, Dowell, Burgess and Cavanaugh (2009) reported that nearly a third (29.5%) of the boys and 27.8% of the girls who were their population sample reported that they had posted rude comments online.

Dowell et al. (2009) showed that other types of harassment carried out by teenagers include embarrassing others by making jokes, and harassing foreigners. Online harassment (playing jokes, making rude comments, intentionally embarrassing someone online, or bullying) is a type of risky activities conducted by teenage students.

Morrow and Downey (2013) defined cyber-bullying as intentional aggression used via the Internet or any electronic device to inflict psychological harm on others. Cyber bullying is carried out by young adults to cause them to feel powerful by exacting their own social position and minimising that of their victim in their discussion group (Festl and Quandt, 2013). Involvement in cyber-bullying via the Internet can be accomplished anonymously by young adults and can take many forms, including flaming, harassment, cyber stalking, denigration, imitation, exclusion and trickery (Moross, 2017). Male students are more likely to bully others online than female students,

and many teenagers said that they felt angry, unhappy and depressed after being bullied online (Mishna et al., 2010).

- i. **Commercial risks:** This involves advertising/commercial misuse, illegal downloading, gambling, etc. Transferring music from the Internet into users' computers is unauthorised for copyright reasons and researchers consider online illegal music download to be theft (Jambon and Smetana, 2012).
- ii. **Privacy risks:** This involves giving/posting personal information, attacks on privacy, hacking and identity theft. Many young students post their personal information, onto social media websites. Research shows that 31% of boys and 27% of girls admitted that they had carried out this act (Livingstone and Haddon, 2008). The posting of personal information and personal pictures can lead to many risks, such as harassment, cyber-bullying, privacy attack and unwanted sensual solicitations (Livingstone and Haddon, 2008).

According to the FBI, cyber terrorism could be any means of threatening others. Another form is hacking. Nowadays hackers are able to penetrate even fairly well-protected systems, which poses a great threat to the security of individuals and nations alike and increases the risk to young people and children (Singh and Siddiqui, 2011). Identity theft is an easy and anonymous way to carry out illegal acts without being exposed to any risk of getting caught (Singh and Siddiqui, 2011). Phishing is a common method of internet attack to get personal information like name, date of birth, credit card number or bank account. People receive fake mails from banks with Yahoo or Gmail identities, asking them to share certain information without which their accounts will be closed (Avais, Wassan, Narejo and Khan, 2014).

Igwe and Ibegwam (2014) highlighted some cyberethical issues to include plagiarism, copyright, hacking, fair use, file sharing, online etiquette protocols, posting incorrect/inaccurate information, cyber-bullying, stealing or pirating software, music and videos, online gambling, gaming and internet addiction. Others are privacy, security, electronic monitoring of employees, collection and use of personal information of consumers and identity theft.

Brey (2007) posited the following six types of morally questionable behaviour that depend on the use of information technology in higher education.

1. Digital plagiarism

Plagiarism is a common form of academic dishonesty that has habitually existed in education and among academics. It is one of the major forms of academic violation, where assignments handed in by students may turn out to be copied version in whole or in part of an existing published text. Nowadays, the advent of information technology and its accessibility to students has added to the sources that students have at their disposal to plagiarise with minimal detections (Vedder, 2008:343). As Austin and Brown (1999) have argued, plagiarism has become easier for college students in some ways. Word processing programmes permit students to simply cut and paste data from the Internet or different electronic media to develop a paper that seems to be an original work and students' use of internet data which will be unobtainable in early sources makes documenting educational dishonesty tougher for the faculty (Hinman, 2008). Notably worrisome is the existence of -term paper mills, which provide pre-written term papers to students on a spread of topics, as well as others which provide already written papers specifically for undergraduates for a fee (Brey, 2007).

2. Breaking copyright and software theft

Osborne (2017:112) reiterated that digital piracy and unauthorised copying of copyrighted media (music works, movies and software programmes) is widespread throughout society. Moreover, those who engage in such activity do not consider themselves to be doing something that is patently immoral. This is certainly true for undergraduate students. Nwogu (2015) and Osborne (2017) found that most students who engaged in the act do not perceive the illegal copying of patented materials as unethical behaviour. This attitude of college students seems to match developments in the current information age, in which the Internet increasingly functions as the most important information medium that people use.

Himma (2008:150) has argued that the very structure of the Internet undermines the notion of private intellectual property on the web. The inner dynamic of the Web moves us increasingly toward a much more communal notion of property. As he explains, the Internet encourages copying because the very nature of information technology necessitates making copies, and perfect copies can be prepared at almost no cost because making digital copies does not involve physical theft from the person who owns the original. It may be added to this that many information sources on the Internet are not obviously copyrighted, and many even lack an identifiable author (Thelwall,

2002; Brey, 2007).

3. Hacking

Hacking involves breaking into cyber technology devices for unauthorised purposes, which may be either mischievous or non-malicious. Hacking includes snooping around on someone's personal computer through isolated access, destroying or modifying files to which one has not been allowed access, releasing computer viruses, file or password theft, exposing personal information, and electronic fraud (Adam, 2008:154).

Malicious hacking is clearly an immoral act that students may engage in for a variety of reasons. They may simply be oblivious of their transgression into a computer system, they may just be curious, they may be out to harm someone, they may want to benefit themselves, or they may have entirely different reasons. Non-malicious hacking, on the other hand, has been defended by hackers as morally acceptable and socially harmless or even beneficial (Baase, 2012).

Clearly, academic institutions need strong policies and guidelines on hacking (including policies that define what kinds of information technology access are unauthorised for whom) and probably need to distinguish malicious from non-malicious hacking (Brey, 2007).

4. Improper use of information technology

Hacking is the unauthorised use and access to information technology resources to which one is not supposed to have access. However, students may also have authorised access to the network resources of the university, but then go on to use these resources inappropriately. They may have a university Internet account, or they may use their personal devices on the network or computer software that is owned by the university, or they may use computerised services offered by the university and do so in a way that does not meet the university's standards for proper use of that particular resource (Tarafdar, Darcy, Turel and Gupta, 2015).

For example, students may open up a popular website or service that generates loads of traffic that incapacitates the university's server: e.g., peer to peer downloads of music and films. Likewise, staff members may use the university's server or official devices to view or download content that is either illegal or against the university's policies (e.g., pornography or racist contents). Members of the academic community may also spread computer viruses or worms. Clearly, universities need to enact policies where there is non-regarding the ethical use of cyber technology resources in an

academic context by students and staff (Brey, 2007).

5. (Anonymous) harassment and hate speech

In universities, there may be various electronic means of communicating messages to other members of the academic community, as well as to persons outside the university. As in face-to-face communication, these information technology-mediated forms of communication can be used to bully, send threatening, obscene, inflammatory or harassing messages. These may include discriminatory messages to disparage individuals or groups based on gender, race, sexual orientation, religion, age or disability. Such messages are generally not considered acceptable in an academic setting, as educators strive to ensure that the classroom, if not the campus at large, functions as a safe, non-threatening environment for students as well as for staff (Bynum, 2008).

Baase (2012) observed that an attribute of information technology-mediated communication that deserves special discussion is the ease of sending anonymous or pseudonymous messages: for example, using anonymous remailer services. She pointed out that anonymous messages posted over the Internet can have good and bad uses. She claimed that anonymity provides protection for victims of violence and abuse and users of illegal drugs, who seek counselling and advice, and for whistle-blowers who wish to report unethical or illegal activity in their organisations, without fear of retribution. However, anonymity can also be used for negative and anti-social purposes: to perpetrate fraud, to harass people, to threaten or libel people with impunity, and to ruin their reputation by spreading rumours (Kling, and Courtright, 2003; Brey, 2007). Universities may hence want to consider having policies for anonymous electronic communication.

6. Breaches of information privacy and confidentiality

Privacy is generally considered to be an individual right in western countries, and many nations have privacy laws (or data protection laws, as they are sometimes called in Europe). It is nowadays generally recognised that new technologies, and particularly information and communication technologies, raise new privacy issues (Reynolds, 2015:75). Privacy issues for example concern electronic databases and online privacy (Cate, 1999; Brey, 2007).

Many of these new privacy issues can be expected to apply to universities that make use of online instructions and communication. In such universities, many important activities of members of the university can, in principle, be monitored or recorded electronically. This includes not only student

administration but also classroom discussion, student-to-student and student-to-faculty e-mail contact, and the online behaviour of students in general. The walls of classrooms and offices of such universities are more permeable than those of classical universities, making eavesdropping much easier, and it happens much more frequently that the things that are said and done in them are recorded so as to be available for later scrutiny, or can be copied for distribution (Reynold, 2015:76).

Privacy policies remain limited in many conventional academic institutions for the protection of student records from being accessed by third parties without authorisation. It is now common to find many student records are nowadays stored in electronic format. These policies must be supplemented with good system security. Electronic records should be adequately protected so as to avoid unauthorised access to them. Many universities nowadays also have policies that address the electronic posting of grades, which are considered to be privacy-sensitive. Many more privacy issues can be raised at a university that has much of its communication and instruction online (Roblyer, McDaniel, Herman and Witty, 2010).

Considering the confidentiality of asynchronous online group discussion or one-to-one and one-to-many, members of such groups cannot be too sure of the privacy of their discussions and that social or academic engagements are not logged or monitored by administrators, and whether in some cases access to them cannot be easily hacked. In a study of privacy in online learning environments, Tu and McIsaac (2002:135) contend that discussions over a connection that is not secure may force students to risk personal information disclosure or inhibit discussions in the group. He argued in favour of more private interaction environments, which he claims to be key to increasing interactivity. As he claims, a sound learning environment will allow learners to adjust to the ideal levels of privacy and give students more secure and more comfortable environments to increase their social presence to enhance social interaction.

Other relevant online privacy issues that may occur include:

- 1. *Personal information on public computers:*** Public access to university information technology devices in the student lab may inadvertently expose digital footprints of the user's personal information on the accessed computers. For instance, cached web pages (accessed web pages that are left in temporary storage on the disk drive and may remain there even after a browser is closed) and cookies (small files that are put on a hard disk by a website to identify users and

their preferences) may be available for inspection by others (Beycioglu, 2012).

2. *File sharing:* Student or faculty computers may contain software that makes files on them accessible to other users on the campus network and outside without knowledge of the owner, or allow files to be stored on a central server that are then accessible to others without their permission. This could allow strangers to read these files that may contain personal information (Brey, 2007).

3. *Publicly accessible institutional databases:* Many universities have databases that have public access: for example, databases that contain directories for students and staff, and repository containing students' thesis and dissertations. These databases may contain privacy-sensitive information for which students and staff have given no permission (Brey, 2007).

4. *University web pages and bulletin boards:* Web pages maintained by the university, faculty or students might contain personal information that invades the privacy of others. Likewise, postings and re-postings (forwarded messages) on bulletin boards or in other electronic forums may contain personal information of third parties for which no authorisation has been given (Brey, 2007).

5. *Search engines:* Search engines may be another means through which personal information on students and staff can be harvested. For instance, a university's own search engine may be used to harvest personal information that is found on the university's intranet or website. Where such search engine has access to many sites, it may give a detailed profile of members of the academic community. It may tell about a student, for example, the courses he/she is enrolled in, the groups he/she is a member of, and the campus events he/she has participated in (Brey, 2007).

6. *Third-party market research:* Students are potential population for some online marketers and market researchers, and they may often enlist educators to help them acquire digital information on students or solicit directly to students. The private data collected by these parties is likely to be sensitive. It is incumbent on university to have privacy policies to protect the privacy rights of students and to create secure learning environments in which members of the community interact with each other on the basis of trust (Mayer and Mitchell, 2012).

Wagner and Sanders (2001), in their study in the United States of America, developed a profile of those who illegally copy software by looking at undergraduate and graduate students and the extent

to which they pirate software. The results, based on self-reporting, revealed that males pirate software more frequently than females, and older students more than younger students.

3.8 Empirical Evidence on the Influence of the Constructs of TPB on Cyberethics

Behaviour Intention of Undergraduate Students

The Theory of Planned Behaviour (TPB) is an extension of the theory of reasoned action (TRA) formulated by Ajzen (1985). The theory states that behavioural intention is a function of attitude towards behaviour and subjective norms. The theory has been applied to ethical decision-making as it relates to cybertechnology usage. The theory espouses three independent factors: attitude, subjective norms and perceived behavioural control.

3.8.1 Influence of attitude on cyberethics behaviour intention

Siegfried (2004) noted that university students' attitudes towards various cyberethics behaviours, such as software and music download, are generally perceived as acceptable. He went further to say that university students believe that using a university system for their personal benefits is not a bad habit since it does not affect others negatively. Aliyu et al (2010) note that attitude towards cyberethics behaviour significantly influences the way cybertechnology is used. According to Ajzen and Fishbein (1980), perceptions of one's attitude can influence the individual to act unethically. Attitudes towards cyberethics behaviour were shown to depend on some background factors, such as general attitude, personality traits, moral values and the sense of right and wrong. Other studies have identified perceived personal gain, personal beliefs and attributes (i.e. religious values) (Leonard and Cronan, 2005; Kreie and Cronan, 2000). Attitude towards cyberethical intention has also been blamed on economic and hedonic benefits and negative moral judgement (Cesareo and Pastore, 2014). Chiang and Lee (2011) note that female students in a Chinese university have high regard for effective use of cybertechnology, particularly in respecting regulation, privacy and intellectual property rights. It can be said that many undergraduate students have negative attitudes to cybertechnology usage because there is a lack of legal and moral restriction. Negative attitudes to the use of cybertechnology have brought about great loss to many companies. Vitell and Muncy (2005) stated that \$1.5 billion was lost in the United States due to piracy of cybertechnology software.

Kreie and Cronan (1998) estimated that billions of dollars were being lost to piracy due to various unethical uses of cybertechnology, mostly by university students all over the world. Martin, and

Woodward (2011) maintain that a better understanding of users' attitudes toward effective use of cybertechnology is necessary because it will provide opportunity for the Internet to flourish as a safe place, which will reduce both the internal and external threats to information and communication technology and systems.

Prosser and Ward (2000) argue that positive attitudes of university students to ethical usage of cybertechnology will promote effective teaching and learning in the university environment. Studies on attitudes toward ethical usage among university students in Turkey (Beycioglu, 2009) revealed poor attitudes toward cybertechnology usage, particularly among learners in lower levels in the universities. Peace, Galletta and Thong (2003) conducted a study on 201 undergraduate students using TPB. The study discovered that individual attitudes, subjective norms and perceived behavioural control were significant precursors to the intention to illegally copy software. Snyder, Jones, and Lo Bianco (2005) noted that the attitudes of parents towards the use of cybertechnology influence how their children will use cybertechnology.

Kelly, Lyng, McGrath and Cannon (2009) discovered that there is a positive relationship between age and respondents' attitudes as related to information system ease of interaction. Lehnerk, Park and Singh (2015) listed various factors that influence unethical behaviour and the use of cybertechnology among universities to include economic factors, social factors and cultural factors. ICT researchers observe that poor attitudes and unethical use of ICT among universities is a serious problem in the ICT and educational sectors (Chatterjee, Sarker and Valacich, 2015; Karim, Zamzuri and Nor, 2009).

Al-Rafee and Cronan (2006) argue that university students' attitude toward digital piracy is a function of their beliefs, which is related to their behaviour, including happiness, excitement, age and perceived importance of the issue. Banerjee, Cronan and Jones (1998) listed various determinants that influence information ethics attitudes to include moral beliefs, organisational climate and self-esteem. Kuo and Hsu (2001) linked information ethics attitude to self-efficacy, Thong and Yap (1998) attribute it to ethical judgment processes, while Sims, Cheng and Teegen, (1996) and Gattiker and Kelley (1999) cited age as a determinant. In addition, gender, age, marital position, level of education and cybertechnology knowledge and experiences are some of the factors that influence both negative and positive attitudes in cyberethics behaviour (Loch and Conger, 1996; McCabe, Butterfield and Trevino, 2006). Loch and Conger (1996) argued that

individual character is the factor that determines ethical and unethical issues relating to cyberethics behaviour, particularly among university students.

3.8.2 Influence of subjective norms on cyber behaviour of undergraduate students

Subjective norm can be described as perceived social pressure needed to perform or not perform a particular behaviour. It is the individual's perception of the social pressures put on him to perform or not perform the behaviour in question (Ajzen, 1985). Subjective norms are the normative beliefs held by the individual. Various researchers have examined cyberethics behaviour using subjective norms (Al-Jabri and Abdul-Gander, 1997; Al-Rafee and Cronan, 2006; Cronan and Al-Rafee, 2008; Conger, Pratt and Loch, 2013). They employed subjective norms to explain cyberethics behaviour among university students. Some studies regard unethical usage of cybertechnology among university students as a serious issue (Moores and Chang, 2006). Subjective norms are personal, behavioural and social norms, including the influence of parents and friends who provide norms and value judgment that can influence behaviour (Grube, Morgan and McGree, 1986). Leonard, Cronan and Kreje (2004) conducted a study among students in an American university. The study investigated cyberethics issues concerning ethical behaviour intention using subjective norms. The finding revealed that behavioural intention was basically influenced by attitude, personal normative beliefs, ego, strength, sex and moral judgment. In addition, Al-Rafee and Cronan (2006), Peace et al. (2003), and Bebetosi and Antoniou (2009) studied the university perception of information ethics. It was discovered that attitudes and beliefs about personal behaviour have influence on cyberethics behaviour, especially concerning the use of cybertechnology.

According to the Theory of Planned Behaviour, the stronger the subjective norms, the stronger the intention to perform a behaviour (Ajzen, 2005). This indicates that university students experience social pressure from referents not to engage in a behaviour, and it may prevent them from avoiding the negative behaviour. The Theory of Planned Behaviour has been discovered to influence unethical behaviour in the use of cybertechnology (Beck and Ajzen, 1991; Passow et al., 2006; Stone et al., 2010). The construct in favour of subjective norms has been found to be positively related to unethical use of cybertechnology among university students (Stone et al.; Mayhew et al.). In another study among engineering and humanities students in a university in the USA, findings revealed that subjective norms are more strongly related to intention to engage in cyberethics behaviour among

the university students (Harding et al.).

Whitely (1998) argued that unethical use of cybertechnology is higher when university students perceive that society is encouraging various forms of negative behaviour. University students may engage in unethical use of cybertechnology if it is an acceptable norm in the society. McCabe and Trevino (2001) note that unethical behaviours were lower when university students perceived that their course mates would disapprove if they engaged in the acts. Udris (2016) conducted a cross-national academic survey to examine the role of family, school and other social norm variables on cyberethics behaviour of adolescents. Using 68,507 participants drawn from 30 countries, the study revealed that all the social variables were significantly associated with either illegal downloading or hacking to some degree.

Stone et al (2010) Beck and Ajzen (1991) and Harding et al (2007), in their various studies noted that subjective norm is a factor that influences intention of university students to engage in various unethical behaviours. Beck and Ajzen (2007) noted that subjective norm is significantly related to the intention of university students' academic misconduct (Stone et al 2010).

In addition, subjective norms have been seen to be significant predictors of intention to engage in unethical cyber behaviour by undergraduate students. It was also discovered that subjective norms were a major factor favourable towards academic dishonesty, which significantly influenced the intention to cheat in tests and examinations (Mayhew et al., 2009). This could be explained by the fact that university students held an unfavourable subjective norm towards cyberethics behaviour. The unfavourable subjective norm could be relevant to their normative beliefs to comply with their mates who are perceived to be disapproving of unethical behaviour in cybertechnology usage. This implies that subjective norms towards unethical behaviour could lead to a decrease in the intention to engage in unethical behaviour when using cybertechnology among university students. This may lead to lower reports or involvement in unethical behaviour in the use of cybertechnology by significant others.

3.8.3 Influence of perceived behavioural control on behavioural intention towards cyber behaviour

Unethical use of cybertechnology was found to be very high among university students when they perceived that their mates were engaged in various negative ways of using cybertechnology (McCabe and Treviño, 1997). Knowing that their mates have previously engaged in unethical use

of cybertechnology and are getting away with it may increase the desire to join in the behaviour. Peace, Galletta and Thong (2003) conducted a study among university students. Their findings revealed that individual attitudes, subjective norms and perceived behavioural control were very significant precursors to the intention for them to illegally download pirated software. It has been reported that there is a significant relationship between lower academic levels and unethical use of cybertechnology in universities. It was discovered that unethical use of cybertechnology was higher among university students who perceived themselves to be more knowledgeable about the use of cybertechnology (Whitely, 1988).

Stone et al (2010) employed the use of structural equation modelling to show that there is a direct path, not only from perceived behavioural control to intentions but also from behavioural control to unethical behaviour, in the use of cybertechnology. Ajzen (1988) noted that perceived behavioural control reflects the individual's opinion of their ability to perform the behaviour. Perceived behavioural control includes the university students' perception of their own skills, abilities, emotions, compulsions, opportunities and dependence upon others. The Theory of Planned Behaviour indicates that perceived behavioural control influences intention and behaviour. These were not supported in the research conducted by Foltz, Schwager and Anderson (2008), which revealed that many university students do not apply cybertechnology policies, which are supposed to guide them on the ethical usage of cybertechnology.

3.9 Ethical Issues and Intellectual Property

The issues concerning intellectual property have been of interest to cyber ethicists, who frequently attempt to identify attitudes of users of cybertechnology towards the ownership of content or software (Stahl, Eden, Jirotko and Coeckelbergh, 2014). According to Kuzu (2009), ethical issues arising from intellectual property are about the most controversial. Intellectual property is a creation of the mind or the intellect, such as literary or artistic work, innovation, design, trading style, computer notation or programmes, with a commercial value, which includes, but is not limited to, copyright property. Intellectual property is the major mainstay of the information industry. The laws of South Africa identify three types of intellectual property: patents, which protect inventions; trademarks, which protect the unique name or symbol identifying businesses or products; and copyrights, which protect the original works of authors, composers, artists, musicians, film-makers and software developers (Vedder, 2008:375). Due to their intangible nature, vulnerability to stealing and unethical

appropriation, creators of intellectual property are awarded some forms of rights and protection to prevent other persons from illegal use and appropriation (Spinello, 2011; Adekola and Eze, 2015). Such forms of legal award are often referred to as intellectual property rights. The governments of South Africa and Nigeria have laws for the protection of intellectual property in their various constitutions.

Another important ethical issue is accuracy of information. Kenneth and Donald (2015) opine that accuracy is the degree to which information on or in a digital database matches true or accepted values. Considering the amount of information generated per second, inaccurate information, as a result of unethical behaviour regarding cybertechnology use, might cause unbearable damage to individuals or institutions. In the pursuit of accurate information for nation building and promotion of democratic values, the Independent Communication Authority of South Africa (ICASA) approved the code and mechanisms for the National Association of Broadcasters on content regulations. One of its functions is to monitor the environment and enforce business compliance with rules, regulations and policies. Similarly, the Nigerian government has signed the Freedom of Information bill into law to enable the citizens have access to accurate and reliable information on social, economic and political issues.

Another ethical issue has to do with privacy rights. The modern privacy benchmark originated from the 1948 Universal Declaration of Human Rights. It established the protection for territorial and communication privacy. Privacy right is also found in various other international instruments (Bygrave, 2014:196). Privacy is at the core of any fledgling democratic system like Nigeria and South Africa. Constitutional provision for the protection of privacy is stipulated in the South African common law in Section 14 of the 1996 constitution of South Africa. Data protection in the processing and handling of personal information is also an aspect of safeguarding right to privacy, and it is guaranteed legal protection in the constitution of South Africa. The act states: *“A person’s right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions”* (Protection of Personal Information Act, 2013).

In the same vein, the right to privacy is provided for in Section 37 of the Nigerian 1999 Constitution. The Data Protection Act drafted as an instrument to guarantee protection for privacy as a result of the threat brought about by cybertechnology is inconsistent with international legal obligations (Federal Government of Nigeria, 1999).

3.10 Challenges in Efforts by Undergraduate Students to Act Ethically Correct in Cyberspace

According to a policy brief of the Economic Commission for Africa (2014), the growth and increasing cyber technological exposure in Africa, and especially in the educational sectors, is characterised by cybercrime and a lack of policy. Most computers are infected with viruses and other malicious software and there is limited level of awareness of cybertechnology-related security issues, i.e. cybertechnology regulations, laws and other allied agencies. Bear (2014) commented on challenges in the efforts made by students to act ethically in cyberspace on university campuses and the challenges of teaching cybertechnology misuse implications. He argued that, in the institution explored, ethics is often the last priority. Other factors include restricted perceptions of cybertechnology literacy, problems measuring objectives related to computer implications and ethics, lack of trained staff and f teaching materials about cyberethics. Walczak et al (2010) highlighted lack of adequate training on cyberethics, lack of incentives to incorporate cyberethics into the curriculum, inconsistent policies on academic dishonesty on campus, curriculum overload, lack of room for cyberethics education, lack of qualified academics who are trained to teach cyberethics, and the restriction perception of cybertechnology.

Despite the undeniable benefits ascribed to cybertechnology, users and organisations are confronted with new challenges stemming from unethical information practices including invasions of personal privacy and theft of intellectual property (Stylianou, Winter, Niu, Giacalone and Campbell, 2013). A study by Lee (2010) cited in Greening, Kay and Kummerfeld (2006) also highlighted some barriers to students' ethical behaviour in the university cyberspace as it concerns the problem of the integration of ethical contents into technical units. Others have, however, noted that separating the moral issues will result in a lack of connections and will poorly reflect injection of ethical issues and computing into the field. This notion was also articulated in the study by Melo, Claudia, De Sousa and Thiago (2017) whose study expressed concern about the open challenges facing the educational system due to lack of coordinated and isolated courses delivery in cyberethics education for undergraduates engineering students. Indeed, cyber security experts estimate that 80 per cent of personal computers on the African continent are infected with viruses and other malicious software (Dolliver and Poorman, 2018:139). The increase arose from growth

and increase in technological exposure.

In their study, Lowry, Posey, Bennett & Roberts (2015) drew attention to the challenges of internet policy development and suggested that acceptable use policies are generally drawn up after an incident has occurred and are usually reactive in nature. Using this model, policy developers initiate standards for dealing with specific cyber behaviours that have previously occurred while trying to forestall future problems. Thus, the articulation of the acceptable use policies often conveys a disciplinary tone understood by students and other users as rules to follow, as opposed to a guiding framework for decision-making (Herath and Wijayanayake, 2009).

Iorga and Sztankovszky (2013) in their study of university students in Romania found that intellectual theft is the most common unethical cyber behaviour in the universities. They asserted that the gains obtained by intellectual theft are both direct and indirect in the academic environment, in that students plagiarise in order to write their undergraduate theses while their professors plagiarise in order to be promoted. Iorga and Sztankovszky (2017) reported that the term “copying” is a general one to students, who do not differentiate between copying from their colleagues, from written sources during exams or from books or specialised publications in order to write an essay.

Closer home on the challenges in efforts for students to behave ethically correct in cyberspace are studies done by researchers in Africa on the phenomenon of cyberethics. For instance, Dadzie (2011:68) observed some internal and external obstacles in information ethics within the context of the university environment in Ghana. The study noted a lack of teaching module on cyberethics and a lack of experts and professionals to teach the course, since most faculties in the institutions are already overburdened with different courses, which makes the introduction and subsequent approval of a new course by the academic board of the university in Ghana a hard decision to take. The study also observed external challenges like the absence and lack of policies or laws, the absence of national strategies or national information policy (NIP) on cyberethics or information ethics. The situation, as noted by the author, may not be unconnected with the slow nature of the judicial system to curb the negative practices regarding cyberethics behaviour. An earlier study by Ocholla (2009:86) also noted these and more challenges. Other challenges faced by undergraduate students in their efforts to act ethically correct in cyberspace include restricted perceptions of computer literacy and cybertechnology, problem with the objectives related to cyber technology

implications and ethics, lack of trained staff, and the lack of teaching content and materials (Haughton, Yeh, Nworie and Romero, 2013).

3.11 Influence of Cyberethics Policy in Strengthening or Promoting Ethical Conduct in Cyberspace

Academic institutions recognise the importance of curtailing students' internal cybertechnology misuse or unethical cyber behaviour, defined as students' unacceptable use of cybertechnology in terms of application, organisation and ethical conduct in cyberspace (Phyo, Furnell, and Phippen, 2007). There are several strategies used by institutions to reduce unethical cyberethics behaviour. Surveillance systems and continuous monitoring are being adopted by institutions around the globe to spy on their students and other users of their network. (Zetter, 2007). Adopting policies is another method used by institutions to deter misuse (Case and Young, 2002). The most common form of regulation of cyber behaviour within academic institutions is the acceptable use policy (AUP), which is seen as a major step towards promoting cyberethics. The AUP, or cyberethics policy, is usually a document that every user of cybertechnology within academic institutions must sign prior to accessing the resources on the university network. Its aim is to prevent illegal and unethical activities within the institution's cyberspace. The overall goal of the institution's cybertechnology service is to enhance teaching, learning and innovations, such that any activity that is not related to this goal could be frowned upon. The development of acceptable use policy serves as a reactionary attempt to cope with unethical cybertechnology behaviour, both inside and outside the university environment. This approach has created a debate around the role that institutions must play in policing inappropriate activity and the effectiveness of such policies (Davidson & Gottschalk, 2010:7).

Supporters of acceptable use policy emphasise the need for a clear course of action for dealing with ICT issues. According to DiScala and Weeks (2013), established internet policies help to remove uncertainty regarding the security of computer equipment, access and sharing of materials and the availability of services. In a hierarchical analysis of acceptable use policies, Laughton (2008) notes that policies often serve to interpret the role of technology in the educational curriculum and, as a result, faculty, students and the public gain the level of assurance necessary to use cybertechnology in a responsible manner. Dill (2005) states that in addition to establishing guidelines for responsible use, written policies provide the reason and support for administrative

action when dealing with specific issues that occur within the university.

Critics of AUP suggest that using it as the sole method for dealing with ICT issues is an insufficient way to establish a culture of responsibility for ICT use. Scholars highlighted the challenges that arise in both the development and application of the policy, and suggested that the result is the establishment of ambiguous guidelines inapplicable to practical circumstances (Boynton, 2004; Kafai, Nixon and Burnam, 2007).

In their recent work, Lowry, Posey, Bennett and Roberts (2015) draw attention to the challenges of internet policy development and suggest that AUPs are generally drawn up after an incident has occurred and are, therefore, reactive in nature. Using this model, policy developers initiate standards for dealing with specific cyberethics behaviours that have previously occurred while trying to forestall future problems. Thus, the articulation of an acceptable use policy often conveys a disciplinary tone understood by students and other users as rules to follow, as opposed to a guiding framework for decision-making.

Many researchers (Lennie, 2013; Simonson, Smaldino and Zvacek, 2014) have also recently found that in many cases, students demonstrated misconceptions about internet policies that existed within their institutions, and this misunderstanding led to inappropriate use. A recurring example that proves this misunderstanding is the conflicting perceptions students have regarding the violation of intellectual property rights. Lewis, Ross and Holden (2012) found that despite policy guidelines regulating the copying and distribution of shared software programmes, students remained uncertain about what constitutes a copyright infringement. In addition, the conflicting legal and ethical principles surrounding the broader issue of intellectual property rights created confusion about what a violation of copyright actually is. What is apparent in these examples, as well as many others, is that while trying to integrate cybertechnology into teaching and learning and instruction process, managements of institutions must deal with highly debated, continually changing, and often times difficult to understand policies regulating students' cybertechnology behaviour and internet use (Davies, 2002:60).

Taherdoost, Namayandeh and Jalaliyoon (2011) conducted an academic survey to investigate knowledge of educational framework on the future career and behavioural experience of undergraduate students in dealing with ethical dilemmas and cybertechnology ethics. The study suggests that there is a need for concrete efforts by professional bodies and institutions to update

policies, codes and rules guiding ethical behaviour in cyberspace. Livingstone, Haddon, Görzig and Ólafsson (2011) found that users also showed a lack of awareness regarding the guidelines in their institutions' policies and tended to use personal judgments when deciding what constitutes inappropriate use. Renee Taylor, Won Whang and Tettegah (2006) also found that faculty and students did not share the same perspectives of issues relating to cybertechnology use, which led to differing interpretations of written policies.

3.12 Ethical Theories and Cyberethics

The etymology of ethics comes from the Greek word “ethos”. Ethos reflects guiding beliefs or ideals that govern a community, such as: practical skills, wisdom, virtue, goodwill and goodness. Ethics can be described as the systematic study of morality. Britz (2013) views ethics as the study of human behaviour regarding what is good or bad about man and how he relates with himself and others in the environment. Every human society practices ethics because every society attaches value, on a continuum of good to bad and right to wrong, to an individual's actions, according to where the individual's actions fall within the domain of that society's rules and canons (Blaj, 2017).

Ethics can take so many different routes so that one may not be able to decide easily on what is truly ethical from a theoretical perspective. The interpretation of what is ethical might also differ according to situations. However, there are some universal guidelines that guide human actions in all societies, such as do not kill, steal or lie. Nonetheless, it should be kept in mind that, sometimes, there is no generally appropriate method for acting and also the decision of how you can act needs to comply with an evaluation of choices as well as repercussions originating from each choice. This is where moral concepts assist in examining exactly what would certainly be one of the most honest habits when encountering an ethical dilemma (Mihelic, Lipicnik and Tekavcic, M., 2010). Morality can be regarded as the set of norms that guides human factual behaviour, whereas ethics is seen to be the theory and reflection of morality. Morality could also be seen as social conventions about right and wrong that are so widely shared that they become the basis for an established consensus within a given society (Fodorean, 2018). Quinn (2014) distinguished morality and ethics by stating that morality is the guideline that describes moral behaviour, while ethics is the rational examination of any behaviour or circumstance to determine wrong or right using an ethical theory or theories. Morality is practice (normative) and ethics is rational examination (objective). An ideal

goal of this moral philosophy is to better understand the universal dichotomy that differentiates right and wrong actions. Although almost everybody would concur that cheating and lying are dishonest, viewpoints about exactly what makes up ethical habits can differ drastically. Mindsets towards cyber piracy - the practice of unlawfully downloading music and films and making copies of software application or allowing others to gain access to software application to which they are not entitled - range from strong opposition to approval of the practice (Namlu and Odabasi, 2007:212).

Cybertechnology ethics reflect the current trend in research attention to information and communications technology (ICT). The review of cybertechnology ethics or cyberethics was based on the more established fields of computer and information ethics. Computer and information ethics as a branch of applied ethics can be described as that field of study that analyses social and ethical impacts of ICT (Baynum, 2008). The more specific term, cyberethics, is a dynamic field of study that identifies ethical issues in the use of cybertechnology, the corresponding moral, legal and social implications and the evaluation of the social policies and laws that are framed in response to issues generated by its impact on the society (Tavani, 2013; Spinello, 2012; Kizza, 2013; Quinn, 2013; Baase, 2013). The study of cyberethics, which includes computer ethics, has grown significantly since the early 1980s when Moor (1985) and Johnson (1985) published seminal papers that helped defined the field and, ever since, the field has grown in strength and recognition among communities of information science (IS) scholars. Cyberethics, as a field of applied ethics, is related to information ethics - a more general field which includes computer ethics, media ethics, library ethics and bio-information ethics (Stahl and Flick, 2011).

An ethical theory establishes if an activity or collection of activities is ethically right or wrong. Codes of ethics are prepared based on ethical theories. Furthermore, ethical theories additionally explain the procedures of reasoning, description, as well as justification made use of in ethics (Frize, 2012; Kizza, 2013). There are many ethical theories that have been discussed in the field of cyberethics by various researchers. Many studies have been undertaken recently that draw on moral theoretical concepts to bear on the behaviour of cybertechnology among young adults within the university environment. Some authors (Grunwald, 2005; Granitz and Loewy, 2007; Zhang, 2010; Calvani, Fini, Ranieri and Picci, 2012; Plaisance, 2013) have called for a consideration of the moral dimensions of cybertechnology; yet others have sought to advance some universal

ethical principles for the use of cybertechnology (Capurro, 2006). The moral ethical theories that are discussed from the ongoing are usually drawn upon by researchers in the field of cyberethics. Any of these theories could provide insightful theoretical lens into the investigation of cyberethics behaviour of young adults or undergraduates students.

Meta-ethics: As opposed to descriptive ethics, this domain consists of analysis of interpretation of key terms in ethics: for instance, justice, virtue and obligation. Put simply, meta-ethics explores the logic of moral reasoning (Briggle and Mitcham, 2012). Sometimes even meta-ethics concepts might be required to identify ethical courses of actions (Smith, Allhoff and Vaidya, 2008; Briggle and Mitcham, 2012).

Normative ethics: This could also be referred to as the middle layer of the scope of ethical theories. It theorises about the basic guidelines methodically differentiating right from wrong (Martin, 2003). Normative ethics attempts to formulate and defend basic understanding of good, principles of right conduct and the character of virtue. Normative ethics articulates what individuals should do and what they ought to believe. Much of normative ethics consists of what makes people and actions virtuous or vicious, good or bad, right or wrong. The field of normative ethics, from the perspective of researchers, could be theoretical or applied. The relationship between theory and contextual practice in ethics is, however, much debated. Some prefer the term practical ethics, arguing that moral reasoning is not as simple as applying principles of methods in deductive fashion. Others prefer a case-based form of moral reasoning that deals with the particulars of context as opposed to a predetermined theory (Briggle and Mitcham, 2012). The idea of normative ethics is to identify morally appropriate procedures within a given circumstance.

Applied ethics: A bottom layer of the application of ethical theories, this is a branch of normative ethics referring to disciplines, including medical ethics, business ethics and cyberethics (Himma and Tavani, 2008). Applied ethics is the area wherein normative ethical theories get related to specific problems within sufficiently well-defined areas of inquiry to give response to questions. In applied ethics, one is involved with the specific ethical issues that arise from the area being examined, though there may be overlap between two separate areas of applied ethics.

Deontological ethics: Deontology is derived from the Greek word *deon*, which means “duty” or “obligation”. Etymologically, it is referred to as the science of duty. The contemporary usage, however, refers to the theory of ethics whereby at least some acts are morally obligatory regardless

of their positive or negative consequence on human beings (Moriarty, 2008). Immanuel Kant, a German philosopher, was the first thinker who systematically presented the main lines of a deontological position. In Kantian ethics, the objective principles of the universal moral law have the form of commands or imperatives. Most imperatives, according to Kant, are either hypothetical (i.e. if you want X, do Y) or categorical (do not do Y). Kant believes that categorical imperative is aimed at establishing a universal law that could be valid for all rational moral agents (Stamatelos, 2007; Vargas, 2016). There are two aspects to the study of deontology: act-deontology and rule-deontology.

According to act-deontology, every judgment of moral obligation is built upon its own merits. Act-deontologists, in this regard, decide separately the correct path to take and actions to perform in each particular situation. This is otherwise known as situation-specific deontological theory. While it is accepted that a decision could be reached on the basis of intuitive knowledge, it is argued that this relates to the specific situation. Despite being situation-specific, it could also be argued that decisions are still based on intuitive values of rightness or goodness, not on any consideration of consequences (Baase, 2003:16). Many current theorists describe this as situation ethics and it is the view of ethics shared by many existentialists (Kirby and Slevin, 2003; Kizza, 2013).

According to rule-deontology, one's duty in any situation is to act within rules, without exception. Here, ethical decisions are not dependent on consequences; although, unlike act-deontology, ethical decisions cannot be situation-specific. Rather, rule-deontologists consider that universal rules apply on the basis of the universal intrinsic value or goodness of an act (van den Hoven, 2008:66). This singular interpretation of ethics is promoted by Kant, and it is the underlying principle adopted by people who claim to be guided by conscience (Kirby and Slevin, 2003; Kizza, 2013). This theory believes that an act is considered good when an individual performing the action has a good reason to do so.

Deontological theories include both duty-based and rights-based approaches to ethical reasoning (Spinello, 1997). An important implication of duty-based theories is that an individual must fulfil their duties even when their actions yield unhappy endings or consequences. For instance, deontology suggests that parents have a responsibility to take care of their children even if they have to lose some privileges. This is related to a human being's rational capability and, according to Johnson (2001), the capability for rationality is a quality that differentiates humans from other

creatures. Human beings are rational beings who are competent to deliberate within, and among themselves, and decide their behaviours. In addition, having rational capacity means having the ability to be moral: plants and animals are not moral agents because they cannot rationalise their actions. It follows that humans should live their lives seeking the greatest good, not personal happiness, because they have the capacity to recognise moral principles and to follow them. In other words, the fact that human beings are rational agents suggests that the highest goal of human beings lies beyond their personal happiness (Evans and Over, 2013:10).

In general, deontological theories argue that it is always the duty of a moral agent to do what is right. Actions performed should be such that they could serve as a model of behaviour for others. In particular, one should always act as one wish others to act towards them. It is a fundamental duty of people to treat others with respect and not solely as a means to their own purposes (Moor, 1999). Treating others with respect means not violating their rights, and fulfilling just treatment (Donnelly, 2013). Based on these stated principles, it would be wrong to steal another person's information, as doing so, according to Kant, implies that the individual from whom the information is stolen is treated to an end of achieving one's goal or economic advantage (Haupman, 2011).

The influence of Kant's categorical imperative emerges as a result of a connection between the moral and rational paradigms that it follows (Radcliffe, 1997). Particularly, Kant affirmed that a person is irrational if he or she does not accept the categorical imperative. Radcliffe expressed that the underlying concept of Kant's argument is that a moral judgment must be promoted by good reasons. The justifications are good when they apply in other cases always. As an implication of this imperative, it is wrong for someone to regard himself as special and violate a law. Valid moral reason is consistent with all people always. If it follows that consistency is a requirement of the categorical imperative, then rational agents accept the categorical imperative because rational agents accept the concept of consistency. The acceptance of the principle of categorical importance on rational agents implies that they desire to discard their needs or desires and follow moral rules (Tavani, 2013). Radcliffe (1997:112) posits that, although Kant was not the first philosopher who acknowledged a requirement of consistency in moral rules, "He was the first to make it the cornerstone of a fully worked-out system of morals".

Criticism of the categorical imperative lies in the analytical disagreement that ethical rules are absolute. Particularly, the concept does not address circumstances where universal guidelines

conflict (Spinello, 1997). Kant argued that one ought to refrain from an act known for being evil despite the fact that it may generate good consequences. For example, Kant pointed out that an individual ought not to lie even when lying could save another person's life. He affirmed that the implications of a decision are always unknown. Consequently, one should prevent any known evil act. A criticism of this view emphasises Kant's denial of ethical responsibility for any negative consequences that can result through following moral rules, while he favoured responsibility for any bad consequences from unethical acts (Radcliffe, 1997:73).

In addition to the Kantian version of the deontological theory, there is also W. D. Ross, who observed, like other deontological philosophers, that everyone has duties to perform as a reflection of their moral convictions (Fieser, 2009). His theory, however, differs from others in that it includes a *prima facie* duty, the actual duty an individual chooses when two or more of his duties are in conflict due to a more important or higher obligation. This difference makes his theory an extension of Kant's (Spence and Quinn, 2008). Precisely, Ross agreed with Kant that moral rules are ultimate and irreducible (Spinello, 1997:35). Unlike Kant, Ross contended that these obligations are not "absolute or prevailing without exception". He used the phrase moral imperatives - which duty should apply under most circumstances - instead of categorical imperative, which suggests that obligations hold up in every situation.

Consequentialist theory: Consequentialist theorists argue that people choose the action with the most suitable possible consequences. An act is right or wrong according to its consequences. It has no moral value aside from outcomes (Bynum, 2006). An act is correct if and only if it is reasonably expected to produce the utmost good or least harm in comparison with alternative action choices. Consequentialism also requires some account of what counts as good (Briggle and Mitcham, 2012). A person is allowed to break existing rules, in a consequentialist system, only if the foreseeable consequences of that particular violation are better than the consequences of not breaking that system. However, the consequentialist system is concerned only with the foreseeable consequences of those violations, not the foreseeable consequences of that kind of violation being publicly allowed. Thus, consequentialism simply says that an action is right or wrong by relying on its consequences or effects on the society. There is no concept of what is morally acceptable, only social good, in a consequentialist system. The approach is often difficult to apply because sometimes it results in the interests of a minority being sacrificed for those of a majority. Also it is difficult to identify the majority and minority groups often times (Bynum, 2006). In addition,

there is the issue of what constitutes the “good” of the society and how to measure that “good” (Spinello and Tavani, 2004).

Utilitarianism is a form of consequentialism identified by J.S. Mill and Jeremy Bentham in the nineteenth century, to advance a decision-making rule efficient in guiding social policies in a world being modified by science, technology and the Industrial Revolution. The term utilitarianism is from the word “utility” (Johnson, 2001). Utilitarian followers are interested in only those social policies that produce utmost good for the greatest number of individuals. Consequently, this theory is established upon the principle of utility or the greatest happiness principle which states that “an action is right or wrong to the extent that it increases or decreases the total happiness of the affected parties” (Spence and Quinn, 2008:74). Additionally, utilitarianism is determined by circumstances (Johnson, 2001).

The basic principle of utilitarianism is that everyone should behave in a manner that engenders utmost happiness for the greatest number of people. A utilitarian philosopher argued that happiness is the utmost good because everything else in life is desired as a way of achieving contentment. Contentment is the utmost desire of humans, and thus all actions must be examined on the grounds of whether they maximise or diminish human happiness (Fox and Reece, 2012).

An action is therefore right or wrong depending on whether it increases the sum total of human happiness (Forester and Morrison, 1994). For Bentham, happiness is the physical pleasure one derives and hence his theory is often called hedonic utilitarianism. For Mill, happiness includes any need, desire or interest that a person decides to follow and hence his theory is termed preference utilitarianism (Guidi, 2008).

As today’s world is going through another revolution because of the advances in cybertechnology, it is essential to understand the workings and concerns of this ethical theory (Forester and Morrison, 1994). The period of progress of utilitarianism was marked by democratic development and social reforms, which were the reasons for the development of such a principle (Singer, 2011). As democratic societies increased all over the world, utilitarianism became more prominent. In one form or the other, utilitarianism is the root of largely all contemporary economics and public policy formations. Politicians and various governmental agencies commonly consider the rewards and risks that may well flow from alternate regulatory actions and adopt those judged to produce the utmost benefits (Briggle and Mitcham, 2012).

Virtue ethical theory: While consequentialist ethics concentrate on the state of affairs that arises from an agent's actions, virtue ethics concentrate on agents in their entirety (that is, their character). Virtue ethical theory is based on human character, development and personality. Johnson (2001) asserts that one meaning of virtue in the ancient Greece is excellence. The virtue theory states that character is built because of habit (Fieser, 2009). According to Whetstone (2001), virtue ethics place special emphasis on moral character development with the expectation that any subsequent decisions made by the person will be consistent with that character. Dyck and Wong (2010) explain the concept by remarking that virtue ethics are behaviours that, when practised, shape a person's character, that past actions strongly impact on a person's future actions, and that virtue ethics provide a useful means for examining the varying perceptions that drive people's actions. The idea of virtue ethics implies a group of personal traits and qualities that provide a base for an individual to lead a virtuous life and, through repeated inculcation and practice, such qualities develop into habits, which enable individuals to make the right decision when confronted with ethical situations (Charlesworth and Sewry, 2009).

3.13 Gaps in Literature

Research gap is seen as a area which missing or insufficient information limits the ability to reach a conclusion for a question (Gowry, 2014). According to Robinson, Saldanha and McKoy (2011), five types of research gaps are: population, intervention, comparison, outcomes and setting. Similarly, Miles (2017) proposed a new seven core research gaps model: Evidence gap, knowledge gap, practical knowledge conflict gap, methodological gap, population gap. The studies that informed this chapter adopted various strategies to examine cyberethics and misuse behaviour in various contexts and especially within the academic environment. Several articles were reviewed. The main approaches adopted in these studies, in order of frequency of use, are: survey, literature review, case study, meta-analysis, and others. Worthy of notice is the fact that there is not enough research in the area of cyberethics, though a considerable number of research works was done on cyberethics behaviour and other related terms. Given the focus of this study, studies of related nature are on those focusing on cyberethics behaviour. For example, Thomas and Ahyick (2010) focused on helping information systems students improve their ethical decision making. The study found that while students who had taken courses and orientation were more aware of the issues in cyberethics misuse and thought them important, their behaviour was not changed significantly. There was also no difference in their perception of what influenced their ethical decision making

despite that the students had taken an entire course module in information ethics. It also recommended a further research to determine how to help students apply ethical principles in the realms of cyberspace and their own lives. The study of Voiskounsky (2009) on web plagiarism as a cyberethics problem x-rayed how Russian students have few moral barriers to web plagiarism. The study is, however, lacking in theoretical rigour. Tahat et al (2014) used theoretical constructs to evaluate cyber ethical misuse behaviour of Middle-Eastern countries. Their study results show that respondents have lower regards for intellectual property violations. A closer study to the current one is by Chiang and Lee (2011) on ethical attitude and behaviour regarding computer use. The study adopted a survey of political science students in Taiwan to study their intentions towards observing ethics in the areas of digital right on freedom of expression, freedom of association, equal access to information, confidentiality and protection of intellectual property. The study showed that attitude, subjective norm and perceived behavioural control of the respondents all had significant impact on personal observation of information ethics, and recommended that future research is required on cyberethics in Taiwan and elsewhere.

Chatterjee, Sharker and Valacich (2015) used scenario-based academic investigation to uncover the nuances of several factors influencing young adults' unethical cyber behaviour and cybertechnology use. The study results showed nonlinear and idiosyncratic relationships between the study constructs. However, the study results suffer from some limitations and are especially lacking in appropriate qualitative data that could have revealed additional nuances in tensions and dialectic relationships in the studied variables. Similarly, a study by Acilar and Aydemir (2010) on attitudes of future managers and employees toward ethical use of computers revealed that students who use cybertechnology were more likely than not to show unethical usage tendencies and behaviour. However, the study samples were lacking in scientific rigours. A cross-cultural study conducted by Martin and Woodward (2011) compared the cyberethics of American and European technology students. They discovered significant differences in the rating of the ethicality of the studied scenarios, as American students rated most scenarios as more unethical than the European participants. The study was also lacking in scientific rigours, as samples were not scientifically representative: details of the precise socio-demographic characteristics of respondents in the context of some of the studies were generally lacking, most studies were conducted with only single methodological approach (i.e. quantitative). Another noticeable gap is that existing theories for exploring current phenomenon such as cyberethics behaviour of students

seem to be inadequate or incomplete. Therefore, the current study will fill this gap by extending the findings of these previous works, through both qualitative and quantitative methodological approaches, to unravel the phenomenon of cyberethics behaviour of undergraduate students in the studied institutions.

3.14 Implication of Literature Review

The literature review of this study has serious implications for the field of cyberethics in the African context. Although only a few studies on the topic of cyberethics have been carried out on the African continent in general, and in the countries of South Africa and Nigeria in particular, the studies conducted in the two African countries, and in other parts of the world, are represented here and as such it gives this study a universal scope in terms of literature.

The theoretical framework referenced ethical theories, focusing on the Theory of Planned Behaviour (TPB) as the main theory, which sums up all the variables that express cyber behaviours and the awareness of cyberethics. The fact that this theory covers subjective norms, behavioural control and attitudes portrays a progression of how university students operate under the aegis of the university system when utilising cyberspace.

Theoretically, often, the expression of cyberethics is planned behaviour. Although the theory has strengths and weaknesses and has been criticised for its weaknesses, it, however, thoroughly applies to the subject matter of this study because of its direct and extant relationship with other ethical theories and the practical deliberation that accompanies unethical behaviour among students in cyberspace.

Literature revealed that awareness regarding university policies on the Internet is very low among students and that many universities in developing countries do not even have policies regulating the use of cyberspace. This portrays a high level of ignorance among students and faculty regarding cyberspace even though they are in citadels of learning. This has implications for the extent of their intellectual development and adherence to global intellectual advancement.

Literature revealed that there is need to train staff and students on the preponderance of unethical behaviours in cyberspace and the necessity of creating policies to discourage the misuse or abuse of cyberspace. This implies that serious and aggressive awareness campaigns are necessary to ensure that students and faculty are aware of what is acceptable and unacceptable behaviour online,

so as to safeguard the integrity of the university.

Despite the paucity of literature in Africa, attempts have been made in this area of study, even as there is the urgent need for more studies to be conducted. Although most universities and higher institutions of education are now into online registration, and in some cases online teaching, the importance of ethical cyber behaviour is not clear to many of them.

The fact that plagiarism is one of the highest unethical behaviours among African academics and students in cyberspace is adequately captured in literature. It should be noted, however, that in some cases, what is labelled plagiarism is not really plagiarism but contents similarity. This is not meant to exonerate plagiarists but to warn academic witch-hunters against victimising competent intellectuals by lumping them with the preponderance of mediocres.

Literature showed that unethical cyber behaviour is a reality, which has bedevilled every known society covered by cyberspace. This means that the battle against unethical cyber behaviour is a global one, and requires a great deal of seriousness among all stakeholders to eradicate it. It is, however, worth noting that the baby should not be thrown away with the bath water. In other words, violators of cyberspace should be corrected and not destroyed.

3.15 Summary

This chapter comprehensively discussed concepts that are vital to the study. It examined the concept of ethics and reviewed the relationship between ethical theories and cyberethics. Areas like meta-ethics, normative ethics and applied ethics were critically discussed.

The chapter also highlighted the importance of deontological ethics as dichotomised into act and rule deontologies. Issues like consequential ethics were reviewed, while the correlation between virtue and ethics as expounded in virtue ethical theory was also critically reviewed.

The chapter also reviewed the link between cybertechnology and internet usage, while throwing more light on what cyberethics entails, the emergence of cyberethics and the incidence of cyberethics among students. Also explored was the literature that documents the level of awareness of cyber ethical behaviour among undergraduate students and the types of cyberethical behaviour that are common among undergraduate students.

The chapter discussed several empirical evidences regarding the influence of the constructs of the Theory of Planned Behaviour on cyberethical behaviour intention of undergraduate students, the

influence of attitude on undergraduate students' cyberethics behavioural intentions, subjective norms on behavioural intention of cyber behaviour of undergraduate students and perceived behavioural control on behavioural intention towards cyber behaviour among students in universities.

This chapter has provided a critical review of literature on the cyberethics behaviour and related themes, with a published study covering several continents on the globe where the phenomenon of cyberethics behaviour has been a constant cause of concern in higher education. Previous research has focused on students' attitudes toward knowledge of, and engagement in, cyberethics in overseas educational contexts, and there is also a growing body of research on African undergraduates' understanding of, and stance on, these practices. However, little research attention has been given to institutional policies on cyberethics within the African context, though similar research has been conducted in other settings. The chapter reported studies that have examined demographic variables, the Theory of Planned Behaviour, ethical theories, awareness of the phenomenon of cyberethics in the context of universities, and among undergraduate students and professionals. It was assumed that the involvement and use of cybertechnology, such as desktop, laptop, tablet, software, smartphones and the Internet for various academic activities by institutions and students required ethical conduct. The ubiquitous nature of these technologies has not only produced a dramatic increase in the incidence of criminal activities but has also led to the emergence of what seems to be a new variety of cyberethics behaviour.

This chapter also identified challenges to undergraduate cyberethical behaviour in universities and the influence of cyberethics policy in strengthening or promoting ethical conduct in cyberspace within the university environment. The major challenges faced by undergraduate students when they choose to act ethically correct in cyberspace were discussed.

The next chapter presents the research methodology for the study.

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Introduction

This chapter illuminates the research methodology, process and procedure used to explore undergraduate students' experience of cyberethics behaviour. The chapter is organised into the following subsections: Introduction, Theoretical/Paradigmatic perspective, pragmatism, and the mixed-method design are clarified and justified. This is followed by an outline of the quantitative and qualitative data collection approaches, along with justifications for each decision.

4.2 Theoretical/Paradigmatic Perspective

The construct paradigm is attributed to Thomas Kuhn. Paradigms play an integral role in science. The foundation of paradigm was laid in Thomas Kuhn's work titled *The Structure of Scientific Revolutions*, first published in 1962 (Mouton, 1996:203). Paradigms are patterns of beliefs and practices that regulate inquiry within a discipline by providing lenses, frames and processes through which investigation is accomplished (Weaver and Olson, 2006:460). Paradigms are established by communities of scholars with shared beliefs about the nature of reality and knowledge construction. As human constructions, they are historically and culturally embedded discourse practices but are neither immutable nor inviolate (Greene and Caracelli, 2003). There are various opinions on research paradigms in research enquiries. Scotland (2012) affirms that every paradigm has its link to ontological assumption as well as methodological approaches. Ontology refers to the nature and existence of social reality. Epistemology on its own constitutes that which is knowledge, and the ways of knowing together make up the foundations on which social enquiry is framed (Ngulube, 2015:127). The selection of research paradigms and methods is determined by (a) the current state of knowledge about a certain phenomenon, (b) the purpose of the study, and (c) the related research question/s (Creswell, 2013). A philosophical assumption refers to as worldviews (Creswell, 2014:7). The ontological, epistemological and methodological prescriptions of social enquiry are housed in paradigms which form the road map of any academic investigation. In the present study, an examination of a wide body of existing literature from cyberethics and related fields revealed that cyberethics behaviour is a pervasive and fundamental human motivation. However, the concept of cyberethics behaviour has been inadequately explored in extant literature. With respect to undergraduates within the academic environment in sub-Saharan Africa in particular, it was

apparent that a number of issues had not been addressed.

This study therefore sought to explore:

1. the relationship between demographic characteristics and cyberethics behaviour of undergraduate students in the two selected universities;
2. the level of awareness of cyberethics behaviour among students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria;
3. the types of cyberethics misbehaviour among students in the studied universities;
4. the influence of the Theory of Planned Behaviour (TPB) on cyberethical intention in the two universities;
5. the challenges to students' cyberethics behaviour at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria;
6. the influence of cyberethics policy in strengthening or promoting ethical conduct in cyberspace at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria.

Paradigmatic and methodological decisions were guided by the afore-listed issues for the study in cyberethics behaviour.

Exploring the phenomenon of cyberethics behaviour in relation to undergraduate students can be very challenging, just as it is to understand the inherent patterns and challenges of cyberethics misbehaviour. The aim of the study was to develop meaningful stories and to find discernible patterns of regularity amidst the variety, and contextualising same within the studied academic environments. To understand these inherent challenges and patterns of behaviour of young adults in cyberspace, it was necessary to understanding the phenomenon of cyberethics behaviour from multiple perspectives.

Cyberethics being a multidisciplinary concept, it is not inappropriate to combine different perspectives and approaches in a single study. After all, social science researchers simultaneously utilise multiple forms of data to better understand studied phenomenon

(Zachariadis, Scott and Barrett, 2013). Similarly, many authors concur that multiple paradigms can coexist for viewing the different aspects of a complex study. These provide an understanding of phenomena from different philosophical viewpoints (Creswell, 2014; Ngulube, 2015). Not surprisingly, Amirkhani, Vahdat and Khezrian (2010) view cyberethics as an interdisciplinary field that requires different forms of knowledge to better understand respondents' cyberethics intention and behaviour.

According to Adams (2008:150), the dominant paradigm or worldview commonly adopted in information studies researchers is the positivist, interpretivist and critical social theory. Ngulube (2015:127) suggests that, researchers should adopt the paradigm that is suitable to the context and issue under investigation. This means that, the worldview of a researcher allows him a greater opportunity to view the phenomenon under study with a critical mind of why and how cyberethics behaviour issues unravel in academic settings among undergraduate students.

The complex nature of human behaviour also implies the acceptance and importance of diverse perspectives. This study, therefore, does not subscribe to the assumption of incommensurability of different paradigms or that one paradigmatic approach is superior to another. In essence, the study is devoted to the acceptance of differences and diverse perspectives. The complexity and pluralism of the contemporary world demands such a commitment. However, the study acknowledges that social science and humanity researchers approach their work with a set of assumptions about the social world, the value of knowledge and the purpose of research. Whether these assumptions form a formal philosophical paradigm or are more of a crude mental model (Greene, 2007), the activity of social inquiry requires an underlying conceptualisation of the situation. Greene and Caracelli (2003) argue that research rests on the researcher's mental picture of what social reality is like, what counts as knowledge, what ought to be studied and how. Likewise, the question of values cannot be avoided, because value presuppositions influence the language that researchers and others use to describe reality. The current study shares this perception, and because of its philosophical assumptions and values, and the nature of the research project, pragmatism was selected as the most appropriate theoretical perspective. The discussion that follows details the nature of pragmatism and how it was used in this study.

4.3 Pragmatism

Pragmatism is a philosophical movement founded by Peirce (Houser, 2005) and James (1998). It is a theoretical and philosophical perspective that has become prevalent in the literature in the last two decades (Collins, Johnson and Onwuegbuzie, 2013; Teddlie and Tashakkori, 2009). The term pragmatism is derived from the Greek word for action, from which the words “practice”, “practical” and “praxis” originate (Lalonde, Bourgault and Findeli, 2010). Davies and McKittrick (2015) regarded the pragmatic approach as an alternative epistemological paradigm to positivism, which complements the weakness of one methodology with the strength of the other one and thereby circumventing the contentious issues of truth and reality. Pragmatism stresses the critical analysis of facts and practical applications of the use of pluralistic approaches to derive knowledge about a problem, and integration of findings (Creswell, 2013). Thus, rather than deductive reasoning and universal premises to attain specific conclusions, or inductive techniques that seek general conclusions based on specific premises, pragmatism approves a flexible abductive approach to solving practical problems. Johnson, Onwuegbuzie and Turner (2007) claimed that pragmatism helps the researcher to offer an epistemological justification and logic for mixing approaches and methods in a single study. Hartrick Doane (2003) claimed that this approach can move research beyond the boundaries and restrictions of a single paradigm towards theory construction tailored to fit practical situations.

The tenets of pragmatism emphasise development and change (Makinen 2008): that is, commitment to what works in practice, appreciation of plurality and desire for integrated results. Therefore, it is appropriate for the study of cyberethics behaviour.

4.3.1 Pragmatic knowledge claims

Creswell (2013) advocated that the knowledge claims behind a philosophical approach must be made clear early in the research process, as other methodological choices flow therefrom, and in fact inform the design. Asserting a knowledge claim means that researchers begin a study with certain assumptions about how they will learn and what they will learn during their inquiry. Philosophically, researchers make claims about the nature of reality (ontology), what constitutes knowledge (epistemology), what values underpin the study (axiology), how to write about knowledge (rhetoric) and the procedure for investigating knowledge (methodology). Pragmatism provides a basis for the following knowledge claims and related methodological assumptions:

- Pragmatism is not confined to one system of knowledge or philosophy or reality. Thus, the pragmatist is theoretically unencumbered by an allegiance to any one specified framework and avoids the restrictions forced by strict obedience to one epistemology (Greene and Caracelli, 2003).
- Pragmatists convey the importance of focusing on the research question/s and using pluralistic approaches to derive knowledge to best address the question/s (Tashakkori and Teddlie, 2008).
- In pragmatism, there is a concern with applications - that is, what works - and solutions to problems. Methods are not of primary importance, the problem is dominant, and researchers use all approaches to understand the problem (Patton, 2002).
- Researchers operating from this paradigm are at liberty to choose the methods, techniques and procedures of research that best address their research question (Creswell, 2013).
- Investigators often use both quantitative and qualitative data because they work to provide the best understanding of the research problem at that time (Creswell, 2013).
- Pragmatists base their knowledge claims on criteria such as accuracy, scope, simplicity, consistency and comprehensiveness (Howe, 1998).
- Pragmatists consider that single methods focus on a limited view of reality. The use of multiple methods provides a more comprehensive view by focusing on different slices of reality. Thus, pragmatist researchers are encouraged to draw liberally from both quantitative and qualitative assumptions when they engage in their research (Cherryholmes, 1994).
- There is a concerted and thoughtful emphasis on consequence as the defining characteristic of the pragmatic stance (Greene and Caracelli, 2003).
- In pragmatism, the essential criteria for making design decisions are practical, contextually responsive and consequential. Practical implies a basis in one's experience of what will and will not work. Contextually responsive involves understanding the demands, opportunities and constraints of the situation in which the inquiry will take place. Consequential means that the truth of a statement consists of its practical consequences, particularly the statement's agreement with subsequent experience (Greene and Caracelli, 2003).

Thus, pragmatism spans the divide between different worldviews, different assumptions and diverse methods, opening the door to combining different sorts of information aggregation and analysis appropriate to a case study approach (Creswell, 2013). Some academic investigations in information studies that have adopted the pragmatic paradigm include Almualla (2012), in her study to examine the pedagogy for teaching computer ethics in universities in Bahrain. Supavai (2014) equally used the pragmatic paradigm in a study to measure moral reasoning and psychometric property of cyberethics scale in Boston.

4.4 Research Design

Research design refers to procedures for research that span the decisions from broad assumptions to detailed methods of data collection and analysis (Creswell 2013). A convergent mixed method design was used in this study. This design allows quantitative and qualitative data to be collected and analysed separately, while findings from the two research approaches can be compared to have a clearer understanding of the research problem (Creswell and Plano Clark 2011; Creswell 2013, 2015). This study will adopt a concurrent parallel design by combining the strength of survey design within a case study research approach. The strategy and blending of the two designs provided a deeper understanding of the nature of the phenomenon under investigation because their utility is built on the strength of both quantitative and qualitative data collection methods (Creswell, 2008; Saunders, Lewis and Thornhill, 2012).

4.4.1 Case studies

According to Yin (2003), a case study approach is appropriate when researching contemporary, real-life situations where the phenomenon of interest is enmeshed within the setting of the work. Case studies have the capacity to provide purposive, situational, interrelated descriptions of phenomena, connecting practical and complex issues to theoretical abstractions (Stake, 2000). Case studies commonly explore, describe and/or explain the case or phenomenon of interest and generate context-constituted knowledge about real-life events (Yin, 2003).

A case study is usually organised around a small number of research questions. The issues explored are complex, situated and problematic relationships. They attract attention to ordinary experience, but also to the language and understandings of disciplinary knowledge (Stake, 2000). A case study pays attention to and abides by the personal identity and singular nature of participants and their

social world (Clarke & Reed, 2006). Therefore, a case study provides an appropriate framework to research and explain the concept of cyberethics behaviour as experienced by undergraduate students from two distinct settings. For the present study, the interests are not only in undergraduate students' behaviour per se, but also in what a study of their experiences might reveal about the phenomenon of cyberethics. as it relates to the students' use of cyber technology. This clearly suggested the use of a multi-site instrumental case study. The temporal and geographically defined single unit of analysis was current undergraduate students from two university sites. The phenomenon or case of interest was their cyberethics behaviour.

4.4.2 Survey Research

Bryman (2012) defines a survey research as a cross-sectional design in relation to which data is collected predominantly by a self-completed questionnaire or by structured interviews on one or more cases and at a single point in time, in order to collect a body of quantitative or quantifiable data in connection with two or more variables, which are then examined to detect patterns of relationship between them. According to Cohen, Manion and Morrison (2011), survey design is used to gather data at a time with the intention of describing the nature of existing conditions or to identify standards against which existing conditions can be compared or determined from the relationships that exist between specific events. The goal of survey research is to derive comparable data across subsets of the chosen sample so that similarities and differences can be found (Cooper and Schindler, 2008). It is usually applied to a sample of a population and involves acquiring information on one or more groups of people, accurate portrayal or account of their characteristics in real-life situations, their opinions, attitudes and experiences, among other information. This is realised by asking questions and tabulating their answers in order to discover meaning, describe what exists and obtain information on the status of the phenomena (Leedy and Ormrod, 2014; Creswell, 2014).

Saunders, Lewis and Thornhill (2009) describe the survey design as being concerned with the description of phenomena and documentation of aspects of a situation. It is important in answering questions such as who, what, where and how much. The choice of survey research design in this study was largely informed by the adopted research approach, the nature of data that was to be collected, the sampling design and the methods of analysing the collected data. Researchers have noted two types of survey design as either cross-sectional survey design or longitudinal survey

design (Creswell, 2012; Gray, 2014:266). This study will adopt a cross sectional survey to enable the description of cyberethics behaviour and to determine the factors that influence undergraduate students' cyberethics attitude and afford deeper understanding of the challenges to students cyber practices within the studied institutions (Majumdar, 2005). Further, the survey research design is often used to collect data using two basic forms of data collection: questionnaire and interview. As such, the researcher considers the forms and weighs the pros and cons of each (Bryman, 2012). By using this design, it was possible to scan and investigate a wide range of issues from a population sample and generalise them to the target population.

In line with the objectives of this study of cyberethical behaviour of undergraduate students, the survey research become germane to this study because it would be a hard task to collect data from the totality of the student population who would have limited time to attend to the demands of a survey instrument. The economy of time and cost are also paramount factors in the choice of survey research for this study, as the survey research will enable adequate access to the major research respondents. Numerous studies have used the survey research in their investigations. For instance, studies done by Johnson (2017) on how attitude, subjective norm and perceived behavioural control affect information security behaviour intention.

4.5 Population of the Study

The term population refers to the total group from or about which certain information is required to be ascertained (Banerjee and Chaudhury, 2010). A research population consists of individuals or elements with similar characteristics. It also comprises all the members of a group who are of interest to the researcher (Fraenkel and Wallen, 2009). The population in this study refers to the members of a group of people defined as respondents to whom the researcher measurements refer by reported results, findings and inferences (Babbie, 2010; Babbie and Rubin, 2010). The sum of these elements form the study population, which in this study includes all the undergraduate students and staff members in the ITS/ICTREC of the two selected institutions in South Africa and Nigeria. For the study, the total population of undergraduate students was three hundred and eighty undergraduate students, while for the staff it was fourteen information technology professionals.

4.5.1 Accessible population

The accessible population is the fraction of the sum total research population which the researcher

can access due to reasons of availability and convenience, and the population to which the conclusions for generalisation are applied. This population is a subset of the target population. However, it is from the identified accessible population that the researcher draws the samples for the study. Based on the foregoing, the accessible population for this study was the undergraduate students and staff members in the information technology sections of the two universities in South Africa and Nigeria. These were fifteen thousand, eight hundred and forty-seven in the Federal University of Agriculture, Abeokuta, Nigeria, and fifteen thousand, five hundred and forty-two at the University of Zululand, South Africa. The total number of accessible population in the two institutions was thirty-one thousand, three hundred and eighty-nine.

4.6 Sampling Procedures and Methods

Sampling refers to investigating a part to glean information about the whole (Corbetta, 2003). It entails the process of selecting some elements of the population that is used to provide data in order to draw conclusions about the entire population (Cooper and Schindler, 2008). The typology of sampling procedures or strategies in mixed methods have been classified into time orientation and the relationship of the quantitative and qualitative samples (Collins, Onwuegbuzie and Jiao, 2007:276): that is, whether the qualitative and quantitative phases occur sequentially or concurrently. Sequential sampling procedure includes the qualitative stage coming first and then the quantitative afterwards, while for the concurrent sampling design, the data gathered from the sample selected for one phase do not inform the data gathered from the sample selected for the other phase. They could, however, be integrated at the data interpretation stage of the study. In most studies, it would be impossible, time consuming and expensive to conduct an investigation on the whole population of study and as such the choice of a sample offers the researcher a workable solution in terms of cost and time (Majumdar, 2005). A sampling technique was therefore applied to obtain a representative sample from faculties and colleges in the studied universities. For this study, the concurrent multilevel sampling design was adopted in this study, where to achieve an in-depth understanding of the factors influencing cyberethics behaviour of undergraduate students, and to ensure a high degree of credibility of the collected data, the study adopted concurrent multilevel sampling design from different levels of investigation (i.e. different populations: students and ITS/ ICTREC staffs of the two universities). The quantitative phase involves sampling of undergraduate students while the qualitative phase was designed for the staffs in the information technology sections in the two universities. Both probability and non-probability

sampling techniques were used in this study. The probability sampling technique refers to the controlled and randomised procedure that ensures that each member in a population is given a known non-zero chance of selection (Bloomberg, Cooper and Schindler, 2011). In probability sampling, elements in a population are chosen randomly and have a known probability of selection. Ritchie and Lewis (2013) agreed that probability sampling draws participants randomly from a wider population and has high representation. According to Cohen, Manion and Morrison (2011), the probability sampling technique has less risk of bias and allows two-tailed tests in the statistical analysis of the quantitative data. Probability sampling techniques can be simple random, systematic, stratified or cluster.

Cooper and Schindler (2008) described the non-probability sampling technique as an arbitrary and subjective procedure whereby each member of the population does not have a known non-zero chance of being selected. It is also non-representative (Cohen, Manion and Morrison, 2011). In non-probability sampling, units are deliberately selected to reflect features within a sampled population and hence the characteristics of the population are used as the basis for selection (Ritchie and Lewis, 2012). Cohen, Manion and Morrison (2011) regarded non-probability sampling as good in piloting a questionnaire. Examples of non-probability sampling techniques are convenience, quota, purposive/judgmental, dimensional and snowball sampling.

On the question of sampling to research design, Tashakkori and Teddlie (2003) observed that pure experimental studies use probability sampling technique while qualitative researchers usually apply purposive or non-probability sampling techniques. They, however, add that no research tradition can claim a specific sampling technique and that research can vary or apply a mix of variety of sampling techniques. For the final field work, this study adopted probability sampling to select undergraduate students, while non-probability sampling was used to select key

individuals at the Information Technology Section (ITS) of the universities. A more detailed account of the probability and non-probability sampling techniques used in this study is given below.

4.6.1 Stratified sampling technique

This study employed a stratified sampling method. This method was used because it can provide richness and accuracy of data from respondents of different strata. This method is considered practical to this study because it is aimed at obtaining differentiated information from various

stratums but with certain limitations such as time and cost (Cavana, Delahaye and Sekaran, 2001; Sekaran, 2010). Importantly, this sampling technique can help ensure homogeneity within a group (i.e. undergraduate students in a particular faculty or college), and heterogeneity across groups: i.e. different faculties and colleges (Cavana, Delahaye and Sekaran, 2001; 2007). In the sampling process, respondents were first divided into mutually exclusive groups or stratums: i.e. branches. On this basis, it was assumed that there is heterogeneity across groups (i.e. faculties and colleges) but there was homogeneity within each group (i.e. undergraduate students). Since the reported numbers of samples (i.e. undergraduates) for each faculty/college were not equal, disproportionate stratified sampling was employed.

A stratified sampling method was adopted due to the diversity of faculties and collegiate mandate and the likely differences in the structure of education (special and semi-comprehensive educational structure) in the two universities. The essence is to obtain more insight into the perception of students' cyberethics behaviour.

4.6.2 Purposive/judgmental sampling

Purposive/judgmental sampling is a non-probability sampling technique whereby a researcher chooses participants judgmentally for their unique characteristics, experiences, attitudes or perceptions (Cooper and Schindler, 2008). The technique is commonly used in business, marketing, social psychology and political research. The weakness associated with this technique is the lack of assurance that a sample is representative of the population. It is, however, less costly and one spends less time in the field. It is termed appropriate in exploratory studies: for example, trying a new product (Cooper and Schindler, 2008). Saunders, Lewis and Thornhill (2009) attribute the strength of the purposive sampling technique to its ability to enable a researcher select cases that are most suited to answer the research questions. One can select members of the population who are deemed to be better placed in providing the needed information and leave out the ones who may not have the required information (Cohen, Manion and Morrison, 2011).

The purposive sampling technique was used in this study, first, to select the two universities in Nigeria and South Africa, based on the ease of access to data collection and the fact that the researcher worked in the Nigerian university and was, at the same time, a student at the South African university. The second consideration for the purposive sample in the study was the selection of information-rich university staff members who oversaw the information technology

units of the two universities under study. The participants for the follow-up interview were purposively selected due to their unique experiences and perceptions on the phenomena that were being investigated.

The justification for using purposive sampling to select the universities was anchored on the suggestion of Neuman and Robson (2014) that using purposive sampling in an enquiry allows the scholar to have easy access to the study participants and quick access to information. Gikenye (2012) supported the use of purposive sampling to select contexts or places that suit the information accessibility of a researcher. Hence, the University of Zululand, KwaDlangezwa, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria, were purposively selected for the study.

4.6.3 Systematic random sampling

Creswell (2014) and Cooper and Schindler (2008) describe systematic sampling as a probability sampling technique in which one chooses every *n*th individual, case, element or subject in a population or sampling frame until one reaches the desired sample size. In this sampling technique, the subjects, cases or individuals may not have to be numbered (Bryman, 2012). This technique was specifically applied to randomly select undergraduate student participants from the stratum. Undergraduate university students in year one to three were included in the study. They were randomly selected from the faculties, after obtaining permission from the relevant lecturers to visit the computer labs during contact hours or sessions for the distribution of the research instruments. The computer labs were included because computer and internet training courses were compulsory for all students in the two semesters of 2017 at Unizulu. Moreover, the computer lab serves as an alternative point of call for those students who do not have personal laptops, and who might need to use the Internet and the institution's network for learning, training, social and educational purposes (Jamil and Shah, 2014).

The ITS staff were requested to provide a list of all the general computer labs, facilitators of those computer labs, as well as the timetables for all the modules, where a large pool of these participants could be reached. Modules were randomly selected from the timetable provided and the course facilitators were contacted. Upon acceptance by the course facilitators, who first introduced the fieldwork stakeholders (researcher and assistances) and the nature of the study, the researcher and his team then distributed the questionnaire and stood by to address problems or uncertainties that

the participants may encounter while responding to the study instrument. After the group of participants were briefed on the purpose of the research, and had consented to participate, hard copies of the questionnaire were then handed out to every tenth student. As Cooper and Schindler (2008) and Saunders, Lewis and Thornhill (2009) noted, this technique is suitable in geographically dispersed populations and it is easy to explain and train research assistants. The only disadvantage associated with the systematic sampling technique is periodicity and monotonic trends in the population (Cooper and Schindler, 2008). To overcome these weaknesses in this study, the researcher exercised constant vigilance by changing the random start number in each cluster computer lab and by strict observance of the random interval across the entire pool of students or respondents.

4.6.4 Sample size

Saunders, Lewis and Thornhill (2009) describe sample size as a group that is a subset of the population of interest. Gagne and Hancock (2006) contended that determining sample size is challenging but also important so as to provide a basis for the measurement model and to increase construct validity and reliability in a theory-driven study. There are several ways of determining the sample size of a given population. For instance, there is the use of formulas (Krejcie and Morgan, 1970). Data collected from samples can also be used to draw inferences about a population without examining all its members; hence the economy of time, effort and money. The following constitutes the sample size of this study.

$$\frac{(\quad)}{[\quad]}$$

If the total number of undergraduate students at the University of Zululand 2016/2017 Unizulu, (Fact & Figure, 2017) = 15542, and the total number of undergraduate students at the Federal University of Agriculture, Abeokuta, 2017 = 15847, then

$$N = \text{is the total population of the two universities} = 15,542 + 15,847 = 31,389$$

A confidence interval of 95% is chosen, L= is the error percentage 5% and confidence interval of 0.5, and from the z-table, the confidence interval 95% coincides at 1.96.

When the above values are substituted into the formula, we have:

$$\frac{()}{[]}$$

$$n = 380$$

Hence, the sample size for this research is 380 participants.

4.6.5 Sampling frame

A sampling frame is the sample group that is drawn from the target population and it needs to be representative of this larger population. The demographic profile of the sampling frame, for example in terms of gender, race, age, educational level and socio-economic status, should ideally mirror the profile of the target population. It is a list of all those within a population of study and this may include individuals, households or institutions (Babbie, 2010). Facts and figures containing the enrolment list of undergraduate students at the University of Zululand (15,542) and the registry section of the Federal University of Agriculture, Abeokuta (15,842), were obtained to determine the sampling frame for this study. The obtained lists were hence computed to determine the units that were included in this study. Sampling frame in this study includes as many undergraduate students as are found in the target population in the studied universities in South Africa and Nigeria. The demographic profile of the sampling frame, for example in terms of gender, age, faculty, institution, educational level, should ideally mirror the profile of the target population. However, consideration was also based on the participants' knowledge or their informed advocacy on the phenomenon of cybertechnology behaviour. Specifically, participants were included in the sampling frame for this study based on the following criteria: young adults (typically between the ages of 18-24) having been using cybertechnology (internet, intranet, laptop, smartphone, amongst others) on the university network, digital natives who grew up with (Butterfield, and Crews, 2012). Another consideration for the sampling frame was the inclusion of staff members with unique experience and perception on the phenomenon of cybertechnology

behaviour of undergraduate students. The researcher conducted an interview with the ITS/ICTREC managers of the two universities. Their choice was informed by their experience, as they were deemed better placed to provide needed information on the cyberethics behaviour of the undergraduate students on the universities' cyberspace and network. The two senior staff members (network managers and staff in charge of the university network) were all regarded as important respondents because they make decisions, oversee the implementation of the various strategies regarding cybertechnology activities in the universities, and are in charge of policy issues affecting cybertechnology use and the resultant behaviour from undergraduate students. Therefore, information about the use of cybertechnology by undergraduate students collected from this category of respondents was crucial to this study.

To confirm the estimated sample size, the sample size calculator, following the approach of Hoyle, Harris and Judd (2002), was also utilised to get the sample size from each cluster:

University of Zululand $n = (15,542/31389) * 380 = 188$ students

Faculty of Arts $(3,666/15,542) * 188 = 45$

Faculty of Commerce, Administration and Law $(3,904/15,542) * 188 = 47$

Faculty of Education $(4,718/15,542) * 188 = 57$

Faculty of Science and Agriculture $(3,199/15,542) * 188 = 39$

FUNAAB $n = (15,847/31389) * 380 = 192$ students

College of Management Sciences $(2,512/15,847) * 192 = 30$

College of Environmental Resources Management $(1,157/15,847) * 192 = 18$

College of Animal Science and Livestock Production $(1,210/15,847) * 192 = 14$

College of Agricultural Management and Rural Development $(2,423/15,847) * 192 = 29$

College of Plant Science and Crop Production $(1,643/15,847) * 192 = 20$

College of Biological Sciences $(1,525/15,847) * 192 = 18$

College of Food Science and Human Ecology $(1,625/15,847) * 192 = 19$

College of Veterinary Medicine $(552/15,847) * 192 = 6$

College of Engineering $(900/15,847) * 192 = 11$

College of Physical Science $(2,300/15,847) * 192 = 27$

Table 4.1: Sampling Frame for Selection of Respondents

FACULTIES/UNIVERSITIES	STUDENT	SAMPLE	PERCENTAGE
------------------------	---------	--------	------------

POPULATION SIZE			
Faculty of Arts	3666	45	1.2%
Faculty of Commerce, Administration and Law	3904	47	1.2%
Faculty of Education	4718	57	1.2%
Faculty of Science and Agriculture	3199	39	1.2%
Total in University of Zululand	15542	188	1.2%
College of Management Sciences	2512	30	1.2%
College of Environmental Resources Management	1157	18	1.2%
College of Animal Science and Livestock Production	1210	14	1.2%
College of Agricultural Management and Rural Development	2423	29	1.2%
College of Plant Science and Crop Production	1643	20	1.2%
College of Biological Sciences	1525	18	1.2%
College of Food Science and Human Ecology	1625	19	1.2%
College of Veterinary Medicine	552	6	1.2%
College of Engineering	900	11	1.2%
College of Physical Science	2300	27	1.2%
Total in Federal University of Agriculture Abeokuta	15847	192	1.2%
Overall Population	31389	380	1.2%

The overall total number of the study population in the universities was 31,389. The study aimed at a minimum sample size of 380, at a confidence level of 95% and a confidence interval of 5% (Krejcie and Morgan, 1970). However, the researcher felt the need to even up the number to 400.

The reason was to enhance a large response rate since students' attitudes, when it comes to responding to survey research, have been characterised as poor (Fosnacht, Sarraf, Howe and Peck, 2017).

4.7 Data Collection

This section details the methods that were used to collect data. Research data can be collected using various instruments, depending on the nature and type of information required. Data collection is the process of collecting data for a study that will be analysed and interpreted with the aid of questionnaires and structured interviews. The choice of appropriate participants for a study is their selection based on experience and expert opinions (Gray, 2014). This in turn informs the survey output and unit of analysis. The major entities being analysed in this study were individual undergraduate students and ITS staff members. For this purpose, data was obtained from university students in various faculties and colleges. Subsequently, the results from the survey questionnaire were then to elicit further data from ICT professionals in the information technology section of the universities.

4.7.1 Questionnaire

The questionnaire is an instrument for the elicitation of data delivered to and completed with the aid of a participant of a study. Here, the participant is requested to respond to a set of questions in a predetermined manner. The questions can be either close-ended or open-ended (Saunders, Lewis and Thornhill, 2009). The questionnaire allows more generalised results that are less inclined by the personal subtleties of the individual interviewee and the individual impressions of the interviewer (Bazerman, 2003). The questionnaire instrument was considered appropriate due to its capacity to cover large samples. It was also considered cost-effective to administer, barring the influence of the researcher (Bryman, 2012). Moreover, the use of a questionnaire improves standardisation of information given since each respondent gets the same questionnaire in the same format.

The major instrument of data collection for this study was the questionnaire. The copies of the questionnaire were administered to the selected undergraduate students in their various faculties and colleges in the two universities, one in Nigeria and the other in South Africa. The questionnaire was structured to ensure that all the variables in the study were addressed.

The questionnaire was adopted in this study to understand the participants' perceptions of

cyberethics behaviour. Equally assessed were the other factors that influence cyberethics behaviour of undergraduate students, as well as the challenges to cyberethics compliance in the studied institutions. This study used the Likert scale. The Likert scale is the most frequently used method to measure attitudes and behaviours in institutional research (Sekeran and Bougie, 2010). The forced scale was chosen for this study because cyberethics behaviour is an ethical issue, as it deals with rightness or wrongness of cyber behaviour and, as such, this measure allows the respondents to choose for or against cyberethical intention or the behaviour under investigation. The use of the Likert scale was preferred in this study to facilitate the collection of data on a variety of studied phenomena and constructs. It also enabled exploration, measurement and obtainment of different degrees of responses and the determination of the intensity of different aspects of a variable (Agarwal, Xu & Poo, 2011).

The weaknesses associated with the use of questionnaires include the inability to probe or ask further questions, the risk of unanswered questions, difficulty in answering some questions, lack of seriousness when answering the questions and low response rate (Bryman, 2012). Considerable efforts were made to overcome these weaknesses by ensuring that the questions were clear and unambiguous. The instrument had few open-ended questions while the instructions were simple and very clear. The questionnaire had a good cover letter, aimed at motivating the respondents by highlighting the purpose of the study. Consequently, the questionnaire was administered to these target groups in the universities with the help of research assistants. The research assistants were guided on how to clarify queries arising from the questionnaire. To develop the questionnaire, the existing literature and published studies on cybertechnology ethics, cyberethics and the scale developed by Chatterjee, Sarker and Valacich (2015) was modified to fit this current study. The design of the questionnaire consisted of simple close-ended and very few open-ended questions. Many close-ended questions were on five-points Likert-type scales.

The questionnaire was organised into two sections. The first section was designed to capture the biodata and other particulars of the respondent, in this case their college or faculty as the case maybe, gender, age, current level of study, cybertechnology skills and cybertechnology experience. The questionnaire was structured to first elicit personal information before asking in-depth questions as a way of calming the respondents and encouraging them to respond to subsequent questions (Cargan, 2007).

The second section of the questionnaire presents the respondents with questions grouped according to the research objectives. The measurement tools for each category consisted of both close-ended and open-ended questions. The close-ended questions were structured on 5 Likert scale points. The five points represented their level of agreement or disagreement with the statement presented.

Table 4.1 below shows the links between questionnaire items on the appendix and their various links to the study research objectives.

Table 4.2: Linkages of Questions in the Questionnaire with Research Objectives

Objective of study	Items in data collection instrument that are linked to study research objectives
1. Is there relationship between students' demographic variables and their cyberethics behaviour in the University of Zululand and the Federal University of Agriculture?	Appendix 5: Question 1, 2, 3, 4, 5, 6
2. What is the level of awareness of cyberethical behaviour among students in the two universities in Nigeria and South Africa?	Appendix 5: Questions 7a (29 items), 7c Appendix 6: 1a and 1b and 3, 4, 5
3. What are the types of cyberethics behaviour exhibited by undergraduate students in the two universities?	Appendix 5: Question 8 (17 items) Appendix 6: Question 2, 6
5. Is there influence of the theory of planned behaviour (TPB) on the behavioural intention of undergraduate students in the universities in Nigeria and South Africa?	Appendix 5: Questions 9a, 9b, 9c, 9d,
5. What are the challenges in efforts by undergraduate students to act ethically correct in cyberspace at the two universities?	Appendix 5: Question 10 (21 items) Appendix 6: Question 6b, 6c,

6. Is there any impact of cyberethics policy on compliance with ethical conduct in cyberspace in the two institutions?	Appendix 6: Questions 9, 10, 11, 12, 13, 14
--	---

4.7.2. Interview

Semi-structured personal interviews were conducted to gather relevant data from purposively selected key staff in the information technology sections of the studied universities. Consistent with the advantages described by Kothari (2004), and Cooper and Schindler (2008), this technique was deemed appropriate for this study since it allowed the changing of wordings and explanations for questions, which seemed inappropriate with a particular respondent. Interviews were also seen to provide greater flexibility in varying attention and time spent with a given respondent of the study. To develop the interview questions (see appendix 6), the existing literature and published works on cyberethics, cybertechnology ethics and other related terms were consulted. Likewise, the study also adapted tools from previous related studies such as by Cilliers (2017), Jamil, Hussain and Tariq (2013).

4.7.3 Pilot study

Piloting of instrument for this study was carried out at the Nimbe Adedipe Library of the Federal University of Agriculture, Abeokuta, Nigeria. Using convenient sampling, 157 completed questionnaires were collected from the 200 pilot questionnaires distributed, representing about 66% response rate. The high response rate could be attributed to the administration of the questionnaire during the 24-hour library service period, towards the year 2016 examinations.

Changes indicated by the validation panel and the field test were incorporated when the instrument was developed. The obtained results were used to modify and improve the questionnaire before they were administered in the selected universities in Nigeria and South Africa.

4.8 Validity and Reliability of Instruments

Validity is an instrument used to find the degree to which the instrument measures what it ought to measure (Gray, 2014:307). It is the ability of the researcher to draw meaningful and justifiable inferences from scores about a sample population (Creswell, 2005). Ellis and Levy (2009) identified the following as means of achieving validity in research: internal validity, face validity,

criterion related validity, construct validity, content validity, statistical conclusion validity and external validity. The first draft of the research instrument was given to the supervisor, students and colleagues, whose views and comments were then used to modify the instrument for the data collection. Table 4.3 shows the results of the reliability test of the research instrument.

Table 4.3: Reliability Test of the Research Instrument

Reliability Statistics			
Sections	Research Question	Cronbach's Alpha	Number of Items
A	Demographic Characteristics of Respondents	0.341	7
B1 (Q7a).	Awareness and Types of Cyberethical Behaviour (List of Cyberethical Behaviour)	0.953	30
B1 (Q7b)	Cybertechnologies	0. .894	03
B1 (Q7d)	Elements of Cybertechnology Behaviour Awareness	0.818	12
B2 (Q8)	Constitutes of Cyberethical Behaviour	0.883	17
B3 (Q9a)	Influence of Attitude, Subjective Norm and Perceived Behavioural Control on Cyberethical Behaviour Intention (Aattitude toward Cybertechnology Behaviour)	0.906	08
B3 (Q9b)	Subjective Norm	0.856	08
B3 (Q9c)	Perceived Behavioural Control	0.868	08
B3 (Q9d)	Influence of Behavioural Intention on Cybertechnology Behaviour	0.822	11
B4 (Q10)	Challenges of Cyberethical Behaviour on University Campus	0.940	21
	Over all	0.958	125

Reliability is defined as the consistency with which a measuring instrument yields certain results when the entity being measured has not changed (Leedy and Ormrod, 2011). Gray (2014) listed the following as ways of measuring reliability in research: stability, equivalence, internal reliability, inter-judge reliability. Test re-test method was used during the pilot study to establish the reliability of the instrument. The study used the Cronbach's alpha to determine the internal co-efficiency for the whole of the questionnaire. Cronbach's alpha values of 0.70 and above are

typically employed, as a rule of thumb, to denote a good level of internal reliability. Values between 0.50 and 0.69 denote an acceptable level of reliability and values below 0.50 denote poor and unacceptable levels of reliability.

The overall reliability of the entire scale, comprising 125 items, returned a Cronbach's Alpha Co-efficient of $r = 0.958$. This implies that the scale is highly reliable to measure the constructs which it was designed to measure and can as well be recommended for future use by any researcher conducting a relevant research or who wishes to continue from where this study stops. The reliability of each of the items featured in the scale returned reliability co-efficient of above 0.90. This implies as well that each of the items in the scale is significant, relevant and adequate to capture data on the subject for which they were designed and developed. Furthermore, the reliability of the sub-scale of the instrument as revealed above returned the following: Awareness of cyberethical behaviour, $r = 0.953$; types of cyberethical behaviour, $r = 0.883$; attitude towards cyberethical behaviour, $r = 0.906$; subjective norms, $r = 0.856$; perceived behavioural control, $r = 0.868$; cyberethical intention, $r = 0.822$; and challenges towards students behaviour ethically, $r = 0.940$.

The reliability factor for the questionnaire was 0.925, which denotes an acceptable level of reliability (Bryman, 2012).

4.9 Data Analysis

Data analysis consists of many interconnected processes that help to summarise gathered data and analysing them in such a manner that provides responses to the research questions (Kothari, 2004). Due to the nature of the data collected in this study and in line with the post-positivist paradigm, a mixed method data analysis was required. This involved a combination of qualitative and quantitative data analysis methods.

Descriptive statistics and Statistical Package for the Social Sciences (SPSS) version 23 were used to analyse the quantitative data collected using the structured questionnaire, since it allowed for easy manipulation of statistical data analysis and interpretation of quantitative study findings (Pallant, 2013). Before analysing the raw data, each completed questionnaire was evaluated to check for missing data, ambiguity and errors, after which the questionnaire responses were coded and keyed in using the SPSS software. Regression analysis in SPSS has five methods on how variables are handled in the model. These include: stepwise method, enter method, backward

method, analysing method and remove method. This study employed the enter method to evaluate how a group of related variables regressed on given dependent variables. The stepwise was also deployed to determine the most suitable determinants for a given regression model (Bryman, 2012). The results generated from the quantitative data analysis were presented visually using frequency counts and tables.

Qualitative data gathered using semi-structured interview schedule were analysed using thematic content analysis. Leedy and Ormrod (2010) stated that qualitative researchers construct interpretive narrative from their data and try to capture the complexity of the phenomenon under study. Qualitative researchers thus use a more personal, literary style, and often include the participant's own language. Robson (2011) agreed with the views of Leedy and Ormrod (2010) and further stated that qualitative analysis remains much closer to codified common sense than to the complexities of statistical analysis of quantitative data. Therefore, qualitative data analysis is based on assumptions and the use of interpretive (theoretical) frameworks to ensure a final written report or presentation that includes the voices of participants and the reflexivity of the researcher. Semi-structured interviews allow for thematic analysis of the qualitative data (Srivastava and Thomson, 2009). It also involves gathering and analysing the contents of the text to make sense out of it (Newman, 2006). This helps to reduce data and makes interpretation easier. The recorded interviews were transcribed, after which the transcripts and notes were prepared to show the relationship that exist between the variables of the study. Table 4.2 shows the relationships between the study research questions, approach of data collection, sources of data and methods of data analysis.

Table 4.4: Research Questions, Sources of Data and Data Analysis

No.	RQ	Theoretical framework	Research paradigm	Research Design	Data sources	Respondent	Data analysis
1.	What is the influence of individual	Individual characteristics	Positivism	Survey	Questionnaire	Students	Descriptive statistics,

	characteristics on cyberethics behaviour						Chi square
2.	What is the level of awareness of cyberethics behaviour?	Awareness	Mixed	Survey+ case study	Questionnaire and interview	Students, Director of ITS and staff	Descriptive statistics, Chi square
3.	What are the types of cyberethics behavior of Undergraduate students?	Awareness	Mixed	Survey + case study	Questionnaire and Interview	Students, Director of ITS and staff	Descriptive statistics, Chi Square
4.	Influence of TPB on cyberethics behaviour	Attitude, Subjective norm, Perceived behavioural control	Positivism	Survey	Questionnaire	Students	Pearson Product moment Correlation Coefficient Regression analysis
5.	What are the challenges to cyberethics?		Mixed	Survey+ case study	Questionnaire and interview	Students, director of ITS and staff	Likert scale, descriptive statistics
6.	What is the influence of cyberethics policy on the promotion of ethical conduct in cyberspace?	Policy	Intepretivism	Case study	Document analysis and interview	Director of ITS/ICTREC and staff	Thematic analysis

4.10 Ethical Consideration

Given the importance of ethics to this study and the field of information system research, the University of Zululand ethical guidelines and policies were regarded prior to data collection. All elements of this investigation were guided by the ethical review protocol and guidelines issued by the committee. As a result, there were minimal risks involved in this study. Participation in the study was voluntary, and participants were provided with the opportunity to withdraw at any time.

Participants were only included in the study after they had indicated their willingness to

participate in the study through the completion and signing of an informed consent (Appendix 3) that outlined the nature of the research and the conditions of their participation. Participants were further informed that if they decided to withdraw from participating in the study, all the data pertaining to them would be destroyed immediately and not be used.

The collection of data for the study was done solely, and in some occasions by research assistants from other stakeholders. The perceived benefits for participating in the study include the opportunity for the participants to share their experiences and knowledge and contribute to relevant literature on the study. Participants had the opportunity to have someone listen to their views carefully and to engage in the process of reflecting on their experiences. This study has also complied with the ethical guidelines of the Federal University of Agriculture, Abeokuta, Nigeria.

4.11 Methodological Challenges Encountered during the Field Investigation

Data collection and the research field work normally consider budgetary cost, data management, data quality, duration and access to respondents in the locations of study. Some of these aspects could not be clearly revealed through the initial pilot study. For instance, managing appointments with the ICT staff for the interview session at the studied universities was a herculean task. The staff members were initially reluctant to grant the interview on ethical issues involving the usage of cyber technology on the university campus. Getting them to also settle down for interviews was difficult because their attention was often distracted. While it was anticipated that the respondents at the Nigerian university involved in the study would be easily accessible, getting the institution to approve the administration of the instrument to the undergraduate students was difficult, as the institution was in the middle of examinations, which made getting access to, and convincing the major respondents to respond to the research instrument, challenging, but for the assistance of a few course representatives and academic staff members. It was equally challenging to get the students at the South African university to respond to the instrument diligently.

4.12 Summary

This chapter presented the research methodology that has driven this study titled “Cyberethical Behaviour of Undergraduate Students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria.” The chapter discussed the research paradigm,

research methods, research design, population of study, sampling procedures, data collection procedures, data analysis, validity and reliability and finally ethical considerations.

The study population included two participating universities as mentioned in the title. Of these two universities, the study fieldwork was conducted at the University of Zululand while the pilot study was conducted at the Federal University of Agriculture, Abeokuta, Nigeria. Time and cost were major constraints that informed this methodological decision. Participants in the eventual field of study were randomly selected and considered for inclusion based on their knowledge and exposure to the phenomenon under investigation. The sampling method adopted for the qualitative aspect of the study was purposive sampling. Validity and reliability of the research instruments were measured using the Cronbach's alpha with acceptable values. Data were collected through the use of survey instrument and interview schedules. Quantitative data were analysed with the aid of SPSS to generate descriptive and inferential statistics. The qualitative data was also analysed thematically and presented using narration. The study ensures compliance with the University of Zululand-issued ethical guidance protocol.

The next chapter presents the analyses and interpretations of survey data.

CHAPTER FIVE

PRESENTATION AND INTERPRETATION OF SURVEY

QUESTIONNAIRE FINDINGS

5.1 Introduction

The previous chapter discussed the research methodology. This chapter presents the results of data from the fieldwork that was collected from undergraduate students of the universities under investigation. The study aimed to investigate the cyberethics behaviour of undergraduate students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria, with a view to providing solutions to cyberethical challenges in the studied universities. This presentation of the analysis and findings is sequential, guided by the order of the research objectives and instruments, in order to make logical interpretations.

From the two universities, students' enrolments, based on faculties and colleges, were sampled as follows: University of Zululand: Faculty of Arts, Faculty of Education, Faculty of Commerce Administration and Law, Faculty of Science and Agriculture; while at the Federal University of Agriculture, Abeokuta, the following colleges were included: College of Management Sciences, College of Environmental Resources Management, College of Animal Science and Livestock Production, College of Agricultural Management and Rural Development, College of Plant Science and Crop Production, College of Biological Sciences, College of Food Science and Human Ecology, College of Veterinary Medicine, College of Engineering, and College of Physical Science. Although these faculties and colleges may seem incomparable in terms of discipline, the university undergraduate students were generally targeted for their quick learning and interest in the use of information technology (cybertechnology) for making informed decisions while surfing the Internet for information on social or educational needs. A combination of quantitative and qualitative approaches was used in the data analysis. Data collected from the quantitative instrument were coded and analysed using descriptive statistics and the Statistical Packages for Social Sciences (SPSS), version 25.0. Findings from the survey are thus presented in tables with frequencies and percentages. Data from the interview schedule were also presented using thematic analysis.

The chapter is presented and organised along the themes of the research questions and key variables or constructs of the Theory of Planned Behaviour as applied in the study.

Overall, 450 undergraduate students were invited to participate in the survey, out of which 380 subjects completed and returned the questionnaire, giving a response rate of 84.4%. From the expected 16 members of staff of ICTREC and ITS, who are the key informants on the phenomenon under study, 14 were interviewed, showing a response rate of 88%. Studies have shown that 50 to 70% response rates are very good for analysis and reporting of survey findings (Ayooluwa, 2016; Hardigan, Popovici and Carvajal, 2016; Edmonds and Kennedy, 2016). Hence, the response rates for both survey (84.4%) and the interviewers (88%) for this study were considered statistically adequate for this study.

Five research assistants, with support from course representatives, hostel committee members and faculty members, provided useful assistance in the distribution and return of the research instrument. The descriptive and inferential statistics from the results are presented below.

5.2 General Background Information of Respondents

The frequency results on all background variables were first summarised and presented in one table. Results on elements of various background constructs are presented in descending order to facilitate clarity.

5.2.1 Distribution of participants by gender

Participants in this study were asked to indicate their gender on the questionnaire. The distribution of respondents by gender in Table 5.1 reveals that 188 respondents (44.7%) from the University of Zululand were male, 44.7% were female, while 1.6% were non-conforming. Similarly, the results also showed that of the 192 respondents from FUNAAB, 58.3% of students were male while 41.7% were female. This implies that there were more female respondents in UNIZULU while there were more male respondents from FUNAAB. This could also be attributed to the fact that, worldwide, males are more inclined towards the sciences than the arts/humanities, compared to females.

Table 5.1: Gender Representation of Students

Gender	South Africa (=188)		Nigeria (=192)		Total(*N=380)	
	No of respondents	Percentage	No of respondents	Percentage	No of respondents	Percentage
Male	84	44.7	112	58.3	196	51.6
Female	101	53.7	80	41.7	181	47.6
Non-conforming	3	1.6	0	0.0	3	0.8

Note: *N=380 is the total number of completed questionnaires out of 450 copies distributed to respondents in the study.

5.2.2 Age of respondents

The results presented in Table 5.2 show the age range of respondents in the studied universities.

Table 5.2: Age Range of the Students

Age range	South Africa (=188)		Nigeria (=192)		Total(*N=380)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
17-20 years	52	27.7	41	21.4	93	24.5
21-25 years	110	58.5	125	65.1	235	61.8
26 years and above	26	13.8	26	13.5	52	13.7

(Source: Survey Data, 2018)

Note: *N=380 is the total number of completed questionnaires out of 450 copies distributed to respondents in the studied universities.

The results in Table 5.2 indicate that 27.7% of respondents were within the age bracket 17-20, 58.5% were between the age range of 21-25, while 13.8% of respondents were 26 years and above in UNIZULU. Similarly, 21.4% of respondents were within the age range of 17-20, and 65.1% were within the age range of 21-25, while 13.5% of respondents were 26 years and above in FUNAAB. The highest population of undergraduate students was between the 21-25 age bracket in the studied

universities.

5.2.3 Average age of respondents

This section describes the average age of participants in the studied universities as presented in Table 6.

Table 5.3: Average Age of Respondents

Age Bracket (Years)	Midpoint t (x)	South Africa (=188)		Nigeria (=192)		Total (N*=380)	
		N	xf	N	xf	N	xf
16 – 20	18.0	52	93	41	738	93	1674
21 – 25	23.0	110	2530	125	2875	235	5405
26 – 30	28.0	26	728	26	728	52	1456
		Σ 188	Σ 3351	Σ 192	Σ 4341	Σ 380	Σ 8535

(Source: Survey Data, 2018)

Note: *N=380 is the total number of completed questionnaires out of 450 copies distributed to respondents in the studied universities.

South Africa

$$\text{Mean} = \frac{\sum fx}{\sum f} = 17.8$$

Nigeria

$$\text{Mean} = \frac{\sum fx}{\sum f} = 22.6$$

Overall

$$\text{Mean} = \frac{\sum fx}{\sum f} = 22.5$$

5.2.4. Distribution of students by their year of study

The study further investigated the distribution of students by their year of study and the result is as shown in Table 7 and subsequent figures.

Table 5.4: Distribution of Students by Year of Study

Current year of study of students	South Africa (=188)		Nigeria (=192)		Total*N =380	
	No of respondents	Percentage	No of respondents	Percentage	No of respondents	Percentage
Year 1	17	9.0	6	3.1	23	6.1
Year 2	66	35.1	50	26.0	116	30.5
Year 3	51	27.1	40	20.8	91	23.9
Year 4	52	27.7	94	49.0	146	38.4
Non-responsive	2	1.1	2	1.0	4	1.1

Note: *N=380 is the total number of completed questionnaires from respondents in the studied universities.

The results in Table 5.4 show the distribution of undergraduate students by year of study. There were more year two students (35.1%) who participated in the study at the University of Zululand, and the least is year 1 students (9.0%). Similarly, the year 4 students scored higher (49.0%) in the level of participation at the Federal University of Agriculture, Abeokuta.

5.2.5 Distribution of respondents by cybertechnology skills

Respondents were asked to indicate in the research questionnaire their level of cybertechnology skills, and the results are as shown in Table 5.5 below.

Table 5.5: Distribution of Students by Cybertechnology Skills

Level of cybertechnology skills of students	South Africa (=188)		Nigeria (=192)		Total (*N=380)	
	No of respondents	Percentage	No of respondents	Percentage	No of respondents	Percentage
Beginners	36	19.1	37	19.3	73	19.2
Intermediate	117	62.2	114	59.4	231	60.8
Advanced	34	18.1	40	20.8	74	19.5
Non-responsive	1	0.5	1	0.5	2	0.5

The results of the cybertechnology skills possessed by the respondents reveal that a total of respondents (19.8% from Nigeria and 18.6% from South Africa) are beginners. For respondents with intermediate skills, there are 115 (59.9%) from Nigeria and 118 (62.8%) from South Africa. Respondents with advanced cybertechnology skills from Nigeria are 39 (20.3%) while those from South Africa are 35 (18.6%). This implies that there are more respondents with intermediate cybertechnology skills from South Africa than Nigeria, and more respondents with advanced skills from Nigeria compared to South Africa. It appears that the level of skills development is largely dependent on the commitment and resources of individual institutions. Perhaps a more compelling factor for the successful development and adoption of cybertechnology in any educational institution is its readiness for e-learning.

5.2.6 Distribution of respondents by years of experience using cybertechnology

Respondents were asked to indicate their years of cybertechnology use. The results of the respondents' experience in using technology reveal that respondents from Nigeria with less than a year's experience are 15 (7.8%) and from South Africa 20 (10.6%). Respondents with 1-2 years' experience from Nigeria are 30 (15.6%) and from South Africa 33 (17.6%). Respondents from Nigeria with 3-4 years' experience are 44 (22.9%) and from South Africa 48 (25.5%). Respondents from Nigeria with 5-6 years' experience are 45 (23.4%) and from South Africa 32 (17.0%). Respondents from Nigeria with 7 years' and above experience of using cybertechnology are 58 (30.2%) and from South Africa 55 (29.3%). The results here imply that there are more respondents with 7 years' experience of using technology from the two countries. Table 5.6 shows the distribution of respondents by years of experience with the use of cybertechnology.

Table 5.6: Distribution of Students by Years of Their Use of Cybertechnology

Years of use of cybertechnology by students	South Africa (=188)		Nigeria (=192)		Total (*N=380)	
	N	Percentage	N	Percentage	N	Percentage
Less than a year	20	10.6	15	7.8	35	9.2
1-2 years	33	17.6	30	15.6	63	16.6
3-4 years	47	25.0	43	22.4	90	23.7
5-6 years	32	17.0	44	22.9	76	20.0
7 years and above	55	29.3	59	30.7	114	30.0
Non-responsive	1	0.5	1	0.5	2	0.5

5.2.7 Distribution of students by average years of use of cybertechnology

Respondents were asked to indicate the average years of their use of cybertechnology, and the results are as shown in Table 5.7.

Table 5.7: Distribution of Students by Average Years of Use of Cybertechnology

Years of use of cybertechnology	(x) Midpoint	South Africa		Nigeria		Total	
		N	xf	N	xf	N	xf
0 – 0.9	0.5	20	10	15	7.5	35	17.5
1 – 2	1.5	33	49.5	30	45	63	94.5
3 – 4	3.5	47	164.5	43	150.5	90	315
5 – 6	5.5	32	176	44	242	76	418
7 – 10	8.5	55	467.5	59	501.5	114	969
		Σ 187	Σ 867.5	Σ 191	Σ 906	Σ 378	Σ 1814

South Africa

$$\text{Mean} = \frac{\Sigma fx}{\Sigma f} = 4.6 \text{ years}$$

Nigeria

$$\text{Mean} = \frac{\sum fx}{\sum f} = 4.7 \text{ years}$$

Overall

$$\text{Mean} = \frac{\sum fx}{\sum f} = 4.8 \text{ years}$$

The results in Table 5.8 show that the mean and average score for undergraduate students at the University of Zululand is 4-7 years, at FUNAAB it is 4.7 years, while for the overall study it is 4.8 years.

Table 5.8: Distribution of Respondents by Faculties/Colleges of Study

Country	Colleges/Faculties	Frequency	Percentage %
Nigeria	COLMAS	44	22.9
	COLBIOS	11	5.7
	COLVET	4	2.1
	COLENG	18	9.4
	COLANIM	20	10.4
	COLPLANT	16	8.3
	COLERM	21	10.9
	COLFHEC	7	3.6
	COLAMRUD	29	15.1
	COLPHYS	22	11.5
	Total	192	100.0
South Africa	Arts	45	23.9
	Education	62	33.0
	Science and Agriculture	41	21.8
	Commerce, Administration and Law	40	21.3
	Total	188	100.0

The results of the demographic characteristics of the respondents based on colleges and faculties revealed that a total of 192 undergraduate students participated in the study. These participants were selected from ten colleges in the Nigerian university and four colleges in the South African university. Thus, the distribution of participants based on faculty/college in Table 5.8 shows that 62 respondents (33.0%) were from the faculty of education, 46 (24.5%) Arts, 41 (21.8%) Science and Agriculture, and 39 (20.7%) were from Commerce, Administration and Law (UNIZULU). Likewise, the results from the data collected from participants in FUNAAB revealed that 22.9% were from Management Science, 15.1% from Agricultural Management and Rural Development, 11.5% were from Physical Science, 10.9% were from Environmental Resources Management, 10.4% from Animal Science and Livestock Production, 9.4% are from Engineering, 8.3% from College of Plant Science, 5.7% are from College of Biological Science, 3.6% from Food Science and Human Ecology while 2.1% were from College of Veterinary Medicine.

The results show that undergraduate students who are respondents in this study are more in the Faculty/College of Education, Management Sciences, Agricultural Management and Rural Development. The results, based on the population strength of each institution, also imply that there were more participants and more colleges selected from the Nigerian university compared to the South African university.

5.3 Research Question Analysis

Research question 1: What are the relationships between students' demographic variables and their cyberethics behaviour at the University of Zululand and the Federal University of Agriculture?

In order to fully understand the demographic or background profiles of the study participants, a chi-square analysis was run for all the demographic characteristics and the cyberethics behaviour variables in the study (on the research instrument). The background profile or demographic variables that were tested and cross-tabulated against other variables using chi-square were:

- College or course of study
- Gender
- Age

- Level of study
- Cybertechnology skills
- Cybertechnology experience

The results point out variations of significance in the relationship between the demographic variables and cyberethics behaviour of undergraduate students in this study as presented in Table 12.

5.3.1 Relationship between course of study and cyberethics behaviour

The course of study was found to have a statistically significant relationship with six variables in Nigeria as against three in South Africa, as indicated in Table 5.9. The Cramer's values show that the relationship is moderate.

Table 5.9: Relationship between Course of Study and Cyberethics Behaviour

Variable/Construct	Pearson Chi- square value	South Africa	Symmetric measures Cramer's V	Pearson Chi- square value	Nigeria	Symmetric measures Cramer's V
		Asymptotic Significance values (2-sided)			Asymptotic Significance values (2-sided)	
Cyberpiracy	20.696	0.055	0.192	87.594	0.000**	0.338
Cybersex and/or Pornography	10.258	0.593	0.135	52.530	0.037**	0.262
Privacy violation	9.871	0.627	0.132	58.878	0.009**	0.277
Blackmailing and disseminating junk mail	6.452	0.892	0.107	50.290	0.057	0.256
Disseminating fake news	20.718	0.055	0.192	47.281	0.099	0.248
Cybercrime	6.371	0.896	0.106	62.274	0.004**	0.285
Cyberstalking	16.055	0.189	0.169	44.083	0.167	0.240
Cyberfraud	14.002	0.301	0.158	49.768	0.063	0.255
Cyberbullying	7.171	0.846	0.113	48.691	0.077	0.252
Hacking/carding/phreaking/crack ing	9.937	0.622	0.133	48.312	0.082	0.251
Cybervandalism	12.219	0.428	0.147	45.985	0.123	0.245
Accessing inappropriate	29.431	0.003**	0.228	38.291	0.366	0.223

or illegal online material						
Identity theft	22.815	0.029**	0.201	30.555	0.725	0.199
Denial of service theft	37.472	0.000**	0.258	35.480	0.493	0.215
Data mining	7.255	0.840	0.113	31.329	0.690	0.202
Cybersquatting	6.834	0.868	0.110	47.836	0.090	0.250
Spoofing and phishing	12.750	0.622	0.150	53.751	0.174	0.237
Violating intellectual property	15.013	0.450	0.163	36.887	0.800	0.196
Violating software license agreement	14.680	0.475	0.161	55.977	0.126	0.241
Using another user's password	21.110	0.133	0.193	53.143	0.189	0.235
Unleashing worms and viruses	12.303	0.656	0.148	57.408	0.102	0.245
Cyber libel	13.463	0.567	0.154	62.404	0.044**	0.255
Cyberterrorism	13.264	0.582	0.153	71.052	0.080	0.272
Cyberespionage	9.740	0.836	0.131	44.855	0.478	0.216
Copyright violation	18.468	0.239	0.181	61.167	0.054**	0.252
Plagiarism	23.982	0.065	0.206	49.581	0.296	0.227
Cyber smearing	16.261	0.365	0.170	67.798	0.016	0.266
Worms and viruses	18.300	0.247	0.180	58.331	0.088	0.246

The results show a moderate strength of association between the course of study and cyberethics behaviour. The finding meant that cyberethics behaviour had a relationship with course of study in the university context. All other variables, except the ones asterisked, are not found to vary with cyberethics behaviour.

5.3.2 Relationship between gender and cyberethics behaviour variables

The gender of undergraduate students was found to have statistically significant relationship with four variables as indicated in Table 5.10. The Cramer's V values show that the relationship is fairly moderate in each of the presented independent variables.

Table 5.10: Relationship between Gender and Cyberethics Behaviour

Variable/Construct	South Africa			Nigeria		
	Pearson Chi- square value	Asymptotic Significance values (2-sided)	Symmetric measures	Pearson Chi- square value	Asymptotic Significance values (2-sided)	Symmetric measures
			Cramer's V			Cramer's V
Cyberpiracy	11.911	0.155	0.178	5.369	0.252	0.167
Cybersex or Pornography	39.119	0.000**	0.323	13.363	0.010**	0.264
Privacy violation	14.336	0.073	0.195	6.646	0.156	0.186
Blackmailing and disseminating junk mail	9.923	0.270	0.162	5.248	0.263	0.165
Disseminating fake news	9.004	0.342	0.155	2.530	0.639	0.115
Cybercrime	7.142	0.521	0.138	8.224	0.084	0.207
Cyberstalking	3.424	0.905	0.095	3.436	0.488	0.134
Cyberfraud	5.766	0.673	0.124	5.994	0.200	0.177
Cyberbullying	5.968	0.651	0.126	3.686	0.450	0.139
Hacking/carding/phreaking/cracking	5.750	0.675	0.124	3.898	0.420	0.142
Cybervandalism	10.778	0.215	0.169	6.291	0.178	0.181
Accessing inappropriate or illegal online material	15.532	0.050**	0.203	2.113	0.715	0.105
Identity theft	16.533	0.035**	0.210	7.071	0.132	0.192
Denial of service theft	8.013	0.432	0.146	4.791	0.309	0.158
Data mining	13.082	0.109	0.187	6.269	0.180	0.181
Cybersquatting	7.573	0.476	0.142	3.253	0.516	0.130
Spoofing and phishing	11.446	0.324	0.174	4.759	0.446	0.157
Violating intellectual property	9.751	0.463	0.161	3.335	0.648	0.132
Violating software license agreement	9.245	0.509	0.157	4.669	0.458	0.156
Using another user's password	11.739	0.303	0.177	6.994	0.221	0.191
Unleashing worms and viruses	8.223	0.607	0.148	8.727	0.120	0.213
Cyber libel	10.465	0.401	0.167	2.559	0.768	0.115
Cyberterrorism	17.504	0.064	0.216	1.596	0.902	0.091

Cyberespionage	7.508	0.677	0.141	3.360	0.645	0.132
Copyright violation	11.064	0.353	0.172	7.328	0.197	0.195
Plagiarism	11.889	0.293	0.178	5.612	0.346	0.171
Cyber smearing	20.609	0.024**	0.234	4.771	0.445	0.158
Worms and viruses	17.367	0.067	0.215	6.113	0.295	0.178

The results in Table 5.10 reveal moderate strength of association between gender and most of the twenty-eight variables. These show the significance of gender in the study of cyberethics behaviour. The findings show that the responses reported on the twenty- eight variables between male, female and non-conformist undergraduate students are true and not due to chance. However, the most significant variables that had a strong relationship with gender in South Africa were cybersex or pornography, with a high chi-square value of $\chi^2=39.119$. Accessing inappropriate or illegal online material ($\chi^2 = 15.532$), identity theft ($\chi^2 = 16.533$) and cyber smearing ($\chi^2 = 20.609$), while that of Nigeria shows cybersex or pornography standing at $\chi^2 = 13.363$ respectively.

5.3.3. Distribution of respondents' gender by age

Results from Table 5.11 shows that majority (60.7%) of the male students in University of Zululand, South Africa, were between the ages of 21 and 25 years, and the highest proportion of the female students (57.4%) were between the same age range. However, only 9.9% of the female students in the institution were older than 25 years, while up to 17.9% of the male students fall into the same category. There were more female students than male students in all the age ranges identified, except for a difference observed among those older than 25 years, where there were slightly more male students than female students. There were three students, one from each of the three age categories, who identified as non-conforming. About 61.6% of the male students at Federal University of Agriculture, Abeokuta, Nigeria, fell into the age category of 21-25 years, while 56% of the female students were in the same category. Only 8.8% of the female students were older than 25 years, while up to 17% of the male students fell into the same age category. No student identified as non-conforming. The results show that the majority of both male and female students in both institutions were between 21 and 25 years of age, while there were more male students who were older than 25 years than female students in both institutions. Table 5.11 shows the distribution of the students' gender by age in the two universities being studied.

Table 5.11: Distribution of Students' Gender by Age

Age (Years)	South Africa (=188)			Nigeria (=192)			Total (*N=380)		
	Male (=84) Freq (%)	Female (=101) Freq (%)	Non- conforming (=3) Freq (%)	Male Freq (%)	Female Freq (%)	Non- conforming Freq (%)	Male Freq (%)	Female Freq (%)	Non- conforming Freq (%)
17-20 years	18 (21.4)	33 (32.7)	1 (33.33)	24 (21.4)	17 (21.3)	0 (0.0)	42 (11.1)	50 (13.2)	1 (0.3)
21-25 years	51 (60.7)	58 (57.4)	1 (33.33)	69 (17.0)	56 (70.0)	0 (0.0)	120 (31.6)	114 (30.0)	1 (0.3)
26 years and above	15 (17.9)	10 (9.9)	1 (33.33)	19 (17.0)	7 (8.8)	0 (0.0)	34 (9.0)	17 (4.5)	1 (0.3)

5.3.4 Distribution of students' gender by cybertechnology skills

Results from Table 5.12 reveal the distribution of students gender by their cybertechnology skills. Results show that majority (69.0%) of the male students in University of Zululand, South Africa, had intermediate level of cybertechnology skills, and the highest proportion (57.4%) of the female students in the same institution also fell into the intermediate level of cybertechnology skills. About 16.7% of the male students in the institution were advanced in their cybertechnology skills, while up to 18.8% of the female students were advanced. By implication, there were more male advanced cybertechnology users than male beginners at the University of Zululand, while among the female students in the institution, the reverse is the case.

Results from the Federal University of Agriculture, Abeokuta, Nigeria, show that the highest proportion of the male students (59.7%) in the institution have intermediate level of cybertechnology skills, with the majority of the female students (58.8%) falling into the same level of cybertechnology skills. About 19.7% of the male students were advanced in their cybertechnology skills, while up to 22.6% of the female students were advanced in their skills. In the institution, there were more male beginners in cybertechnology skills than those advanced in their skills, while the opposite is the case among the female students in the institution. This peculiarity could be attributed to the general opinion that personal computers and other devices were marketed almost exclusively to men, and families were more likely to buy computers for boys than girls. The results also show that the gap that has traditionally existed between the percentage of female and male cybertechnology users has narrowed significantly since studies conducted in 2000. Table 5.12 shows the relationship between the gender of respondents and their cybertechnology skills.

Table 5.12: Distribution of Students' Cybertechnology Skills by Gender

Cybertechnology skills*Gender	South Africa			Nigeria			Total		
	Male Freq (%)	Female Freq (%)	Non-conforming Freq (%)	Male Freq (%)	Female Freq (%)	Non-conforming Freq (%)	Male Freq (%)	Female Freq (%)	Non-conforming Freq (%)
Beginner	12(14.3)	23 (22.8)	1 (33.3)	23 (20.5)	14 (17.5)	0 (0.0)	35 (9.2)	37 (9.7)	1 (0.3)
Intermediate	58(69.0)	58 (57.4)	1 (33.3)	67 (59.8)	47 (58.8)	0 (0.0)	125 (32.9)	105(27.6)	1 (0.3)
Advanced	14(16.7)	19 (18.8)	1 (33.3)	22 (19.7)	18 (22.6)	0 (0.0)	36 (9.5)	37 (9.7)	1 (0.3)
Non-responsive	0 (0.0)	1 (1.0)	0 (0.0)	0 (0.0)	1 (1.3)	0 (0.0)	0 (0.0)	2 (0.5)	0 (0.0)

5.3.5 Distribution of students' years of cybertechnology use by gender

According to Table 5.13, the highest proportion of the male students (34.5%) at the University of Zululand had been into cybertechnology use for more than 6 years. Likewise, the highest proportion for the female students (24.8%) in the institution fell into the same category. There is a similar result on male students at the Federal University of Agriculture, Abeokuta, as the highest proportion of male students (39.3%) in the institution had been into cybertechnology use for more than 6 years. However, results on the female students in the institution differ from this pattern, as about 50% of the female students had between 3 and 6 years of cybertechnology use. The results presented in Table 5.13 show the relationship between cybertechnology experience and gender.

Table 5.13: Distribution of Students' Years of Cybertechnology Use by Gender

Years of Cybertechnology Use*Gender	South Africa			Nigeria			Total		
	Male Freq (%)	Female Freq (%)	Non- conforming Freq (%)	Male Freq (%)	Female Freq (%)	Non- conforming Freq (%)	Male Freq (%)	Female Freq (%)	Non- conforming Freq (%)
Less than a year	3 (3.6)	16 (15.8)	1 (33.3)	4(3.6)	11 (13.8)	0 (0.0)	7(1.8)	27 (7.1)	1 (0.3)
1 – 2 years	14 (16.7)	19 (18.8)	0 (0.0)	17(15.2)	13 (16.3)	0 (0.0)	31(8.2)	32 (8.4)	0 (0.0)
3 – 4 years	23 (27.4)	24 (23.8)	0 (0.0)	23(20.5)	20 (25.0)	0 (0.0)	46(12.1)	44 (11.6)	0 (0.0)
5 – 6 years	15 (17.9)	16 (15.8)	1 (33.3)	24(21.4)	20 (25.0)	0 (0.0)	39(10.3)	40 (10.5)	0 (0.0)
7 years and above	29 (34.5)	25 (24.8)	1 (33.3)	44 (39.3)	15 (18.8)	0 (0.0)	73(19.2)	40 (10.5)	1 (0.3)
Non-responsive	0 (0.0)	1 (1.0)	0 (0.0)	0 (0.0)	1 (1.3)	0 (0.0)	0 (0.0)	2 (0.5)	0 (0.0)

5.3.6 Relationship between age of respondents and cyberethics behaviour

The results presented in Table 5.14 show the relationship between the age of respondents and cyberethics behaviour.

Table 5.14: Relationship between Age of Respondents and Cyberethics Behaviour

Variable/Construct	South Africa			Nigeria		
	Pearson Chi- square value	Asymptotic Significance values (2- sided)	Symmetric measures	Pearson Chi-square value	Asymptotic Significance values (2- sided)	Symmetric measures
			Cramer's V			Cramer's V
Cyberpiracy	13.280	0.103	0.188	5.127	0.744	0.116
Cybersex or Pornography	8.069	0.427	0.146	4.194	0.839	0.105
Privacy violation	6.427	0.599	0.131	7.621	0.471	0.141
Blackmailing and disseminating junk mail	8.783	0.361	0.153	4.365	0.823	0.107
Disseminating fake news	5.848	0.664	0.125	11.186	0.191	0.171
Cybercrime	12.051	0.149	0.179	8.550	0.382	0.149
Cyberstalking	4.067	0.851	0.104	9.931	0.270	0.161
Cyberfraud	6.225	0.622	0.129	8.037	0.430	0.145
Cyberbullying	7.347	0.500	0.140	10.367	0.240	0.164
Hacking/carding/phreaking/crackin g	5.457	0.708	0.120	15.769	0.046**	0.203
Cybervandalism	6.931	0.544	0.136	7.300	0.505	0.138
Accessing inappropriate or illegal online material	14.087	0.080	0.194	10.990	0.202	0.169
Identity theft	4.282	0.831	0.107	5.528	0.700	0.120
Denial of service theft	9.444	0.306	0.158	7.083	0.528	0.136

Data mining	9.929	0.270	0.162	6.542	0.587	0.131
Cybersquatting	8.980	0.344	0.155	8.206	0.414	0.146
Spoofing and phishing	2.593	0.989	0.083	8.119	0.617	0.145
Violating intellectual property	10.014	0.439	0.163	6.533	0.769	0.130
Violating software license agreement	6.390	0.781	0.130	11.354	0.331	0.172
Using another user's password	4.177	0.939	0.105	7.211	0.705	0.137
Unleashing worms and viruses	5.055	0.887	0.116	10.592	0.390	0.166
Cyber libel	8.403	0.590	0.149	11.599	0.313	0.174
Cyberterrorism	7.383	0.689	0.140	8.183	0.611	0.146
Cyberespionage	8.876	0.544	0.154	8.553	0.575	0.149
Copyright violation	10.803	0.373	0.170	17.043	0.073	0.211
Plagiarism	13.448	0.200	0.189	5.101	0.884	0.115
Cyber smearing	5.919	0.822	0.125	19.219	0.380	0.224
Worms and viruses	5.461	0.858	0.121	10.399	0.406	0.165

The results show a moderate strength of association between the age of respondents and only one variable shown in Table 5.14. The most significant variable that had a strong relationship with cyberethics behaviour was hacking/carding/phreaking/cracking, with a high chi-square value, that is ($\chi^2 = 15.769$), and only in Nigeria. Other variables and responses from South Africa are not significant.

5.3.7 Relationship between year of study and cyberethics behaviour

The level of study of cyberethical behaviour of students was found to have statistically significant relationship with two cyberethics misuse variables, as indicated in Table 5.15. The Cramer's V values show that the relationship is fairly moderate in each of the variables.

Table 5.15: Relationship between Year of Study and Cyberethics Behaviour

		South Africa			Nigeria	
Variable/Construct	Pearson Chi-square value	Asymptotic Significant e values (2-sided)	Symmetric measures Cramer's V	Pearson Chi-square value	Asymptotic Significant e values (2-sided)	Symmetric measures Cramer's V
Cyberpiracy	33.770	0.006**	0.212	30.796	0.014**	0.201
Cybersex or Pornography	16.211	0.438	0.147	12.073	0.739	0.126
Privacy violation	12.297	0.723	0.128	13.234	0.656	0.132
Blackmailing and disseminating junk mail	22.118	0.139	0.172	17.219	0.372	0.150
Disseminating fake news	21.489	0.160	0.169	25.320	0.064	0.182
Cybercrime	23.134	0.110	0.175	16.937	0.390	0.149
Cyberstalking	11.686	0.765	0.125	21.545	0.159	0.168
Cyberfraud	14.717	0.545	0.140	23.227	0.108	0.174
Cyberbullying	14.776	0.541	0.140	15.177	0.512	0.141
Hacking/carding/phreaking/cracking	15.265	0.505	0.142	15.476	0.490	0.142
Cybervandalism	17.886	0.331	0.154	20.670	0.192	0.164
Accessing inappropriate or illegal online material	26.470	0.048**	0.188	11.985	0.745	0.125
Identity theft	10.468	0.841	0.118	12.455	0.712	0.128
Denial of service theft	18.206	0.312	0.156	15.596	0.482	0.143

Data mining	25.880	0.056	0.186	20.975	0.179	0.166
Cybersquatting	18.222	0.311	0.156	13.859	0.609	0.135
Spoofing and phishing	27.401	0.124	0.191	24.001	0.242	0.177
Violating intellectual property	21.984	0.341	0.171	14.099	0.825	0.136
Violating software license agreement	20.106 5	0.451	0.164	11.238	0.940	0.121
Using another user's password	12.646	0.892	0.130	15.027	0.775	0.140
Unleashing worms and viruses	15.370	0.755	0.143	15.599	0.741	0.143
Cyber libel	16.603	0.679	0.149	16.903	0.659	0.149
Cyberterrorism	17.301	0.633	0.152	15.122	0.769	0.141
Cyberespionage	28.095	0.107	0.193	22.567	0.311	0.172
Copyright violation	15.908	0.722	0.145	13.198	0.869	0.131
Plagiarism	18.446	0.558	0.157	11.484	0.933	0.123
Cyber smearing	11.056	0.945	0.121	18.150	0.578	0.154
Worms and viruses	12.862	0.883	0.131	20.004	0.458	0.162

The results in Table 5.15 reveal a moderate association between level of study and cyberethics behaviour variables in the two universities. They also show the significance of level of study in the cyberethical behaviour of undergraduate students, particularly on the items asterisked in the table. These suggest that the level of study was not very critical in exploring cyberethics behaviour. The variation therefore came from two variables of cyberethics misuse - cyberpiracy and accessing inappropriate or illegal online material - from responses in South Africa, and one variable of cyberethics misuse - cyberpiracy - in Nigeria. However, the most significant variables with strong relationships with the level of study were: cyberpiracy, with $x = 0.006$; accessing inappropriate or illegal online material, with $x = 0.048$ in South Africa; and cyberpiracy, with $x = 0.014$, in Nigeria.

5.3.8 Relationship between cybertechnology skills and cyberethics misuse

Cybertechnology skills were found to have a significant relationship with eight variables as indicated in Table 5.16. The Cramer's V values show that the relationship is moderate.

Table 5.16: Relationship between Cybertechnology Skills and Cyberethics Misuse

Variable/Construct	South Africa			Nigeria		
	Pearson Chi- square value	Asymptotic Significance values (2-sided)	Symmetric measures	Pearson Chi- square value	Asymptotic Significance values (2-sided)	Symmetric measures
			Cramer's V			Cramer's V
Cyberpiracy	21.687	0.041**	0.340	22.330	0.323	0.171
Cybersex or Pornography	10.407	0.580	0.136	31.281	0.052**	0.202
Privacy violation	20.567	0.057	0.191	16.392	0.692	0.146
Blackmailing and disseminating junk mail	32.352	0.001**	0.240	15.313	0.758	0.141
Disseminating fake news	18.521	0.101	0.181	27.187	0.130	0.188
Cybercrime	21.804	0.040**	0.197	21.766	0.353	0.168
Cyberstalking	28.653	0.004**	0.225	21.821	0.350	0.169
Cyberfraud	26.013	0.011**	0.215	31.689	0.047**	0.203
Cyberbullying	21.319	0.046**	0.194	25.585	0.180	0.183
Hacking/carding/phreaking/cracking	16.024	0.190	0.169	21.355	0.377	0.167
Cyber vandalism	24.385	0.018**	0.208	28.278	0.103	0.192
Accessing inappropriate or illegal online material	16.706	0.161	0.172	18.824	0.533	0.157
Identity theft	19.938	0.068	0.188	16.773	0.668	0.148
Denial of service theft	18.590	0.099	0.182	22.041	0.338	0.169
Data mining	13.544	0.331	0.155	24.069	0.239	0.177
Cybersquatting	12.327	0.420	0.148	16.393	0.692	0.146
Spoofing and phishing	23.791	0.069	0.205	30.038	0.223	0.177
Violating intellectual property	9.903	0.826	0.133	16.399	0.902	0.131
Violating software license agreement	15.910	0.388	0.168	23.628	0.540	0.157
Using another user's password	14.836	0.463	0.162	18.888	0.802	0.140
	17.424	0.294	0.176	26.176	0.398	0.165
Unleashing worms and viruses	14.527	0.486	0.160	25.174	0.453	0.162
	0.140	0.193	22.328	0.617	0.153	

Cyber libel	0.039**	0.214	27.985	0.309	0.171	
Cyberterrorism	0.321	0.173	30.427	0.209	0.178	
Cyberespionage	0.393	0.168	23.124	0.570	0.155	
Copyright violation	0.796	0.136	29.668	0.237	0.176	
Plagiarism	0.580	0.153	21.629	0.657	0.150	
Cyber smearing						
Worms and viruses						

The result shows a fairly moderate strength of association between cybertechnology skills, with eight out of the twenty-eight cyberethics misuse variables in South Africa and only two variables in Nigeria. The variables that had strong relationships with cybertechnology skills in South Africa were: cyberpiracy ($x = 0.041$), blackmailing and disseminating junk mail ($x = 0.001$), cyberstalking ($x = 0.004$), cyberfraud ($x = 0.011$), cyberbullying ($x = 0.046$), cybervandalism ($x = 0.018$), cyberespionage ($x = 0.039$), and in Nigeria, cybersex or pornography ($x = 0.052$) and cyberfraud ($x = 0.047$).

5.3.9 Distribution of students' age range by cybertechnology skills

The relationship between the age range and cybertechnology skills of the respondents are indicated in Table 5.17.

Table 5.17: Distribution of Students' Age Range by Cybertechnology Skills

Age*Cybertechnology skills		Beginners Freq (%)	Intermediate Freq (%)	Advanced Freq (%)	No response
17-20 years	South Africa	18 (34.6)	29 (55.8)	5 (9.6)	0 (0.0)
	Nigeria	16 (39.0)	18 (43.9)	7 (17.1)	0 (0.0)
	Total	34 (8.9)	47 (12.4)	12 (3.2)	0 (0.0)
21-25 years	South Africa	15 (13.6)	75 (68.2)	20 (18.2)	0 (0.0)
	Nigeria	19 (15.2)	78 (62.4)	26 (20.8)	1 (0.8)
	Total	34 (8.9)	153 (40.3)	46 (12.1)	1(0.3)
26 years and above	South Africa	3 (11.5)	13 (50.0)	9 (34.6)	1 (3.8)
	Nigeria	2 (7.7)	17 (65.4)	5 (19.2)	0 (0.0)
	Total	5 (1.3)	30 (7.9)	14 (3.7)	1 (0.3)

Table 5.17 shows the distribution of students' age range by their level of cybertechnology skills. Interestingly the results show that the highest proportion of the students in both institutions in each age category were at the intermediate level of cybertechnology skill, while in all the age categories in both institutions, the least proportion of the students were advanced in cybertechnology skills.

5.3.10 Relationship between cybertechnology experience and cyberethics misuse

Cybertechnology experience was found to have statistically significant relationship with a few cyberethics misuse variables as indicated in Table 5.18. The Cramer's values show that the relationship is fairly moderate in each of the presented variables.

Table 5.18: Relationship between Cybertechnology Experience and Cyberethics Misuse

Variable/Construct	Pearson Chi-square value	South Africa			Nigeria	
		Asymptotic Significance values (2-sided)	Symmetric measures	Pearson Chi-square value	Asymptotic Significance values (2-sided)	Symmetric measures
			Cramer's V			Cramer's V
Cyberpiracy	21.687	0.041**	0.340	22.330	0.323	0.171
Cybersex or Pornography	10.407	0.580	0.136	31.281	0.052**	0.202
Privacy violation	20.567	0.057	0.191	16.392	0.692	0.146
Blackmailing and disseminating junk mail	32.352	0.001**	0.240	15.313	0.758	0.141
Disseminating fake news	18.521	0.101	0.181	27.187	0.130	0.188
Cybercrime	21.804	0.040**	0.197	21.766	0.353	0.168
Cyberstalking	28.653	0.004**	0.225	21.821	0.350	0.169
Cyberfraud	26.013	0.011**	0.215	31.689	0.047**	0.203
Cyberbullying	21.319	0.046**	0.194	25.585	0.180	0.183
Hacking/carding/phreaking/cracking	16.024	0.190	0.169	21.355	0.377	0.167
Cybervandalism	24.385	0.018**	0.208	28.278	0.103	0.192
Accessing inappropriate or illegal online material	16.706	0.161	0.172	18.824	0.533	0.157
Identity theft	19.938	0.068	0.188	16.773	0.668	0.148
Denial of service theft	18.590	0.099	0.182	22.041	0.338	0.169

Data mining	13.544	0.331	0.155	24.069	0.239	0.177
Cybersquatting	12.327	0.420	0.148	16.393	0.692	0.146
Spoofing and phishing	23.791	0.069	0.205	30.038	0.223	0.177
Violating intellectual property	9.903	0.826	0.133	16.399	0.902	0.131
Violating software license agreement	15.910	0.388	0.168	23.628	0.540	0.157
Using another user's password	14.836	0.463	0.162	18.888	0.802	0.140
Unleashing worms and viruses	17.424	0.294	0.176	26.176	0.398	0.165
Cyber libel	14.527	0.486	0.160	25.174	0.453	0.162
Cyberterrorism	20.905	0.140	0.193	22.328	0.617	0.153
Cyberespionage	25.930	0.039**	0.214	27.985	0.309	0.171
Copyright violation	16.966	0.321	0.173	30.427	0.209	0.178
Plagiarism	15.830	0.393	0.168	23.124	0.570	0.155
Cyber smearing	10.365	0.796	0.136	29.668	0.237	0.176
Worms and viruses	13.288	0.580	0.153	21.629	0.657	0.150

The results in Table 5.18 show fairly moderate strength of association between cybertechnology experience and seven out of the twenty-eight cyberethics misuse variables. This suggests that cybertechnology experience was not also very critical in exploring cyberethics behaviour. The variations were observed in eight variables in South Africa and two in Nigeria. In South Africa, the variables with strong relationships with cybertechnology experience were: cyberpiracy ($x = 0.046$), blackmail and dissemination of junk mail ($x = 0.001$), cybercrime ($x = 0.040$), cyberstalking ($x = 0.004$), cyberfraud ($x = 0.011$), cyberbullying ($x = 0.046$), Cybervandalism ($x = 0.018$), and cyberespionage ($x = 0.039$), and in Nigeria, cybersex or pornography ($x = 0.052$) and cyberfraud ($x = 0.047$).

5.3.11. Distribution of students' age range by years of cybertechnology use

The relationship between the age range and cybertechnology experience of the respondents is as indicated in Table 5.19 below.

Table 5.19: Distribution of Students' Age Range by Years of Cybertechnology Use

		Less than a year	1–2 years	3–4 years	5–6 years	7 years and above	No response
Age*Cybertechnology skills		Freq (%)	Freq (%)	Freq (%)	Freq (%)	Freq (%)	Freq (%)
17-20 years	South Africa	7 (13.5)	15 (28.8)	13 (25.0)	5 (9.6)	12 (23.1)	0 (0.0)
	Nigeria	5 (12.2)	12 (29.3)	14 (34.1)	6 (14.6)	4 (9.8)	0 (0.0)
	Total	12 (3.2)	27 (7.1)	27 (7.1)	11 (2.9)	16 (4.2)	0 (0.0)
21-25 years	South Africa	10 (9.1)	18 (16.4)	28 (25.5)	25 (22.7)	29 (26.4)	0 (0.0)
	Nigeria	9 (7.2)	16 (12.8)	25 (20.0)	34 (27.2)	41 (32.8)	0 (0.0)
	Total	19 (5)	34 (9.0)	53 (14.0)	59 (15.5)	70 (18.4)	0 (0.0)
26 years and above	South Africa	3 (11.5)	0 (0.0)	6 (23.1)	2 (7.7)	14 (53.8)	1 (3.8)
	Nigeria	1 (3.8)	2 (7.7)	4 (15.4)	4 (15.4)	14 (53.8)	1 (3.8)
	Total	4 (1.1)	2 (0.5)	10 (2.6)	6 (1.6)	28 (7.4)	2 (0.5)

Results from Table 5.19 reveal the distribution of students' age range by years of cybertechnology use. The highest proportion of the students across the different age ranges in both institutions was 7 years of cybertechnology use or more, except for the students within the age range of 17 and 20 years, among which the highest proportion at the University of Zululand showed 1-2 years of cybertechnology use, while for those at the

Federal University of Agriculture, Abeokuta, it was 3–4 years of cybertechnology use. This result is understandable as studies have shown that most children born within the current digital age are earlier adopter and users of digital technology.

Research Question 2: What is the level of awareness of cyberethical behaviour among students in the two universities in Nigeria and South Africa?

To provide an answer to the second research question in this study, respondents were asked to indicate their level of awareness from a list of 28 cyberethical behaviours. The result is presented in Table 5.20.

Table 5.20: Respondents' Level of Awareness of Cyberethics Behaviour

Cyber-ethical behaviour	Country	Not Aware	Somewhat Aware	Not Sure	Aware	Fully Aware
Cyber-piracy	Nigeria	28 (14.6%)	26 (13.5%)	6 (3.1%)	55 (28.6%)	77 (40.1%)
	South Africa	29 (10.1%)	25 (13.3%)	14 (7.4%)	67 (35.6%)	63 (35.5%)
Cybersex or Pornography	Nigeria	28 (14.6%)	33 (17.2%)	6 (3.1%)	60 (31.2%)	65 (33.9%)
	South Africa	42 (22.3%)	28 (14.9%)	8 (4.3%)	55 (29.3%)	55 (29.3%)
Privacy violation	Nigeria	35 (18.2%)	31 (16.1%)	28 (14.6%)	53 (27.6%)	45 (23.4%)
	South Africa	48 (25.5%)	21 (11.2%)	28 (14.9%)	48 (25.5%)	43 (22.9%)
Blackmailing and disseminating junk mail	Nigeria	36 (18.8%)	27 (14.1%)	24 (12.5%)	52 (27.1%)	53 (27.6%)
	South Africa	55 (29.3%)	14 (7.4%)	26 (13.8%)	49 (26.1%)	44 (23.4%)
Disseminating fake news	Nigeria	45 (23.4%)	18 (9.4%)	12 (6.2%)	52 (27.1%)	65 (33.9%)
	South Africa	46 (24.5%)	16 (8.5%)	14 (7.4%)	51 (27.1%)	61 (32.4%)

Cybercrime	Nigeria	42 (21.9%)	23 (12.0%)	18(9.4%)	47 (24.5%)	62(32.3%)
	South Africa	57(30.3%)	15(8.0%)	12(6.4%)	49(26.1%)	55(29.3%)
Cyber-stalking	Nigeria	44(22.9%)	31(16.1%)	20(10.4%)	49(25.5%)	48(25.0%)
	South Africa	45(23.9%)	26(13.8%)	14(7.4%)	56(29.8%)	47(25.0%)
Cyber-fraud	Nigeria	33(17.2%)	31(16.1%)	15(7.8%)	51(26.6%)	62(32.3%)
	South Africa	46 (24.5%)	28(14.9%)	24(12.8%)	49(26.1%)	41(21.8%)
Cyber-bully	Nigeria	45(23.4%)	23(12.0%)	30(15.6%)	50(26.0%)	44(22.9%)
	South Africa	46(24.5%)	28(14.9%)	24(12.8%)	49(26.1%)	41(21.8%)
Hacking/carding/phreaking/cracking	Nigeria	249(12.5%)	29(15.1%)	34(17.7%)	54(28.1%)	51(26.6%)
	South Africa	43(22.9%)	24(12.8%)	30(16.0%)	49(26.1%)	42(22.3%)
Cyber-vandalism	Nigeria	35(18.2%)	25(13.0%)	53(27.6%)	44(22.9%)	35(18.2%)
	South Africa	47(25.0%)	21(11.2%)	41(21.8%)	39(20.7%)	40(21.3%)
Accessing inappropriate or illegal online material	Nigeria	24(12.5%)	36(18.8%)	31(16.1%)	51(26.6%)	50(26.0%)
	South Africa	44(23.4%)	26(13.8%)	30(16.0%)	48(25.5%)	40(21.3%)
Identity theft	Nigeria	229(11.5%)	40 (20.8%)	28 (14.6%)	59 (30.7%)	43(22.4%)
	South Africa	48(25.5%)	21 (11.2%)	24(12.8%)	57(30.3%)	38(20.2%)
Denial of service theft	Nigeria	37(19.3%)	37(19.3%)	31(16.1%)	49(25.5%)	38(19.8%)
	South Africa	61(32.4%)	26(13.8%)	28(14.9%)	43(22.9%)	30(16.0%)
Data mining	Nigeria	25(13.0%)	36(18.8%)	50(26.0%)	50(26.0%)	31(16.1%)
	South Africa	52(27.7%)	29(15.4%)	30(16.0%)	51(27.1%)	26(13.8%)

Cyber-squatting	Nigeria	35(18.2%)	38(19.8%)	43(22.4%)	46(24.0%)	30(15.6%)
	South Africa	56(29.8%)	24(12.8%)	34(18.1%)	50(26.6%)	24(12.8%)
Spoofing and phishing	Nigeria	27(14.1%)	31(16.1%)	44(22.9%)	50(26.0%)	39(20.3%)
	South Africa	57(30.3%)	22 (11.7%)	34(18.1%)	41(21.8%)	34(18.1%)
Violating intellectual property	Nigeria	32(16.7%)	30(15.6%)	34(17.7%)	57(29.7%)	39(20.4%)
	South Africa	54(28.7%)	21(11.2%)	28(14.9%)	50(26.6%)	35(18.6%)
Violating software license agreement	Nigeria	29(15.1%)	24(12.5%)	29(15.1%)	62(24.5%)	48(25.0%)
	South Africa	53(28.2%)	18(9.6%)	38(20.2%)	41(21.8%)	38(20.2%)
Using another user's password	Nigeria	31(16.1%)	24912.5%)	27(14.1%)	58(30.2%)	52(31.1%)
	South Africa	35(18.6%)	19(10.1%)	27(14.4%)	57(30.3%)	50(26.6%)
Unleashing worms and viruses	Nigeria	31(16.1%)	27(14.1%)	34(18.7%)	54(28.1%)	46(23.9%)
	South Africa	39(20.7%)	26(13.8%)	30(16.0%)	50(26.6%)	43 (22.8%)
Cyber libel	Nigeria	35(18.2%)	25(13.0%)	33(17.2%)	60(31.2%)	39(20.3%)
	South Africa	50(26.6%)	25(13.3%)	25(13.3%)	50(26.6%)	38(20.2%)
Cyber terrorism	Nigeria	28(14.6%)	28(14.6%)	48(25.0%)	50(26.0%)	38(19.8%)
	South Africa	53(28.2%)	24(12.8%)	37(19.7%)	37(19.7%)	37(19.6%)
Cyber espionage	Nigeria	29(15.1%)	28(14.6%)	32(16.7%)	59(30.7%)	44(22.9%)
	South Africa	53(28.2%)	22911.7%)	34(18.1%)	38(20.2%)	41(21.8%)
Copyright violation	Nigeria	27(14.1%)	24(12.5%)	27(14.1%)	59(30.9%)	55(28.6%)

	South Africa	40(21.3%)	21(11.2%)	30(16.0%)	47(25.0%)	50(26.6%)
Cyber smearing	Nigeria	29(15.1%)	24(12.5%)	31(16.1%)	51(26.6%)	57(19.7%)
	South Africa	34(18.1%)	20(10.6%)	31(16.5%)	46(24.5%)	57(30.3%)
Worms and viruses	Nigeria	30(15.6%)	23(12.0%)	25(13.0%)	70(36.5%)	44(22.9%)
	South Africa	47(25.0%)	17(9.0%)	26(13.8%)	52(27.7%)	46(24.3%)

Table 5.20 reveals the level of awareness of respondents on 27 identified cyberethical behaviours. The results confirm that the respondents are mostly aware of the entire cyber-behaviours identified in the table. This is shown with a greater percentage of respondents indicating somewhat aware, aware and fully aware of all the identified cyberethical behaviours. This confirms the fact that respondents from both Nigerian and South African universities in this study are mostly aware of the various cyber-ethical behaviours. When given the opportunity to indicate other cyberethical behaviours aside the ones listed in the table, the results reveal that no other one was identified by the respondents. The results hereby provide answer to the research question by revealing that the level of awareness of cyberethical behaviours among the respondents is very high.

Research Question 2: What is the level of awareness of cyberethical behaviour among students in the two universities in Nigeria and South Africa?

As part of the effort to examine the level of awareness of cyberethical behaviour of the undergraduate students in the two studied universities, the respondents were asked to indicate their involvement in the university annual orientation for students. Respondents were asked whether they had any orientation or training regarding ethical use of cybertechnology in the studied institutions, to which they responded as reflected in Table 5.21. The findings revealed that although orientation and training on ethical use of cybertechnology is crucial and critical for ethical use of cybertechnology, the majority of respondents in Nigeria 105 (54.7%) had received orientation in the first year in the university while only 89 (47.3%) respondents from South Africa indicated yes. The results here imply that those who indicated yes from both countries are more than those who indicated no. Therefore, it can be partially assumed that respondents in part have received orientation on the ethical use of cybertechnology. As this might be the first survey regarding cyberethics misbehaviour and undergraduate use of cybertechnology in these

two institutions, it is worrisome that some institutions do not take the issue very seriously. The results are presented in Table 5.21.

Table 5.21: Q2: Orientation on Use of Cybertechnology: the Level of Awareness of Cyberethical Behaviour among Students in the Two Universities in Nigeria and South Africa

Have you received training on ethical use of cybertechnology	South Africa		Nigeria	
	No of Respondents	Percentage	No of Respondents	Percentage
Yes	89	47.3	105	54.7
No	98	52.1	86	44.8
No Response	1	0.5	1	0.5

Research Question 3: What are the types of cyberethics behaviour of undergraduate students in the universities under study?

To provide answer to the third research question of the study, respondents were asked to indicate their level of agreement with a list of 30 cyberethical behaviours. The result is presented in Table 5.22

Table 5.22: Types of Cyberethics Behaviour among Students in the Two Universities

S/N	Cyberethical Behaviour – Average Mean = 2.5	NIGERIA			SOUTH AFRICA		
		FREQ.	MEAN()	SD	FREQ.	MEAN()	SD
1.	Cyber-piracy (software piracy: music and film downloading)	192	3.66	1.468	182	3.69	1.329
2.	Cybersex (online porn) or pornography	192	3.53	1.438	182	3.28	1.562
3.	Privacy violation	192	3.22	1.477	182	3.09	1.519
4.	Blackmailing and disseminating junk mail	192	3.31	1.588	182	3.07	1.565

5.	Disseminating fake news	192	3.39	1.560	182	3.35	1.590
6.	Cybercrime	192	3.33	1.525	182	3.16	1.647
7.	Cyberstalking	192	3.14	1.501	182	3.18	1.541
8.	Cyberfraud i.e. fraudulent	192	3.41	1.493	182	3.06	1.506
	online banking						
9.	Cyberbullying	192	3.13	1.355	182	3.15	1.537
10.	Hacking/carding/phreaking/ cracking	192	3.41	1.348	182	3.12	1.481
11.	Cybervandalism	192	3.10	1.372	182	3.02	1.477
12.	Accessing inappropriate or illegal online material	192	3.35	1.333	182	3.07	1.479
13.	Identity theft	192	3.32	3.938	182	3.09	1.500
14.	Denial of service attack	192	3.33	1.267	182	2.76	1.503
15.	Data mining (indirect gathering of personal information)	192	3.14	1.342	182	2.84	1.439
16.	Cybersquatting	192	2.99	1.328	182	2.80	1.437
17.	Spoofing and phishing	192	3.23	1.375	182	2.84	1.500
18.	Violating intellectual property	192	3.20	1.379	182	2.94	1.507
19.	Violating software license agreement	192	3.39	1.417	182	2.95	1.500
20.	Using another users' password	192	3.39	1.394	182	3.35	1.446
21.	Unleashing worm and viruses	192	3.29	1.392	182	3.16	1.458
22.	Cybersquatting	192	3.21	1.317	182	2.99	1.508

23.	Cyber libel (false statements that harm another reputation)	192	3.21	1.370	182	2.89	1.493
24.	Cyberterrorism	192	3.31	1.387	182	2.95	1.523
25.	Social media profile cloning	192	3.47	1.421	182	3.24	1.491
26.	Cyberespionage	192	3.39	1.415	182	3.49	1.442
27.	Copyright violation	192	3.42	1.371	182	3.37	1.466
28.	Plagiarism	192	3.38	1.478	182	3.17	1.524
29.	Cyber smearing (embarrassment or humiliation on social network)	192	3.66	1.468	182	3.69	1.329
30.	Worms and viruses (malicious programmes shared with the intent of shutting down the network)	192	3.53	1.438	182	3.28	1.562
31.	Others	0	0	0	0	0	0

The results presented in Table 5.22 reveal that there are about 30 existing types of cyberethical behaviours, as confirmed by the respondents from both the Nigerian and South African universities. Cyberpiracy has the highest mean score of 3.6, SD of 1.5 and mean of 3.6, SD of 1.3 among students in Nigeria and South Africa respectively. This is an indication that cyberpiracy is at an alarming rate in the two universities. This is not surprising, as it is worth mentioning that several studies (Charlesworth and Sewry, 2008; Dinev, Goo, Hu and Nam, 2009) have shown that cyberpiracy tends to be higher in collectivist societies like Nigeria and South Africa.

Following this is cyber-sex behaviour: $\bar{x}$ = 3.5, SD = 1.4 for Nigeria, and $\bar{x}$ = 3.2, SD = 1.5 for South Africa. Next is cyber-smearing: $\bar{x}$ = 3.6, SD = 1.4 for Nigeria, and $\bar{x}$ = 3.7, SD =

1.3 for South Africa. This result should be expected due to the anonymous nature of social media and the growing reliance on same for socio-political engagement by students. Others include spoofing and phishing: $\bar{x} = 3.4$, $SD = 1.4$ for Nigeria, and $\bar{x} = 3.2$, $SD = 1.4$ for South Africa. Another prominent behaviour is copyright violation: $\bar{x} = 3.4$; $SD = 1.3$ for Nigeria, and $\bar{x} = 3.3$; $SD = 1.4$ for South Africa. Aside the 30 cyberethical behaviours, respondents were given the opportunity to identify other cyberethical behaviours they were aware of; however, no other one was identified by respondents from either Nigeria or South Africa.

Research Question 4: What is the influence of the Theory of Planned Behaviour (TPB) on the cyberethical intention of undergraduate students in the universities in Nigeria and South Africa?

To answer research question four, respondents were required to respond to the items on the four variables in the Theory of Planned Behaviour. The result is presented in Table 5.23.

The results in Tables 5.23, 5.24 and 5.25 show the general regression results for the influence of the Theory of Planned Behaviour on the students' cyber behaviour in the two universities in South Africa and Nigeria.

Table 5.23: Applicability and Influence of Theory of Planned Behaviour on Undergraduates' Cyberethics Behaviour

	R	R square	Adjusted R Square	Std Error of the Estimate	Durbin-Watson
South Africa (N = 188)					
1	.737 ^a	.543	.535	8.03171	1.579

All the Theory of Planned Behaviour constructs entered into the model. The Durbin-Watson value of 1.579 as reflected in Table 5.23 is higher than 1, which shows that no autocorrelation was detected; hence the regression model is reliable. The R squared value of 0.543 indicates that variables in the theory jointly account for 54.3% of the variation in the students' cyberethics behaviour in the university in South Africa.

In Table 5.24, the results show the general regression results for the influence of the Theory of Planned Behaviour on the students' cyber behaviour in South Africa.

Table 5.24: Influence of Theory of Planned Behaviour on Cyberethics Misbehaviour of Students in SA (N = 188)

	Sum of Squares	Df	Mean Square	F	Sig
Regression	14089.774	3	4696.591	72.806	.000 ^b
Residual	11869.545	184	64.508		
Total	25959.319	187			

The F-ratio in Table 5.24 of the regression model shows that all the TPB variables significantly predict the variable, $F=72.806$, $p < 0.05$ and therefore the regression model is a good fit for the data. This shows the high impact of the Theory of Planned Behaviour constructs on the behavioural intention and hence the cyberethics misbehaviour of students.

In Table 5.25, the results show the individual influence of the constructs of the Theory of Planned Behaviour on the students' cyber behaviour in South Africa.

Table 5.25: Influence of Each Variable on Cyberethics Behaviour of Students

Model	Unstandardised Coefficients		Standardised Coefficients	t	Sig	Collinearity Statistics	
	B	Standard Error	Beta			Tolerance	VIF
(Constant)	15.413	1.601		9.626	.000		
Attitude	-.328	.089	-.260	-3.706	.000	.506	1.978
Sub Norm	.418	.133	.315	3.139	.002	.247	4.042
PBC	.777	.113	.601	6.887	.000	.326	3.064

The standardised coefficients (beta) and the level of significance in Table 28 show that the

three variables were individually statistically significant in influencing students' cyberethics behaviour. The variables are attitude, subjective norm and perceived behavioural control.

The results show the great significance of the TPB variables in influencing the cyberethics behavioural intention of students in the university in South Africa. Table 29 shows the summary of the impacts of the Theory of Planned Behaviour on students' cyber behaviour in Nigeria.

Table 5.26: Summary of Impacts of Theory of Planned Behaviour on the Students' Cyber behaviour (N = 192)

	R	R square	Adjusted R Square	Std Error of the Estimate	Durbin-Watson
Nigeria					
1	.719 ^a	.517	.505	8.87334	1.748

All the variables entered the regression model. Durbin Watson's value of 1.748 as reflected in Table 5.26 is higher than 1, which shows that no autocorrelation was detected; hence the regression model is reliable. The R squared value of 0.517 indicates that TPB variables jointly account for 51.7% of the variance in cyberethics misuse intention of students in the Nigerian university.

Table 5.27: Influence of TPB Constructs on Cyber Behaviour of Students (N=192)

	Sum of Squares	df	Mean Square	F	Sig
Regression	15851.987	3	5283.996	67.110	.000 ^b
Residual	14802.383	188	78.736		
Total	30654.370	191			

a. Predictors: (Constant), ATTD, SBJN, PBC

b. Dependent Variable Behavioural Intention

The F-ratio in Table 5.27 of the regression model shows that all the Theory of Planned Behaviour constructs significantly predict the cyberethics misbehaviour variable, $F = 67.110$, $p < 0.00$ and therefore the regression model is a good fit for the data. This confirms the influence of the theory

of planned behaviour on the cyberethics misuse behavioural intention of students in the Nigerian university; and hence the significance of the eventual influence in determining the cyberethics behaviour cannot be ignored.

Table 5.28 shows the level of significance of each construct on cyber behaviour of students in Nigeria.

Table 5.28: Influence of Each Variable on the Cyberethics Behaviour of Students in the Nigerian University (N = 192)

Model	Unstandardised Coefficients		Standardised Coefficients	t	Sig	Collinearity Statistics	
	B	Standard Error	Beta			Tolerance	VIF
(Constant)	15.654	1.754		8.923	.000		
Attitude	-.312	.099	-.251	-3.169	.002	.410	2.439
Sub Norms	.195	.148	.140	1.314	.190	.226	4.421
PBC	1.026	.123	.747	8.353	.000	.321	3.115

Dependent Variable: Behavioural intention

The standardised coefficients (beta) and level of significance in Table 5.28 show that two out of the constructs were individually statistically significant in influencing the cyberethics misbehaviour of students. The constructs were attitude and perceived behavioural control.

In Table 5.28, the overall regression results in the two universities on the influence of Theory of Planned Behaviour on cyber behaviour of students is as indicated in Table 5.28

below.

Table 5.29: General Summary of Regression Results for the Two Universities (N = 380)

	R	R square	Adjusted R Square	Std Error of the Estimate	Durbin-Watson
1	.726 ^a	.528	.524	8.47378	1.656

Table 5.30: Influence of TPB Constructs on Cyber Behaviour of Students (N = 380)

	Sum of Squares	df	Mean Square	F	Sig
Regression	30174.141	3	10058.047	140.075	.000 ^b
Residual	26998.646	376	71.805		
Total	57172.787	379			

Table 5.31 shows the influence of individual variables on cyberethics behaviour of students in the two universities.

Table 5.31: Influence of Each Variable on Cyberethics Misbehaviour of Students in the Two Universities (N = 380)

Model	Unstandardised Coefficients		Standardised Coefficients	t	Sig	Collinearity Statistics	
	B	Standard Error	Beta			Tolerance	VIF
(Constant)	15.454	1.184		13.049	.000		
Attitude	-.317	.066	-.252	-4.804	.000	.456	2.195
Subjective Norms	.301	.100	.220	3.017	.003	.236	4.230
Perceived Behavioural Control	.910	.083	.680	10.904	.000	.323	3.095

The results in Tables 5.27, 5.28 and 5.31 represent the overall regression analysis of the influence of the independent variables (attitude, subjective norm and perceived behavioural control) on the dependent variable (intention towards cyberethics misbehaviour). The results revealed that students' attitude ($B = 0.252$, $t = 4,804$, $p < 0.05$), subjective norm ($B = 0.220$, $t = 3.017$, $p < 0.05$) and perceived behavioural control ($B = 0.680$, $t = 10.904$, $p < 0.05$) significantly contributed to students' intention towards cyberethics misbehaviour. The results also revealed a positive relationship ($r = 0.726$) between attitude, subjective norms and perceived behavioural control and the intention towards cyberethics misbehaviour; even as the three variables accounted for the 52.4% variation in students' intention towards cyberethics misbehaviour (adjusted $R = 0.524$).

5.4 Summary of Regression Results

Table 26 presents the results of the regression of the influence of the variables of the Theory of Planned Behaviour on cyberethical practices. The regression results show an adjusted R-square value of 0.505 for Nigeria and 0.543 for South Africa. Table 26 and an F-ratio of 67.110 for Nigeria (Table 29) and F-ratio of 72.806 (Table 32), which are

significant at 0.05 level ($0.000 < 0.05$). These results indicate that the three independent variables (attitude, subjective norms, and perceived behavioural control towards cyberethical behaviour) jointly (as indicated by the R-square value) explained or predicted 51.7% of the variations on the influence of the Theory of Planned Behaviour on undergraduate cyberethical behaviour in Nigeria, and 54.3% of the variations on the influence of Theory of Planned Behaviour on undergraduate students' cyberethical behaviour in South Africa. This implies that the influence of the Theory of Planned Behaviour is a little bit more on the South African undergraduate students than on the Nigerian students. Overall, the Theory of Planned Behaviour has influence on the cyberethical behaviour of the undergraduate students from both countries. This indicates that attitude, subjective norms and perceived behavioural control can cause or determine the cyberethical behaviour of undergraduate students.

Tables 5.27 to 5.31 provide information on the individual contributions of each of the three factors in predicting cyberethical intentions. The results show that each of the factors makes significant contributions to the prediction (as indicated by the significance of the t values, which are less than 0.05, as shown in the rightmost column of the two tables 34. Also, it can be seen from the results that the standardised coefficients (Beta values) indicate the relative strength of each factor in the prediction of cyberethical intention and that perceived behavioural control contributed most to the prediction of cyberethical behavioural intentions and eventual behaviour of undergraduate students (Beta value = .747) in Nigeria and perceived behavioural control (Beta value = .601) in South Africa. These results imply that all the three constructs of the Theory of Planned behaviour (TPB) can significantly predict cyberethical intention and behaviour.

Research Question 4: What are the challenges to students' cyberethical behaviour in the universities in Nigeria and South Africa?

To provide answer to this research question, respondents were asked to indicate their level of agreement and disagreement to a list of 21 identified challenges associated with students' cyberethical behaviour in the universities in Nigeria and South Africa. The result is presented in Table 5.32.

Table 5.32: Challenges to Students' Cyberethical Behaviour in Nigeria and South Africa

Challenges	Country	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Social negative influence	Nigeria	5(2.6%)	9(4.7%)	24(12.5%)	68(35.4%)	86(44.8%)
	South Africa	7(7.37%)	14(7.4%)	44(23.4%)	70(37.2%)	53(28.4%)
Ease of performing illegal activities	Nigeria	4(2.1%)	25(13.0%)	35(18.3%)	62(33.3%)	66(34.4%)
	South Africa	6(3.2%)	36(19.1%)	52(27.7%)	54(28.7%)	40(21.3%)
Lack of adequate security measures to ensure compliance with cyberethics policy	Nigeria	6(3.1%)	18(9.4%)	34(17.7%)	68(35.4%)	66(34.4%)
	South Africa	9(4.8%)	30(16.0%)	25(23.9%)	63(33.5%)	41(21.8%)
Lack of enough training and	Nigeria	4(2.1%)	17(8.9%)	32(16.7%)	77(40.1%)	62(32.3%)
Challenges	Country	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Education on implications of ethical violations						
	South Africa	9(4.8%)	19(10.1%)	32(17.0%)	78(41.5%)	40(46.6%)

Lack of policy guidance on appropriate cyber behaviour	Nigeria	6(3.1%)	18(9.1%)	38(19.8%)	70(36.5%)	60(31.3%)
	South Africa	10(5.3%)	20(10.6%)	40(21.3%)	69(36.7%)	49(26.1%)
Over-loaded teaching and learning curriculum	Nigeria	10(5.2%)	17(8.9%)	33(17.2%)	71(37.0%)	61(31.8%)
	South Africa	10(5.3%)	22(11.7%)	41(21.8%)	64(34.0%)	51(27.1%)
Contradiction between copyright and freedom of information	Nigeria	7(3.6%)	18(9.4%)	37(19.3%)	68(35.4%)	62(32.3%)
	South Africa	15(8.0%)	19(10.1%)	56(29.8%)	61(32.4%)	37(19.7%)
Lack of cyber values and ethical conduct in the use of cybertechnology	Nigeria	9(4.7%)	17(8.9%)	37(19.3%)	73(38.0%)	56(29.2%)
	South	9(4.8%)	21(11.2%)	44(23.4%)	70(37.2%)	42(23.4%)
Challenges	Country	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	Africa					
Negative violations of the integrity of the institution's cyber infrastructure	Nigeria	7(3.6%)	23(12.0%)	27(19.3%)	67(34.9%)	58(30.2%)

	South Africa	10(5.3%)	21(11.2%)	61(32.4%)	59(31.4%)	37(19.7%)
Exposure of the institution's network to virus and malware	Nigeria	7(3.6%)	30(15.6%)	49(25.5%)	55(28.6%)	51(26.6%)
	South Africa	9(4.8%)	25(13.3%)	62(33.0%)	58(30.9%)	34(18.1%)
Misuse of institution license software and hardware	Nigeria	7(3.6%)	24(12.5%)	51(26.6%)	59(30.7%)	51(26.6%)
	South Africa	14(7.4%)	33(17.6%)	49(26.1%)	53(28.2%)	39(20.8%)
Management bureaucratic processes	Nigeria	11(5.7%)	18(9.4%)	35(18.2%)	72(37.5%)	56(29.2%)
	South Africa	17(9.0%)	25(13.3%)	44(23.4%)	63(33.5%)	39(20.8%)
Breaches in confidentiality and network security	Nigeria	6(3.1%)	26(13.5%)	31(16.1%)	73(38.0%)	56(29.2%)
Challenges	Country	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	South Africa	11(5.9%)	28(14.9%)	52(27.7%)	60(31.9%)	37(19.7%)
Lack of time and commitments	Nigeria	9(4.7%)	20(10.4%)	39(20.3%)	67(34.9%)	57(29.7%)
	South Africa	18(9.6%)	29(15.4%)	47(25.0%)	60(31.9%)	34(18.1%)

Lack of publicised policies about the unethical use of cybertechnology	Nigeria	7(3.6%)	19(9.9%)	41(21.4%)	62(32.3%)	63(32.8%)
	South Africa	14(7.45)	23(12.2%)	46(24.5%)	67(35.6%)	38(20.2%)
Lack of ethical consideration and consequence of violations	Nigeria	9(4.7%)	22(11.5%)	33(17.2%)	64(33.3%)	64(33.3%)
	South Africa	18(9.6%)	18(9.6%)	50(26.6%)	59(31.4%)	43(22.9%)
Data theft and loss of sensitive institution information	Nigeria	10(5.2%)	20(10.4%)	37(19.3%)	67(34.9%)	58(30.2%)
	South Africa	19(10.1%)	16(8.5%)	48(25.5%)	65(34.6%)	40(21.3%)
Compromised account or passwords	Nigeria	13(6.8%)	14(7.3%)	33(17.2%)	67(34.9%)	65(33.9%)
Challenges	Country	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	South Africa	20(10.6%)	19(10.1%)	38(20.2%)	57(30.3%)	54(28.7%)
Financial constraints	Nigeria	14(7.3%)	12(6.2%)	41(21.4%)	68(35.4%)	57(29.7%)
	South Africa	18(9.6%)	22(11.7%)	42(22.3%)	55(29.3%)	51(27.1%)

Risk to anonymity of users	Nigeria	14(7.3%)	16(8.3%)	35(18.2%)	68(35.4%)	59(30.7%)
	South Africa	19(10.1%)	22(11.7%)	49(26.1%)	57(30.3%)	41(21.8%)
Theft of copyrighted materials	Nigeria	15(7.8%)	13(6.8%)	38(19.8%)	62(32.3%)	64(33.3%)
	South Africa	21(11.2%)	21(11.2%)	48(25.5%)	56(29.8%)	42(22.4%)

As revealed in Table 5.32, the results clearly indicate that the entire list of 21 challenges are significant challenges facing institutions as a result of students' cyberethical behaviour in Nigeria and South Africa. A cursory look at the results in the table confirms that the addition of neutral, agree and strongly agree responses, when added together to each of the challenges identified in the table, gives a high percentage response to each item. This, therefore, confirms and indicates that the 21 challenges are significant challenges associated with students' cyberethical behaviours. Asides from the listing of the challenges in table 35, respondents were also asked to indicate other challenges they think are associated with students' cyberethical behaviours, but which were not listed. However, none was identified by any of the respondents. This means that aside the 21 challenges listed in the table, there are no other challenges in existence that are associated with students' cyberethical behaviours, both in Nigeria and South Africa.

5.5 Summary

This chapter presented the results of the data analysis from the survey of the sampled population of key users of cybertechnology in the universities under study. The study was conducted by means of self-administered questionnaires for undergraduate students. The study results pertaining to cyberethics behaviour were discussed, guided by the study objectives including cyberethics awareness, types of cyberethical behaviour among students, the influence of the Theory of Planned Behaviour on students' cyberethical behaviour, and challenges of the efforts by the undergraduate students to act ethically correct in cyberspace. The findings from this section revealed that of the 450 administered

questionnaires, 380 questionnaires were returned, giving a response rate of 84.4%. The followings are other important findings from the study:

1. There are dominant female respondents from the South African university and more male from Nigeria.
2. The highest population of undergraduate students are in the 21-25 age bracket; the age of most respondents in the University of Zululand was between 21 and 25 years, with the average being 17.8 years. The respondents' overall average age of 22 is within the computer and internet proficiency period, which makes guiding their ethical use of cyber-technology a worthwhile endeavour.
3. There were more year two students (35.1%) who participated in the study at the University of Zululand, and the least of the participants were the year one students (9.0%). Similarly, the year four students (49.0%) scored higher in the level of participation at the Federal University of Agriculture, Abeokuta, Nigeria and were equally the overall participants (76.7%) in this study.
4. For respondents with intermediate skills, there were 115 (59.9%) from Nigeria and 118 (62.8%) from South Africa. Respondents with advanced cyber-technology skills from Nigeria were 39 (20.3%) while those from South Africa were 35 (18.6%). This implies that there were more respondents with intermediate cyber-technology skills from South Africa than Nigeria, and more respondents with advanced skills from Nigeria compared to South Africa.
5. Respondents with 7 or more years of experience in technology use from Nigeria were 58 (30.2%) and from South Africa 55 (29.3%). The results here imply that there were more respondents from the two countries with 7 years' experience of using technology.
6. The results show that undergraduate students who are respondents in this study are more in the Faculty/College of Education, Management Sciences, Agricultural Management and Rural Development. The results imply that there were more participants and more colleges selected from the Nigerian university compared to the South African university.
7. The findings of the study reveal some variations in the relationship between demographic characteristics and cyberethics behaviour of the respondents in South Africa and Nigeria.

8. The results also reveal that a greater percentage is evident by adding the percentages of somewhat aware, aware and fully aware together. This confirms the fact that respondents from both the Nigerian and South African universities are mostly aware of the different cyberethical behaviours. When given the opportunity to indicate other cyberethical behaviours aside those listed in the table, the results reveal that no other cyberethical behaviour was identified by the respondents
9. From the study, it can be partially assumed that respondents in part have received training on the ethical use of cybertechnology. However, a high percentage of the participants - 98 (52.1%) - show that they had never received such training in the university. As this might be the first survey regarding cyberethics misbehaviour and undergraduates' use of cybertechnology in these two institutions, it is a cause for concern that some institutions do not take the issue very seriously.
10. Top on the list of types of cyberethics violations are cyber piracy, with the highest mean scores of $\bar{x} = 3.6$, $SD = 1.5$ and $m = 3.6$, $SD = 1.3$ among students in Nigeria and South Africa respectively, an indication that cyberpiracy is at an alarming rate in the two universities. Following this is cyber-sex behaviour with $\bar{x} = 3.5$, $SD = 1.4$ for Nigeria and $\bar{x} = 3.2$, $SD = 1.5$ for South Africa. Next is cyber-smearing, with $\bar{x} = 3.6$, $SD = 1.4$ for Nigeria and $m = 3.7$, $SD = 1.3$ for South Africa.
11. The variables, attitude, subjective norm and perceived behavioural control were found to be individually statistically significant in influencing students' cyberethics behaviour. The regression results show an adjusted R-square value of 0.517 for Nigeria and 0.543 for South Africa (Table 26), and an F-ratio of 67.110 for Nigeria (Table 29) and F-ratio of 72.806 (Table 32), the two of which are significant at 0.05 level ($0.000 < 0.05$). These results indicate that the three independent variables (attitude, subjective norms, and perceived behavioural control towards cyberethical behaviour) jointly (as indicated by the R-square value) explained or predicted 51.7% of the variations on the influence of the Theory of Planned Behaviour on undergraduates' cyberethical behaviour in Nigeria and 54.3% of the variations on the influence of the Theory of Planned Behaviour on undergraduates' cyberethical intention and eventual behaviour in South Africa.
12. The standardised coefficients (Beta values), which indicate the relative strength of each factor in the prediction of cyberethical intention, show that perceived

behavioural control contributed most to the prediction of cyberethical intentions and eventual behaviour of undergraduate students in Nigeria (Beta value = .747) and in South Africa (Beta value = .601). These results imply that all the three constructs of the Theory of Planned Behaviour (TPB) exert significant contributions in explaining or predicting cyberethical intention and behaviour.

13. The entire 21 challenges listed in the table are significant barriers facing institutions as a result of students' cyberethical behaviour in Nigeria and South Africa. A cursory look at the results in the table confirms that the addition of neutral, agree and strongly agree responses to each of the challenges identified in the table results in a high percentage response to each item. This confirms and indicates that the 21 challenges are significant challenges associated with students' cyberethical behaviours.

The next chapter presents the analysis of findings from the interview with key staff in the ITS and ICTREC sections of the two universities. It also provides the analysis of interview data.

CHAPTER SIX

PRESENTATION AND ANALYSIS OF INTERVIEW DATA

6.1 Introduction

As indicated in chapter four of this study, a combination of methods was adopted to collect data for the study. This chapter, like the previous chapter where quantitative data were presented, reports the findings from the qualitative method. The interview schedule is attached as Appendix 4. The respondents for the interview were selected from the ITS and ICTREC sections of the two universities under investigation. They were the director, head of sections, other administrators and computer lab assistants in the universities.

The universities are located in semi-rural areas in the two countries under investigation. The purpose of this study was to understand the perception of the participants of the phenomenon of cyberethical behaviour of undergraduate students in these studied universities. Were there indicators of cyberethical violations in the studied universities? How do we know? To answer these questions, 14 interviews were conducted with ITS and ICTREC staff of the two universities to obtain their perceptions of cyber practices and behaviour of students in their domain.

Responses to the interview questions from the participants provided a great deal of interesting and useful data that successfully contributed to answering the research objectives and questions of this study. The questions on cyberethics policies were not included in the students' survey and are addressed here. It was believed that the ICT professionals in the two institutions, given their experience, would be able to provide more details about the various policies guiding the management of cyber infrastructures and IP networks of the institutions.

The overall participants for the interview session with relevant key staff of the ICTREC and ITS sections of the two universities are indicated in Table 6.1 below. It should be noted that responses to the interview questions were based on the different expertise of the participants and the extracted verbatim responses were their views.

.

Table 6.1: Interview Participants

Director ICTREC	1
Backend Administrator	2
Lab Assistance	4
Network Administrator	4
Chief System Analyst	1
Head Automation	1
Intellectual Property Officer	1
Total	14

The participants for the interview for this study, as shown in Table 6.1, are key staff members in the ITS and ICTREC sections of the two universities chosen for this study and they are considered key informants on the phenomenon under investigation. The ITS section at the university of Zululand had no director as at the time of this study.

Research objectives that are reported in this qualitative section of the study probed the following:

1. The level of awareness of cyberethical behaviour among undergraduate students;
2. The types of cyberethical behaviour of undergraduate students;
3. The challenges of cyberethical behaviour on the integrity of the universities; and
4. The impact of information technology policy in strengthening or promoting compliance with ethical conduct in cyberspace of the two universities.

It must be noted that questions 1 and 3 on the demographic characteristics and the influence of the Theory of Planned Behaviour on undergraduates' cyberethics behaviour was not addressed in this section as they were based on some specific variables that are examined quantitatively. Similarly, the complex and anonymous nature of some questions may not be amenable to quantitative data gathering. Thus, the interview data provide more detailed information to validate and explain the complex nature of cyberethics issues.

Related themes that emerged after the analysis of the data, which are directly linked to the research questions, are four and are as follows:

Theme 1: Inappropriate behaviour in cyberspace is occasional, and not frequent, due to restriction and monitoring.

Theme 2: Evidence and dimensions of cyberethical behaviour in the universities and their manifestation are included in this theme.

Theme 3: Ethical violations of university network have decisive effect on the image and integrity of the university. At the same time, it affects internet traffic or bandwidth usage, and puts pressure on university cyber infrastructure.

Theme 4: There are restrictions on internet connectivity and control of access to internet services.

Finding 1: From the respondents in both universities, it was revealed that there is urgent need for the university managements to organise training and educational programmes on cyberethics for all categories of students. This will create awareness concerning the development and understanding of ethical use of cybertechnology.

Finding 2: According to the participants, there are indications of weaknesses in the current measures to check cyberethical issues. Therefore, institutions should improve on relevant cyber security measures in order to promote acceptable conduct while engaged in cybertechnology use on campus and beyond.

Finding 3: A number of challenges on unethical use of cybertechnology on campus, with implications for the integrity, security and safety of service delivery to the university community, were identified. Some of these defining challenges include:

- Students' unethical behaviour has decisive effect on the image and integrity of the university;
- Large files from the Internet still the traffic and service provision to other legitimate users;
- Lack of adequate interest on the part of the institutions' executive members;
- Lack of training on ethical use of cybertechnology;
- Students are recalcitrant;

- Policies are not fully implemented; and
- Lack of knowledge of cybertechnology ethics.

Finding 4: The institutions under investigation need to review existing internet policies to reflect clauses on ethical behaviours that will define the cybertechnology behaviour expected from users of their networks.

The study discovered the existence of all these factors in the two institutions, which clearly shows the presence of cyberethical violations among undergraduate students.

The chapter presents details of the findings of this investigation. The research questions will be addressed and findings from the data collection will be discussed by themes with support from participants' statements, as well as quantitative data where applicable. The current chapter is only devoted to the presentation of the findings from the qualitative data collection, and not in-depth interpretations and discussions of findings and their implications.

6.2 The Findings

In seeking to investigate and analyse the findings from this study that aimed to discover cyberethical behaviour of undergraduate students in two selected universities in two different countries in Africa, data were elicited from 14 participants. Participants' responses in the two universities in this study are grouped and presented together.

Four themes were extracted from the coding that was generated from the analysed data and they are based on the four research questions included in this section. The themes are: inappropriate behaviour in cyberspace is occasional and not frequent due to restriction and monitoring in the two universities; evidence and dimensions of cyber behaviour violations in the universities and their manifestation; ethical violations on university network has decisive effect on the image and integrity of the university and service provision of the institutions' cyber infrastructures; and there are restrictions and control of cyber behaviour on the network of the two universities.

Table 6.2: Framework of This Chapter

Research Questions	Themes	Key variables/Descriptors	Data collection methods
What is the level of awareness of cyber behaviour among undergraduate students?	Inappropriate behaviour in cyberspace is somewhat occasional and not frequent due to restriction and monitoring.	• Ignorance • Limited punishments • Nothing wrong in unethical behaviour • Films and music downloads • Students are big consumers of music and films • Students are stubborn • Crack software • Stream video pirated software • limited access to ethical use policy • Lack of reading terms and conditions	• Literature review • ITS/ICTREC staff interview questions 1, 2,3,4,5.

What are the types of cyber behaviour of undergraduate students?	Evidence and dimensions of cyber behaviour in the universities and their manifestation is included in this theme	• Inappropriate behaviour regarding cyberethics • Fake news • Plagiarism • Hacking • Pornography • Online gaming • Financial fraud • Identity theft • Negative behaviour on social media	• Literature review • ITS/ICTREC staff interview questions 1b.5.12
What are the challenges of students' cyber behaviour on the integrity of the university?	Ethical violations on university network has decisive effect on the image and integrity	• Has decisive effect • May impact institution's ranking • Rub on the integrity of the	• Literature review • ITS/REC staff interview questions 6b.6c.7a 7b, 7c
	of the university, service provision of the institutions' cyber infrastructure	• university • Institution's IP may be blacklisted • Introduce all forms of viruses and Trojan that could break down the	

		entire cyber infrastructure	
What is the influence of cyberethics policy on strengthening or promoting compliance with ethical behaviour on the network of the university?	There are restrictions and control		• Literature review • ITS/ICTREC staff interview questions 8,9,10,11,12,13

6.2.1 Level of awareness of cyber behaviour among undergraduate students

This finding revealed the perception on awareness and orientation about cyberethical misbehaviour, which answers research question 1. Questions 1a, 2, 3, 4 and 5 on the interview guide were designed to investigate this phenomenon. Included in this examination are questions about whether the universities provide orientation or specific lessons for students on ethical use of cybertechnology, how the issues of cyberethics are being addressed with the students, and if copies of the ethical guidelines of the universities are given to students during orientation. Majority of the participants, 13 out of 14 (93%), confirmed that there are orientation programmes for freshmen at the beginning of every session, but opinions differ on ethical instructions or

orientation and guidance on the use of cybertechnology in the institutions. The same number of participants also expressed different opinions on the availability of hard copies of the universities' policies for students during orientation. Table 38 presents the comments from the interviewees on the orientation of students on cybertechnology in the two studied institutions:

Table 6.3: Comments on Orientation or Specific Lesson on Ethical Use of Cybertechnology

Participants	Responses
UZ 1	<i>"We actually have orientation, where we teach them in terms of how to use the network of the university and mainly what they are not allowed to access on the university network, but the rest they can access anything except downloading of music and pornographic materials."</i>
UZ 2	<i>"There is orientation in the first week of registration for the first year students but most student hardly attend most of the procedures of the few hours."</i>
UZ 3	<i>"Yes, the university has a plan during registration to earmark some days for orientation, either orientation as a whole or at the lab for all students who register. Yes, we do have orientation for our student but not fully on ethical use of cybertechnology but the use of the network and others."</i>
FUNAAB 1	<i>"...orientations to students is occasional but, it should have been better if it is an annual thing and an avenue to inform students on the ethics in the utilisation of cyberspace and the devices that are networked in the virtual experience. It is also good to note that the orientation should have made available to students a hard copy of the section within the ICT policy that touches on ethics and conduct within the campus."</i>

FUNAAB 2	<i>“Well, I would say there is no programme of such per say but, what we have on ground for the students is that at the beginning of every session we have an orientation for them, we have talks about the use of the Internet, the use of computers, online programmes and the use of portals that we have on campus and so we try at least restrict them to academic applications that we have within the campus without being involved themselves in unethical cyber behaviour.”</i>
FUNAAB 3	<i>“I'm not sure there is. But I know that generally the managements give the students freedom to access the Internet of which aside the orientation lesson given to them in their first week of admission and all that. They're expected to walk by whatever they've been taught. That's how far that I know. So, it's not that we really have specifically, that if you do this, you get this punishment, you can do these.”</i>
FUNAAB 4	<i>“Yes. Basically, for us here, I think it has become part of our policy for new entrants. Their first week is ICT training and it has come to stay. So, it's one of the policies. So, the first thing they would do during their registration, the first classes they will attend during the very first week before they even go for other form of orientation. So, ICT training has come to stay and has become part of our policy. So, we take them through so many of these issues, discussing the use of the Internet, the do's and the don'ts and then we actually outline all of our policies and then the rules that guide the use of our network.”</i>

6.2.2 Types of cyber behaviour of undergraduate students

The opinions of participants on cyberethical issues and their professional experience with students' cyber behaviour and the institutions' guidance on ethical orientations vary. Out of the 14 participants, a common view of 8 (57%) interviewees at FUNAAB was that inappropriate behaviour in cyberspace and on the network of the university is somewhat occasional and not frequent due to measures of restrictions and monitoring by the backend administrators of the university's network. Network usage terms and conditions have been established and set on a prop up page before users can connect. However, even when

students have accepted the terms and conditions stipulated on the pop up pages, some still violate these terms and conditions. 6 (43%) of the participants at Unizulu admit that due to unfettered restrictions to students' access to some social media sites like YouTube, students see nothing bad in downloading music and films and involvement in other social media for anti-social behaviour.

Most participants reported that students do use cybertechnology for purposes other than academic. Participants admitted that there were cybertechnology infractions among the students in the studied universities.

The table below presents the comments from respondents that provide evidence of types of cyberethical issues exhibited by students in the studied institutions

Table 6.4: Types of Cyber Behaviour Exhibited by Undergraduate Students

Participants	Responses
UZ 12	<i>“For students, when you give them access to the Internet, student will try to access anything, they try to download movies, access porn sites, although most of the porn sites are blocked off, but yet you find our student trying to circumvent the security barriers to gain access to these sites.”</i>
UZ 13	<i>“The way it is done here is that, all known downloading sites are blocked off but with the exclusion of educational sites, reason being we don't block actual words like sex, porn or other educational sites that talk about sex. We only block pornographic sites so there won't be access. Others are open for them for educational and instructional purpose on issues about sex education but once we discover violation or abuse through circumventions of the network we block such sites. I think we are also in the learning process.”</i>

UZ 10	<i>“What I have noticed is that, number of students, well for them it is normal to download music and movies online and share it. They see nothing wrong with that. Maybe it is has something to do with us people ignoring something written down because, surely, there are rules and regulations for the students. Before you can access the Internet on the desktop there are rules and regulations. You have to click accept first then you can proceed, but you always found out that students will log in into the system and do the very same thing they said they wouldn’t do by accepting the rule.”</i>
UZ 09	<i>“...very common, I would say they download music, movies and software. They</i> <i>do get sites to download cracked software, stream video, films series and episodes by going back in time to download missed editions.”</i>
FUNAAB 8	<i>“I think our students engaged more negatively on social media platforms to promote rumours, falsehood, to mislead other colleagues through wrong information. Another one is looking for opportunity to make cheap and illegal money by trying to hack into loopholes into financial institutions network. In short, students here are not counted out of the popular financial free fraud called yahoo yahoo, and this is consequence on their use of cyber technology.”</i>
FUNAAB 6	<i>“...and like I said earlier such behavior is still rampart in this area, because once you have access and you are not being regulated, you are bound to go out of the norms expected within an environment like this.”</i>

FUNAAB 7	<i>“We as the administrator of the Internet we are putting something in place to checkmate all these by making sure that students are not allowed to visit some sites that are not ethical and to also regulate what they download or post on the Internet. I think what really makes them to follow these procedures is that we have a good policy on ground that show and guide them on what they can do with their cyber-technology online on our network. This is what is guiding their attitude and usage.”</i>
FUNAAB 2	<i>“For us, we believe in the application of corrective measure and not punitive in resolving unethical violations. We also apply a counter campaign to deter negative use and these in a way have helped to reduce unethical use of cyber technology by students.”</i>
FUNAAB 1	<i>“You cannot rule it out in an institution of this magnitude. It occurs but it is not frequent; it is very rare. Maybe I would say occasionally. I knew that well because the Internet is a global thing and it is a free thing button and, it’s freezing, so I think we once recorded, it’s actually a reported case of</i>
	<i>some student trying to visit some pornographic sites. Yes, and then that was reported and since the act was caught, we try as much as possible to take a step in that direction to see how much of it we can stop within that period. The other ones that are not too visible are some form of attack in the area of trying to break into the network, but this is physically not possible because of some of the security features that we have put in place.”</i>

6.2.3 Challenges of students’ cyber behaviour on the integrity of the university

Participants were asked to state the challenges that they could attribute to students’ cyberethical infractions, as it affects the services provided by their sections and the overall teaching and learning purposes of the university. They gave the following reasons: 7 (50%) - students’ unethical behaviour has decisive effect on the image and integrity of the university; 5 (36%) - policies on ICT are not fully implemented; 6 (43%) - lack of appropriate structure to deal with cyberethics misuse behaviour, lack of regulations and

enforcement to address these various challenges, and the sections are in the learning process and often take reactive actions after violations. Other challenges mentioned by participants are lack of adequate working knowledge of cybertechnology, lack of experts or organised and professional system for faculties to handle cyberethics teaching.

Table 6.5 below shows the comments that provide evidence on the challenges created by students' cyber behaviour that affect the integrity of the university.

Table 6.5: Comments on Challenges of Students' Cyber Behaviour on the Integrity of the University

Participants	Response
UZ1	<i>"...you should realise some of these items that students download are large files (video, films and software) [and] put a still on the network, so you find out that those who want to use Internet for academic purpose are finding the Internet very slow now because 100 of students are or may be downloading music or watching films on the YouTube and so you often get complaints from other legitimate users saying the Internet is slow and what not...."</i>
UZ 2	<i>"...-students are stubborn; they hardly adhere to simple rules of engagement on university network. I would say because you wouldn't tell me that when you are logging into the lab computer for more than six months and there is something written and you always click okay but when someone confronts you, you tell the person you didn't know. I would think above anything is just ignorant. When you enter the lab, you will see a big chart there"</i>
UZ 3	<i>"...-when cybertechnology are used by anyone on the university network, it is the university identity in form of the IP that goes out in terms of somebody accessing something from this network, so in terms of movies and others, for instance if movies and music companies found out that students download movies on the university network, somehow it has impact on the image and identity of the university."</i>

FUNAAB 1	<i>“...if you're happened to be attacked by some of these unethical cyber violations by students, one of the things that can happen is that maybe your IP might be blacklisted and then you may not be able to have access to some, um, research materials online as you are supposed to, and other thing that could happen is that if they tapped into your network, definitely, they introduce all kind of viruses and Trojans that can often break down your entire system and then it becomes vulnerable to so many attacks or it can even destroyed the whole of your database.”</i>
FUNAAB 2	<i>“If we are supposed to be an educational institution we should find academics within the institution engaging educational useful resources that has high impact factors that will add to what will eventually determine the ranking of that university, and you now find students who are higher in population in such university engaging in unethical use of such technology like hacking, phishing etc. Don't be surprise that such acts will results in negative scores for the university and so will bring down and when such is discovered, the university system is penalised because content that are copyrighted to a particular university. When you find student sharing that content indiscriminately also rub on the integrity of the university.”</i>
FUNAAB 3	<i>“Yes, I would say yes because information is power and once it is something that can have strong negative or positive effect on the integrity of the university and students are having access it can surely have implication on the integrity and reputations of the university.”</i>
FUNAAB 4	<i>“...the second issue then was that we do not have enough working knowledge of cyber technology infrastructure by the time we were putting up the draft of our policy. What I mean by that is that we are limited by what was obtainable within our own environment but what we later find out was that we needed to have made more consultations, most especially outside the university and our country to see what is obtainable in highly rated institutions in the world which could have given us more references to come up with near perfect policy.”</i>

6.2.4 The impact of the use of information technology policy in strengthening or promoting compliance with ethical conduct in cyberspace in the two universities

As an important educational mission, the two universities under investigation have adopted regulations to proscribe certain activities and impose sanctions for violations in the bid to manage the use of cybertechnology on campus. However, the restriction and control of these services and facilities to forestall loss of integrity, prevention of unethical use, protection of right of other users, and the integrity of the cyber physical facilities continue to evolve to strengthen and promote compliance with ethical behaviour on the network of these universities. The above are well stated in the FUNAAB ICT Policy (2013) and the Computer Lab Rules (2015) of the University of Zululand. When asked about a written policy regarding the appropriate use of cybertechnology, the participants - 12 out of 14 (86%) - were unanimous in the view that there is the absence of ethical users acceptance policy; 4 (26%) of the participants from Unizulu believe the policy of the university is due for review; 4 (26%) of the lab assistants also said there were rules and regulations guiding the use of university personal devices (computers, laptops, smartphones, tablets). What was apparent in FUNAAB's ICT policy was that it was without a clear guidance on ethical use of cybertechnology by the students. Included in this section are questions on whether the university has a written policy on appropriate use of cybertechnology, the limiting factor for non-availability of cyberethics, how cyberethics policy can be aligned with the mission and purpose of higher education or the overall mission of the university, the best way to communicate the policy to cybertechnology users within the community, and how the university monitors and enforces compliance with ethical use of cybertechnology.

Questions, 8, 9, 10, 11, 12 and 13 in the interview guide investigated this issue.

The table below presents the comments that provide evidence on cyberethics policy in strengthening or promoting compliance with ethical behaviour on the universities' network.

Table 6.6: Comments Regarding Policy on Ethical Use of Cybertechnology on Campus

Participant	Response
UZ 1	<i>"...not that I know of. I think we are still trying to put that in place."</i>
UZ 2	<i>"It is on the university website. There is user access policy in terms of what is permitted or allowed on the university devices and what is not."</i>
UZ 3	<i>"I heard that health and safety do have policy and to send people for training. The staff will in turn educate others."</i>
UZ 4	<i>"... we do have policy but my answer to that I won't say yes or no because we do not have a director, but we do have policies guiding the activities of the section."</i>
FUNAAB 1	<i>"Yes, I think the university has."</i>
FUNAAB 2	<i>"Yes, we have ICT policy, where there in you have regulations on ethical use of the devices that are connected to the university network, the attitudes and behaviours that are allowed are also spelt out."</i>
FUNAAB 3	<i>"I know the university at some time approve internet policy but what I am not sure about is the clauses on ethical use of cybertechnology within the policy."</i>

Table 6.6: Comments Regarding Best Ways to Communicate Cyberethics Policy

Participant	Response
UZ 1	<i>"...we are still working on that, so that whatever cybertechnology devices that will be accessing the network of the university, firstly, will go to a page to ... it won't be mainly to inform about ethical use but to also ensure that the software that are installed on such devices are genuine, licensed and updated."</i>
UZ 9	<i>"It should be design in such a way that it comes up as prop up page before they can navigate into any academic activities online within the campus."</i>
UZ 8	<i>"What I think is that all these platforms that students need to visit all the time as students on campus must be embedded with these forms of ethical use of cyber technology information and there could also be options for them to consent before they move on to the next level of the applications on the platform."</i>
UZ 10	<i>"Unfortunately, I don't think there is any other best way that I can think of communicating to these people because the only thing they do is listen to music, watch video, and you wouldn't waste time and money creating video instruction to inform or educate them on ethical use of these items. To me that would be a waste of time."</i>
UZ 13	<i>"The policy should be made available and accessible to users on all devices when they connect to the network of the university and it should make clear the pros and cons of adherence be made known."</i>
UZ 12	<i>"Students nowadays are more attuned to their devices so if you need to get something across to them you have to tailor your messages towards these various online platforms that they can thus access through their cyber technology devices. At any instance there should be a form of introductory notes informing them about cyberethics and what they need to know about ethical use of their devices on campus."</i>

FUNAAB 3	<i>“The simple channel is still the same is through the university website, that is, in fact, it should be the first point of call if the required infrastructures are there. You know, ordinarily if we want to drive ICT to the degree it should go, you know, most of the things that we do, even our staffs and students when you get on campus, definitely there must be information for you on the site. So the site should be your first point of contact.”</i>
FUNAAB 2	<i>“Awareness, whether electronic or hardcopy, when talk about the awareness, if I have to browse the school site, which is one of the most visited sites in this community, if there can be a portion in form of electronic carver showing the ethical use of cyber technology that is the electronic part. There is a hard copy of the magazine that goes on almost every Friday within the community. It is released every week. With such magazine and circulation and distribution strength, there is a need for a repeated input from the ICTREC to publicise the policy and to equally sensitise the community on ethical use of cyber technology.”</i>
FUNAAB 1	<i>“If students are properly informed and educated in their earlier years in the university on cyberethics issues, it may go a long way for such university to achieve the purpose of teaching and learning with morality. I think regular orientation is very necessary.”</i>
FUNAAB 4	<i>“The university must first verify the level of awareness of the existing policy by creating a forum to appraise the adherence to the policy through an interaction forum with the student. This way the policy assessment will push to confirm understanding.”</i>
FUNAAB 5	<i>“Through the web interface of the university, university social media page, since most students will at one time or the other visit these webpages daily, such medium will be a best opportunity to re-orientate them on what is allowed and frowned at on the university network and campus.”</i>
FUNAAB 6	<i>“Hardcopies of the policy should be made available and distributed to the students through student representatives. The community radio is another</i>

	<i>medium and lastly modules should be developed to educate students on the ethical behaviour either in cyberspace or within the university generally and beyond.”</i>
--	--

6.3 Summary

This chapter presented the results from the interview data, which were collated under four themes, and more specific variables that are related to the research questions. Evidence provided in this chapter did indicate the presence of cyberethical infractions in the studied universities. The findings also revealed some challenges resulting from cyberethical practices of students. Based on the responses from the interview participants, it can be deduced that universities provide cyber connectivity to ease the educational functions of teaching and learning and knowledge dissemination and internationalisation, and to ease the traditional task of research between the stakeholders in the academic community and the external community. Despite the important functions of cybertechnology to the university community, the universities provided access but with some restrictions. Although Unizulu provides complete 24/7 all-round access, results from FUNAAB show limited and regulated access for users on their network.

Findings from the data also show that the two universities employed the use of filters and software to block-off unauthorised access and the use of non-educational and copyrighted websites like pornography, gaming and gambling sites from their network.

Furthermore, the findings also show that rules and ethics guiding the use of the university computer labs are provided to the students on pop up pages at Unizulu but there is need for hard copies of the policy on cyberethics for the generality of the students. Perhaps this shows that the institution still lacks proper coordination on ethical conduct on the university's cyberspace. One of the reasons might be that implementing such policies could be difficult. The result from FUNAAB indicated the availability of an ICT policy but physical copies are almost not also available to the generality of students.

The next chapter of this thesis will discuss the findings from the survey and the interviews. The findings will be interpreted and discussed against the available data in the earlier chapter and the current one.

CHAPTER SEVEN

DISCUSSION OF THE FINDINGS

7.1 Introduction

This chapter presents the discussion of the findings reported in chapters five and six. The discussion is guided by the contextual setting, which is presented in Chapter One, the theoretical framework in Chapter Two and the literature review in Chapter Three. The study sought to examine the cyberethical behaviour of undergraduate students at University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria. The study adopted the Theory of Planned Behaviour and has addressed the research questions presented in Chapter One of this study.

The discussion of the findings has been organised according to the research questions. The chapter begins by discussing the background profiles of the respondents, followed by the details on the issues reported in the last two chapters.

7.2 Social Demographic of the Respondents

Research objective 1: To determine the influence of demographic characteristics on cyberethical behaviour of students

The findings revealed that more respondents from FUNAAB, with 192 (51%) more than Unizulu which has 188 (49%), participated in this study. This could be explained by the disparity in the population of undergraduate students in the two institutions, as has been highlighted in section 4.8. It was also revealed that majority of respondents from South Africa were female (44.7%), while in Nigeria, males were the highest respondents. The highest respondents of females in South Africa can be attributed to the fact that the country has a higher number of females compared to males. This submission supported the finding of the South African Council on Higher Education (2016) which revealed that educational enrolment in higher institutions is in favour of females compared to males. It gives statistical credence to support the fact that females constitute 51% of the total enrolments of students in the universities in the country. A critical examination of South African population revealed that there are more females (50.90%) compared to males. This may be the reason why there is a high number of females compared with males in the studied

university.

In Nigeria, there are 112 (58.3%) male participants and 80 (41.7%) females. This revealed that there are many males in the university. According to a statistical report of the Joint Admissions and Matriculations Board, which is the highest board responsible for students' admission in the country, in the year 2008, about 598,667 males and 455,393 females were given admission to study in various universities in the country.

Another interesting finding from the study is that the age range of participants from the two universities was 21-25 years: 110 (58.5%) for the University of Zululand and 125 (65.1%) for the Federal University of Agriculture, Abeokuta, Nigeria. This can be attributed to the following reasons: (i) young adults between the age group 16 to 24 are the most avid internet users; and (ii) higher education students, who are usually aged between 18-25 years, belong to this age category. According to Statista (2015), a survey on the daily internet usage by young adults in the year 2014 showed that 73% of people in the 16-24 years category are avid internet users. This age bracket is also valuable and considered in information technology parlance as "millennial". They are so referred because of their early exposure to the development and utilisation of cybertechnology, and their opinions on cybertechnology behaviour are more malleable in the discussion of cybertechnology misuse within the context of the university.

Cilliers (2017) in his study on the evaluation of information ethical issues among undergraduate students in a university in South Africa also confirmed in his report that 77% of those between the same age range. The finding of this study supported Adeoye and Adeoye (2017) in their study on digital information skills among undergraduates in Nigerian universities, which revealed that majority of undergraduate students were between 21-25 years of age. This may be due to the country's policy on education that stated that students can only be allowed admissions from 18 years and above (National Policy on Education, 2016).

The findings on cybertechnology skills of the students revealed that majority are of intermediate proficiency at the University of Zululand, with 117 (62.6%), while at Federal University of Agriculture it was 114 (59.4%). Most students who are digital natives are not new users of cybertechnology; therefore, it is favourable to understand practical situations of students' attitude and behaviour through the appraisal of their skills. This is

also in line with the findings of Aderonmu, Aasheim and Rutner (2013), who affirmed in their assessment of the ethical perceptions of information technology and information systems students that the skills and knowledge of cybertechnology of students tend to increase as they progress in their studies in the university. Cybertechnology skills in this study include the user's ability to use a computer, tablet or mobile phone, send email, browse the Internet, make a video call and other sundry daily utilities of the devices.

The results reveal a variation in significance in the relationship between the demographic variables and the variables in the types of cyberethics misuse behaviour of undergraduate students in the two studied universities.

The results in section 5.2 have shown that, overall, unethical behaviour relating to the use of information technology is influenced by demographic variables and variables in the cyberethics misuse behaviour. The variables identified to influence undergraduate cyberethics misuse behaviour were tested, using appropriate statistical methods, in order to check their significance. The results reveal a moderate strength of association between the course of study and cyberethics misuse behaviour. However, the most significant variables that had strong relationships with cyberethics misuse behaviour of undergraduate students in relation to cyberethics misuse variables were demographic characteristics. The findings of this study show that the rate of cyberethics infringement behaviour of university undergraduates was affected by course of study, gender, age, year or level of study, cybertechnology skills and cybertechnology use experience. However, the most significant variables in South Africa that had strong relationships with these demographic characteristics were: cyberpiracy, accessing inappropriate or illegal online materials, privacy violation, cyberstalking, cyberbullying, cybersex or pornography. In Nigeria, the study reports cybersex, cyberfraud, cyberpiracy, hacking and cracking as the major significant variables that correlate with the demographic characteristics. Other specific variables were noted not to have significant influence on the study. This reveals the expanded task that the management of these institutions, through their various ICT sections, could execute to deter misuse behaviour.

The findings are congruent with Hovav and D'Arcy's (2011) study which identified that factors such as age and gender differ significantly in information technology misuse between their U.S. and Korea respondents. Liyanagunawardena and Samarasinghe (2008)

also noted key factors that influence misuse behaviour in Sri Lanka to include skills and knowledge of access. Stylianou, Winter, Niu, Giacalone and Campbell (2012) came up with factors such as age, education, work experience, year of computer use and gender as key unethical information technology practices of users in their study. Lau and Yuen (2014) also noted key demographic variables of gender and socio-economic status of respondents in their study of internet ethics of adolescents in Hong Kong. The results of this study are also in line with the one by Ndubueze, Igbo and Okoye (2013) in their analysis of socio demographic correlates of cybercrime victimisation in Nigeria, in which they identified age, gender, marital status, level of education, and occupation as factors that induce cybercrime. The finding, however, differs from that of Iyadat, Iyadat, Ashour and Khasawneh (2012) whose study reported that gender and academic level had no impact on students' awareness of ethical use of computer. The results of this study indicate that there is either a weak or lack of coordination in the sections that take care of the variables that induce cyberethics misuse behaviour. Others, like Lau and Yuen (2014), have shown that through proactive coordination, university management can facilitate the availability of information on demographic characteristics to enable the ICT sections in their various universities to make timely and credible ethical security decisions.

7.3 Respondents' Level of Awareness of Cyberethical Issues

Research Objective 2: To determine undergraduate students' awareness of cyberethics at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria.

The basis for eliciting respondents' opinions on the level of their awareness of cyberethics misuse behaviour is to determine their consciousness and knowledge of cyberethics misuse issues as highlighted in the survey instrument (Ajzen, Joyce, Sheikh and Cote, 2011). Awareness is the extent of the consciousness of the cybertechnology user about the innovation embedded in the devices. Awareness is also seen as an antecedent of attitude construct and the eventual formation of intention before behaviour. Ethical awareness is also one of the frequently cited models of software piracy by Wagner and Sanders in their model of ethical decision-making process of software piracy, based on general ethical decision-making theory (Wagner and Sanders, 2001). Consequently, it can be inferred that a positive awareness of cyberethics misuse behaviour by an individual is a likelihood that

such individual may engage in cyberethics misuse behaviour.

The field of computer science is a constantly changing environment (Moor, 1985); hence, there is a need for all users of cybertechnology to be aware of the effects of their actions on others. They need to develop and continually update their awareness so that they can identify and address the new dilemmas that cybertechnology will present. Lack of cyberethical awareness has been attributed to ethical dilemmas in cyberspace (Kuan, Idrus, Muton, 2015). This raises the question of how this awareness can be stimulated and how present and future undergraduate students can be prepared to face this challenge. Therefore, most universities and other higher learning institutions stress the need to create awareness among their students about the importance of sustaining ethical conduct in the use of cybertechnology within the cyberspace of their institutions (Isa, Samah and Jusoff, 2008).

As a key priority in the studied institutions in South Africa and Nigeria, the universities, in their network and cyberspace security effort, have put in place awareness and training programmes for freshmen during the universities' annual orientation exercise. Existing research recognises the critical role of education of students in addressing the ethical issues that emerge from the deployment of cybertechnology. However, the options to cyberethical dilemmas that are provided by academics in most institutions rarely provide the real-world guidance needed by undergraduate students after graduation. A study by Nafstad (2003) suggested technology ethics courses taught in institutions of learning tend to deal primarily with codes of conduct, and often lack any relevance to real life. She concludes that cyberethics in the context of education and awareness should be concerned with the recognition of ethical values and assumptions, and the development of ethical competence and sensitivity. From the short review above, key findings emerge: awareness is an important determinant, directly and indirectly, of cyberethics misuse behaviour, and the higher the awareness of cyberethics misuse behaviour, the higher the cyberethics behaviour practice (Galvez and Guzman, 2009).

From the responses to the questionnaire, it can be seen that the level of awareness of cyberethics in the two studied institutions is very high, which is an indicator of students' level of consciousness and knowledge of cyberethics misuse behaviour. A priority for any institution to secure its network and cyberspace is to create and increase awareness and

education, for a broad understanding of the implications of cyberethics misuse behaviour. Hence, emphasis should be laid on education and training exercise for students who will be starting their careers as cyber professionals so that they can explore, in depth, both the conceptual aspects of cyberspace, as well as receive hands-on experience on the tools and techniques of the field (Schweitzer, Gibson, Bibighaus and Boleng, 2009).

Results from this study showed that cyberethical indicators such as cyber piracy, pornography, privacy violation, dissemination of fake news, cyberstalking, hacking, cyberbullying, identity theft, violation of software licence agreement, cyber smearing, copyright violations and the use of another person's password were the most common forms of cyber practices of students. It was also revealed that 82.2% of the respondents were acquainted with cyberpiracy in Nigeria, while 84.4% were highly aware in South Africa. Pornography was 82.3% (Nigeria) while 73.5% of students were fully acquainted with the same indicator. This finding indicates a high awareness of the respondents on cyberethics misuse behaviour.

In addition, the level of awareness of cyber fraud is higher in Nigeria (75%) than among South African respondents (62.8%). It can be inferred from the results that there is a high level of awareness of cyberethics misuse behaviour among students and, consequently, a higher level of cyberethics behaviour practices. The reason for this higher awareness may be due to constant media and news events on the issues of cybercrimes. Similarly, Mayer, Kuenzi, Greenbaum, Bardes and Salvador (2009) found that students have become accustomed to seeing unethical behaviour by many who could have been role models. A case in point in South Africa is the sex scandal surrounding Malusi Gigaba, a cabinet minister, of whom a classified video clip went viral on social media (Rensburg, 2018). The implication is that students and young adults learn by example.

This supports the work of Adetimirin (2017) that the level of awareness of cyberethics varies. This agrees with the work of Akbulut et al (2008) and Beycioglu (2012) that university students are aware of indecent use of cybertechnology. The findings of this study contrast with the following studies: the work of Gan and Koh (2006), that students are not aware of cyberethical misconduct; the work of Moor (2004), that students lack the understanding of ethical issues and the awareness and use of cybertechnology; the work of Marks and Rezgui (2009), that students show deficiencies in their level of awareness

and knowledge of university cybertechnology policy; and the study by Lee (2010), that there is low level of cyberethics among his study participants in South Korea. Could it be that cyberethical awareness has improved significantly during the last eight years and/or there are some hidden cultural variables?

The survey results revealed that the level of awareness of respondents on cyberethical indicators is very high. This finding was corroborated by the ITS and ICTREC staffs of the two universities, who confirmed that their students were aware of the cyberethical indicators and that awareness creation and education have become the institutions' top priorities. This is with the view to developing and sustaining best practices and consistent models of appropriate cyberethical behaviour, both offline and in cyberspace. However, the recognition of cyberethics misuse conducts does not provoke moral outrage, as further evidence from the qualitative data shows that students do engage in ethical violations like cyberpiracy and cyberporn on the Internet even when they are aware of Internet piracy issues and regulations in the university.

A similar conclusion was reached by Moor (2006). He investigated the ethical decision-making model with a sample of information studies students in Hong Kong and discovered that moral recognition does not influence students' ethical judgments and intentions. Overall, these findings are in accordance with the findings reported by previous related studies (Masrom, Ismail and Hussein, 2009; Alhaleem, Eltayeb and Osman, 2010; Aliyu et al., 2010; Williamson, Clow, and Walker, 2011; Kim and Park, 2014; Verrecio, 2016; Adetimirin, 2017; Oyewole, 2017). The aforementioned researchers all reported a high level of awareness of issues associated with cyberethics by their studied respondents. Abolarinwa, Tihamiyu and Eluwa (2015) examined computer ethics and security awareness behaviour, with special focus on tertiary institution undergraduate students in south-western Nigeria. The foregoing study differs from the current study in that a descriptive method was adopted, and data was gathered randomly from 520 students. The study, however, agrees with the present study on the high level of awareness of computer ethics security behaviour.

Similarly, Oyewole (2017) conducted an empirical study to determine the level of awareness and perceptions of computer ethics by undergraduate students of a Nigerian university. The study revealed a high awareness of hacking, internet libel, child

pornography, cyber stalking, cyberbullying, copyright and software theft, digital plagiarism, copyright infringements, and identity theft as the most predominant ethical issues in cyberspace. Oyewole's (2017) study is different from the present study in that the findings and samples were limited to data obtained from 292 students. In addition, survey questionnaire was the only data collection instrument. This is likely to bring about a biased outcome, as other approaches and respondents within the academic community, who are also major stakeholders, ought to be included in determining the cyberethical behaviour of the learned community. Adetimirin's (2017) study was conducted with samples drawn from postgraduate students studying library and information science in some selected Nigerian universities, and her study also corroborated the high level of awareness of cyberethics among the study respondents.

The results from this study run contrary to a related study conducted in South Africa on cyber space, cyber awareness and cyber security by the Council for Scientific and Industrial Research (CSIR) and the University of Venda (2012), which shows that the study respondents from the local communities were not aware or conscious of the negative implication of cybertechnology misuse behaviour. Chandarman and van Niekerk (2017) studied cyber awareness at a private tertiary educational institution and revealed the need to address the specific weakness in the level of awareness of specific populations of users of cybertechnology in order to improve their level of consciousness and knowledge of personal security. Other attributes of cyberethics awareness as argued by von Solms and van Niekerk (2013) is in the interrelationships of knowledge, self- perception of skills, actual skills and behaviour and attitudes. On another perspective, a study by Cilliers (2017) on some public higher institutions in South Africa reported that students were aware of software piracy but felt that it was not unethical to copy software from the Internet. They equally felt that it was unethical to engage in intellectual violation in the use of cybertechnology.

Studies conducted by the Council of the European Union (2015) and other developed countries on the awareness of cyberethics misuse behaviour also support findings of the current study on the cyberethics misbehaviour of undergraduate students at the University of Zululand and the Federal University of Agriculture, Abeokuta, Nigeria. For instance, a project conducted by the data protection and cybercrime division of the European Union

in order to ensure a comprehensive response to cybercrime and other cyber offences involving the use of cybertechnology and electronic evidence has led to a greater awareness of cybercrime by the decision-making body of the union. The important achievements of the project include raising awareness, improving cooperation and bringing about legal reforms, training and establishment of network.

Results from several other studies in different contexts are comparable to the findings in this study. For instance, Sponaugle (2008) assessed undergraduate students' perceptions of ethics instruction in a computing curriculum in a university in the United States. The findings from the self-reported student's research indicated as follows: the pedagogical methods used in the course was instrumental in increasing the awareness of ethics in computing; the four-step analysis approach for decision-making was instrumental in increasing awareness in ethics; and, exposure to the computer ethics course increased the importance of ethics in computing. This is in line with the contextual findings in this study as earlier elucidated in the contextual section 1.2.1. where it was observed that cyberethics tends to be taught in the context of the broader course module in information ethics offered at the undergraduate level in the department of information studies at the university in South Africa (Ocholla, 2009). It must also be noted that course instruction on ethical conduct in cyberspace of the university was, however, not available in the studied Nigerian institution. Kim and Park (2014) also examined the intrinsic and extrinsic factors impacting individuals' cyberethics awareness and behaviour intention in order to understand the compliance with cyberethics by internet users in Korea. The results showed that self-esteem, moral obligation, self-control, cyberethics education and social influence are significantly related to cyberethics awareness. The findings from this study, however, differ from the Kim and Park study, as the perception of undergraduates about cybertechnology ethics in this study was not very highly appreciated regarding the awareness about cyberethical conduct and behaviour in cyberspace of the two universities. It is important to highlight from the foregoing that higher awareness of the phenomenon of cyberethics misuse behaviour by students may not translate to their understanding of the ethical implications of their own attitude, as it is very common in most of the university campuses that more students now own mobile devices than before, and their in-class use of these devices has become some sort of distraction. It is now generally agreed that cybertechnology is omnipresent on campus and in the lives of students, and leveraging the

devices as a tool to engage students' ethical behaviour is still evolving. Past studies reveal that students still have a complex relationship with cybertechnology, for while they recognise the value, they still need ethical guidelines when it comes to their attitude and behaviour in the utilisation of same on university campuses (Dahlstrom, Eden and Jacqueline Bichse, 2014).

7.4 Types of Cyberethics Misuse Behaviours Exhibited by Undergraduate Students at the Two Universities

Research Objective 3: To identify the types of cyberethics misuse behaviours exhibited by undergraduate students in the two universities.

The in-depth interviews revealed some weaknesses in the current measures to check cyberethics misuse behaviour and evidence of some cyber infractions by students in both institutions. Therefore, institutions need to improve on relevant cyber security measures that will check unethical use of cybertechnology in their cyberspaces. It is hoped that these security measures will promote acceptable conduct when students use cybertechnology tools on and off their campuses.

While evidence and findings from the survey also revealed that students from South Africa exhibited major cyber behaviour such as cyberpiracy (software piracy: music and film downloading), cyberstalking, cyberbullying, cyberespionage, and cyber smearing (embarrassment or humiliation on social networks), students from Nigeria have higher cyberethics infringement or misuse behaviour when it comes to cybersex, privacy violation, blackmailing and disseminating junk mail, disseminating fake news, cybercrime, cyberfraud (fraudulent online banking), hacking/carding/phreaking/cracking, cybervandalism, accessing inappropriate or illegal online material, identity theft, denial of service attack, data mining (indirect gathering of personal information), cybersquatting, spoofing and phishing, violating intellectual property, and violating software license. Consequently, findings from this study propose that the existence of moderate variations in results obtained from the two universities on types of violations may be due to restriction and control access to the network at the Nigerian university, student users tend to have a less more favourable attitude towards cyberethics misuse behaviour. The findings of this study on the types of cybertechnology misuse behaviours exhibited by undergraduate

students at the two universities corroborate the works of Karim, Zamzuri and Nor (2009); Molluzzo and Lawler (2012); Martin and Woodward (2011); Tavani (2013); and Khalil and Seleim (2012) that there have been wide ranges of cyberethics misuse behaviours associated with users in colleges and universities. The findings also concur with the works of Harris and Furnell (2012) that users in the academic environment cause breaches in security with respect to the use of cyber technologies. Lau and Yuen (2014) argue that young adults, who are generally referred to as digital natives, have greater access to cyber technology and are greater consumers of information than the generations before them but that they are lacking in discerning and making the right decision when confronted with ethical dilemma. Also supported is the work of Masrom et al. (2009) with the report that there is an increase in the violation of cyberethics misbehaviour in academic environments, especially among students.

However, the findings of this study contrasted with the works of Tahat, Elian, Sawalha and Al- Shaikh (2014) that there is a low level of concern for negative cyber behaviours such as intellectual property violations. Other related studies that the findings of this study align with are discussed in the next paragraph.

The works of Hu, Xu and Yayla (2013), Thomas and Ahyick (2010) and Xu et al. (2013) report that computer hacking and digital piracy have become prevalent among undergraduate students. Also relevant are studies by Dika and Hamiti (2011), Reka and Baloghova (2014), Karim, Zamzuri and Nor (2009). A study by Lucas and Mason of generation X in Australia indicated that 34% of the users of cyber technology admitted to being guilty of unethical cyber technology behaviour. A similar pattern of results was obtained in the studies by Chatterjee, Valacich, and Sarker (2012), and Supavai (2014) that found continued evidence of indifference or unawareness of ethical conduct or implication among selected students. Chele, Lucinschi and Stefanescu (2014) affirmed that 33.3% of the students in their study admitted to accessing adult sites, and also have another false identity on the Internet. The results also confirmed the findings from the studies by Ibrahim (2016) and Ebenezer (2014) on cyberfraud and other cyberethics misuse behavior among youths in Nigeria. Their studies linked the negative phenomenon to inducible psychopathologies and socioeconomic factors.

There is a correlation between these views and other results obtained from developed economies (Weulen Kranenbarg, Holt and Gelder, 2017). The results obtained showed an extensive, non- educational utilisation of Internet-derived information, a lack of knowledge or ignoring of ethical aspects, as well as a poor implication of their actions. Typically, the boundaries of acceptable and unacceptable cyber behaviour are defined by government authorities, who develop laws around specific illegal cyberspace behaviours, and businesses which define inappropriate actions in their terms of service agreements. For instance, an individual may be in contravention of the Copyright Act, as section 27 of the Copyright Act of South Africa prohibits unlawful copying, decimation and distribution of copyrighted materials. The Nigerian Copyright Act Cap. C28 of the Laws of the Federation of Nigeria, 2004, also prohibits the illegal copying and distribution of musical or artistic work and sound recording.

It remains unclear if students are aware of this legal provision for cyberethics misbehaviour. This may explain why they carry on these vices without legal concern. On the other hand, the pervasiveness of cyberethics misuse behaviour among undergraduate students may imply that students and young adults in general are less grounded in ethical norms, and are rarely controlled by rules and ideals (Wolfe et al., 2008). A study by Iyadat, Iyadat, Ashour and Khasawneh (2012) observed that in institutions, ethical violations that are related to hacking into a computer system for illegal purposes, and other misuse behaviours, should be taken very seriously to prevent the legal implications of user violations.

It is important to note that the present evidence relies on students' level of access through mobile phones, laptop, tablets and other portable devices. While it was evident that students from the South African university have more access to these devices from their various bursaries, the students in the Nigerian university rely on their own personal finance to buy these devices. This may explain why there are variations in the types of cyber infractions engaged in by undergraduate students in the two universities. The cheapness and availability of these devices make violations and cyberethics misbehaviour easier to find among students. Other possible explanations for the cyber violations are peer pressures and other social influences.

It can be implied that the existing ethical climate facilitates undergraduate students' misuse

of cybertechnology because there is less legal and organisational sanctions that can serve as deterrents to them. Perhaps the students may not also be aware of existing institutional policies guiding the access to and utilisation of cybertechnology. These findings support the notion that exposure to the punishments attracted by the cyberethics misuse behaviour of other individuals may change the perception of others about the likelihood of being caught cheating, to acting dishonestly.

7.5 The Applicability and Impact of Theory of Planned Behaviour on Cyberethics Misbehaviour by Undergraduate Students in the Two Institutions

Objective 4: To verify the applicability and impact of Theory of Planned Behaviour on the cyberethics misbehaviour of undergraduate students in the two institutions.

Regression results indicate that the study model significantly predicts intended behaviour ($R^2 = .726$, $R^2 \text{ adj} = .524$, $F = 140.075$, $p < .000$). The theory accounted for 52.4% of variance in intended behaviour. The descriptive and inferential statistics were adopted in the analysis to determine the influence of the Theory of Planned Behaviour (TPB) on cyberethical behaviour of the undergraduate students in this study. Generally, the proposition of the Theory of Planned Behaviour states that attitude, subjective norms and PBC determine behavioural intention and, hence, predict actual behaviour (Ajzen 1991, 2013). Results from the study established that the three major constructs of the theory - attitude, subjective norms and perceived behavioural control - individually and positively significantly influenced undergraduate students' cyberethics misuse intention, which in turn significantly correlated with their engagement in cyberethics misuse behaviour.

There is a high impact of the constructs of the Theory of Planned Behaviour on the behavioural intention and, hence, the cyberethics behaviour of students. The findings showed that the joint effects of attitude, subjective norms and perceived behavioural control are significant to influence cyberethics behavioural intention of students in the universities in South Africa. Although the TPB suggests that subjective norms will influence intention and behaviour, these relationships were, however, not supported from the results obtained in Nigeria, where subjective norms were found not to be a significant variable influencing cyberethics misuse intention of students.

This finding is supported by the works of Foltz, Schwager and Anderson (2008); Cronan and Al Rafee (2008); Stone, Jawahar and Kisamore (2010); Martin et al. (2010); Baker and White (2010), in which subjective norms do not influence ethical misbehaviour in their studies. The conflicting findings may be due to students' contextual and social desirability to underreport the

influence of significant others on cyberethics misuse behaviour. They may not be too willing to accept the social influence of these groups on their cyberethical intentions. Previous works on the TPB have found a similar disconnect between subjective norms and people's actual intentions (Peng, Zhu, Tong and Jiang, 2012; Bouhnik, and Deshen, 2014). This, however, supports the work of Taylor and Todd (1995) and Armitage and Conner (2001) that subjective norms, as an independent variable, plays an ambiguous and weak role in cyber technology misuse behaviour. Alternatively, it could simply mean that due to the anonymous nature of the Internet that creates a strong feeling of the ability to act freely without fear, and independent of significant others, students may be motivated to act immorally in the quest for thrill and attention, which may simply override the impact of significant others. Another study (Ibrahim, 2016) previously found that cyberethics misuse behaviours are more often rooted in or influenced by structural or socioeconomic factors rather than influence from significant others. This may explain why Nigerian cyberethics violators, to date, have been consistently implicated in greed and money-oriented and physiological needs rather than psychosocial influence (Ibrahim, 2016; Akpome, 2015). Thus, the foregoing supports the notion that personal normative beliefs and scenarios or situations (Leonard and Cronan, 2001) might have likely influenced cyberethics misuse intention of students in Nigeria.

Overall, the results validate the TPB as a good theory that could be adopted to explain users' behaviour to commit unethical cyber acts. This supports previous findings that attitude, subjective norms and perceived behavioural control predict intention and actual behaviour. In the work of Peace, Galletta and Thong (2003), individual attitudes, subjective norms and perceived behavioural control are significant predictors of the cyber behavioural intention of users. The findings of this study concur with the works of Stone et al (2010), Beck and Ajzen (1991) and Harding et al (2007) in which subjective norm was found to be a major factor that influences the intention of students to engage in various

unethical behaviours within the university system.

In addition, there is high impact of the Theory of Planned Behaviour constructs on the cyberethical misbehaviour of students. This buttresses the work of Yousafzai, Foxall and Pallister (2010) that TPB is the best in explaining users' behaviour, which includes cyberethical behaviour. The findings showed that attitude and perceived behavioural control are significant factors influencing cyberethical behaviour among undergraduate students in South Africa and Nigeria. This reinforces the works of Al-Rafee and Cronan (2006), Bebetosi and Antoniou (2012) that attitude has influence on cyberethics behaviour.

This could support why Venkatesh and Morris (2003) noted that the Theory of Planned Behaviour has often been adopted as a major choice in studying the use of technology. This also, on the one hand, propped up the works of Peace et al. (2003), Cronan and Douglas (2008), Chatterjee et al. (2015), and Chan (2015) that attitudes and perceived behavioural control influence cyberethical behaviour of undergraduate students. However, on the other hand, the study contradicts the works of Al-Rafee and Cronan (2006), Cronan and Douglas (2008), Cronan and Al-Rafee (2008), Chatterjee et al. (2015), and Chan (2015) that subjective norm is also a significant precursor to cyberethics misuse behaviour. This contrasts the works of McCabe and Trevino (1997), and Rettinger and Kramer (2009) with the report that unethical use of cybertechnology is higher when university students perceive that their academic society encourages various forms of negative behaviour.

The results of this study also bolster the work of Ajzen (1991), Myers (1999), Snyder (2005), and Aliyu et al. (2010) that attitude towards a given behaviour influences the individual's engagement in such behaviour, which in this study is cyberethical behaviour. The above submission is in contrast with the works of Roy et al. (2016), O'Driscoll (2013), and Echebarria-Echabe (2013) in which attitude was found to be a weak variable when considering its relationship with actual behaviour. However, the works of Sabatier and Weible (2014), and Del Rosario, Lovell and Redmond (2016) revealed that the potency of the relationship between attitude towards a certain behaviour and the actual behaviour (such as cyberethical behaviour) can be improved with greater specificity. This could be the major reasons for the differences between the results from Ajzen and Fishbein (1980), Roy et al. (2016), Christopher (2010), Myria (2015), O'Driscoll (2013), Echebarria-

Echabe (2013) and that of this present study. Hence, attitude towards cyberethical behaviour is a good predictor of actual cyberethics misuse intentions and eventual behaviour among students. This propped up the work of Siegfried (2004) that university students possessed an attitude which makes negative cyberethics behaviour acceptable among their peers.

In addition, this study supports the work of Ajzen (1991; 2006), with the report that when users have enough degree of actual control over a certain behaviour, there is a high tendency for such individual to perform such a behaviour. Perceived behavioural control through simplicity of access and the students' skills in the use of cybertechnology, as shown from their experience and

amount of access guarantee by the two institutions, could well motivate students' cyberethics behaviour. Thus, the findings of this study also prop up the works of Ajzen (1998), Bandura (1991), (Ajzen and Fishbein (2010), Ajzen (2005), and Ajzen (2006) that perceived behavioural control is a major factor influencing actual behaviour. In this case, the perceived behavioural control towards cyberethics intention and eventual cyberethical behaviour among undergraduate students in this study is a positive driver of their cyberethical behaviour. The findings of this study are also congruent with the works of Abolarinwa et al. (2015), Adetimirin (2017), Cillers (2017), Akman and Mishra (2009), with the submission that developing students' ethical awareness and their understanding of the inherent ethical issues could possibly influence cyberethical behaviours of students. This result could also mean that students' views and opinions of the relative difficulty of cyberethics misuse behaviour on university campuses have no effect on their intention to be involved in these behaviours.

The work of Jackman and Lorde (2014) that perceived ethical importance, which could be related to the perceived behaviour in TPB and institutional attitudes, which could be related to subjective norms and attitudes among students, influence cyberethical behaviour. Also, the findings of this study contrast the work of Ajzen and Fishbein (2011) that subjective norm is a social pressure or perceived social pressure which could influence a given behaviour. The findings of this study also contradict the work of Bandura (1986) and Berkowitz (2005) that peers, which is a subset of subjective norms, have an influence on involvement in unethical behaviour. The difference between the works of Bandura (1986),

Berkowitz (2005) and Ajzen and Fishbein (2010) and the findings from this present study could be traced to the work of Armitage and Conner (2001) who opined that this may be due to methodological and measurement issues.

7.6 Identifying the Challenges in Efforts by Undergraduate Students to Act Ethically Correct in Cyberspace at the Two Universities

Research Objective 5: To identify the challenges in efforts by undergraduate students to act ethically correct in cyberspace at the two universities.

From the results presented in chapters five and six, numerous findings emerged. One of the major outcomes of the study is the identification of the barriers in efforts by undergraduate students to act ethically correct in the cyberspaces of the studied universities in South Africa and Nigeria (as presented in Table 5.4. and Table 6.4). Since very few studies from African institutions focused on this, most of the articles on this issue are from the global north, where the issue is well developed and has been well addressed.

The research not only focused on identifying or listing the barriers that impact the efforts by undergraduate students to act ethically correct in the studied universities in South Africa and Nigeria, but it also identified systemic barriers that have larger impact on students acting ethically correct within these institutions. Based on the forgoing, the results in chapters five and six on this objective can be grouped into personal factors and systemic barriers, and are ranked according to the extent to which they affect cyberethics in the institutions of interest.

Findings from the interview in section 6.2.3 reveal lack of appropriate structure to deal with cyberethics misuse behaviour and lack of regulations and enforcement to address these various challenges. It was also claimed that the sections are in the learning process and often take reactive actions after violations. Other challenges mentioned by participants include the lack of adequate working knowledge of cybertechnology, lack of experts or organised professional system for faculties to handle cyberethics teaching.

The findings from the survey results showed that undergraduate students in Nigeria face more challenges in their efforts to act ethically correct in cyberspace than their counterparts in South Africa. The challenges include social negative influence, ease of performing

illegal activities, lack of adequate security measures to ensure compliance with cyberethics policy, lack of adequate orientation and education on implications of ethical violations, over-loaded teaching and learning curriculum, contradiction between copyright and freedom of information, lack of cyber morality and ethical conduct in the use of cybertechnology, management bureaucratic processes, breaches in confidentiality and network security, lack of time and commitments, lack of publicised policies about misuse of cybertechnology, lack of ethical consideration and consequence of violations, lack of adequate training for teaching cyberethics, poor cyber infrastructure, financial constraints, risk of anonymity of users, and theft of copyrighted materials. Only in the area of lack of policy guidance on appropriate cyber behaviour do students in South Africa have a higher level of prevalence. This implies that Nigerian undergraduate students are more prone to various cyberethical challenges that affect their behaviour. A near-similar pattern of results was obtained by Ocholla (2009) on the challenges of information ethics in Africa, in which he also cited inadequate legislation and weak enforcement, lack of expertise, lack of space in the curriculum, unsatisfactory professional practice and complications arising from cybertechnology use, among others.

The findings of this study also cast a new light on the previous findings by the National Cyberethics, Cybersafety, Cybersecurity Baseline (2009), which also revealed that financial constraints, time commitments, bureaucratic processes and over-loaded curriculum were the challenges frustrating ethically correct behaviour of university students. Similarly, Walczak, et al (2010) in their study showed that faculties lack adequate training and understanding to teach cyberethics. They equally noted the inconsistency in policy instruments, within the academic environment, that could deal with cyberethical misbehaviour.

This bolsters the works of Mihelic (2010), Monahan (2012) and Disoloane (2010) that ethical or unethical behaviour takes place as a result of ethical dilemma, which could also be the various challenges confronting the efficient use of cyber technologies. This could be one of the major reasons why studies such as those of Vallor (2010), Zhang (2010), Calvani et al. (2012) and Plaisance (2013) noted the need for the consideration of the moral dimensions of cybertechnology usage, especially among students. This supports the work of the University of North Carolina (2014) that students are faced with various cyberethical problems occasioned by personal and situational factors that militate against acting

ethically correct in the cyberspace of the universities.

This supports the findings of Moor (1985) and Mason (1986) that most of the cyberethical challenges among users focus on privacy, accuracy, property and accessibility-related issues. Hence, the prevalence of these cyberethical misconducts is not far-fetched when one considers the work of DiScala and Weeks (2013) that establishing internet policies removes uncertainty regarding security in cyber technology usage. To this end, this supports the work of Lowry et al. (2015) that policies are generally used to mitigate the challenges of cyber technology usage, especially among students. However, when comparing the current results to those of older studies, it must be pointed out that some findings of this study are context-bound, as some issues and barriers that prevent students from acting ethically correct are peculiar to the unique socio- psychological and economic context of the two countries of interest.

7.7 Determining the Impact of Cyberethics Policy in Strengthening or Promoting Cyberethical Behaviour in the Two Universities

Research Objective 6: To determine the impact of cyberethics policy in strengthening or promoting cyberethical behaviour at the two universities.

Available literature shows that little has been done on the phenomenon of cyberethics in Africa, let alone comparing universities in Nigeria and South Africa. Results from the interviews and document analysis show the trends in two different directions: that is, proactive and reactive.

In most university settings, as opposed to any other setting and context, the restrictions are less intrusive to students, allowing them the freedom to engage in research using their personal mobile devices and the university's computers, with minimal restraints. However, the issue of cyberethics misbehaviour is broad-based in the cyberspace of academic institutions, which places the universities in an ethical dilemma situation. This has prompted most universities to establish policy guidelines to limit abuse and ensure that harmful contents are not readily available or accessible on the network of the university.

There are several strategies used by institutions to reduce cyberethics misuse behaviour. Surveillance systems and continuous monitoring are being adopted by institutions around the globe to spy on their users. The findings from this study show that the two universities

have adopted regulations to proscribe certain activities on their networks in order to checkmate misbehaviour and strengthen compliance with ethical use. Although, there are policy regulations which stipulate ethical conduct and compliance with the spirit of national and international conventions and laws (FUNAAB ICT policy, 2013), according to this observation, the availability of the policy shows no effect on students' cyberethical behaviour. With this overwhelming observation, the reality is that the policy on ethical use of the university's network is not well communicated to the students at the University of Zululand, South Africa. The interviewed staff members claimed that they were not aware of any user policy document on cyberethics. At FUNAAB, Nigeria, staff members claimed that the policy was available on the

university website, but copies were never made available to students during the university's orientation exercise. This lack of awareness and understanding of the existence of policy on ethical use may be an indication that the policy is ineffective or lacks implementation. This view

is supported by the finding from the study of Olafsson who believes that lack of awareness of guidelines in ethical institutions' policies may lead to students using personal judgements when deciding what constitutes appropriate behaviour in the cyberspace of their institutions. This finding negates those reported by Grant and Grant (2016), where hard copies of clear policy guidelines and a well-designed applied cybertechnology ethics course have been seen to produce measurable positive changes in the ethical stances of students' moral attitudes and behaviour.

Others have shown that establishment and publicity of ICT ethics policy in the university is a way to improve the concepts of justice, fairness and moral rightness among cybertechnology users on university campus (Jung, 2009).

To counter misbehaviour, universities have resorted to limiting access to non-educational sites and downloading of music and video, software or pictures. This is done under the guise of virus control, spam control, users' safety and protection of university bandwidth. One of the informants at the South African university claimed that downloading of music, software or pictures eats up the bandwidth of the connection, causing heavy downturn and network traffic. This is evidenced from the findings from the two universities. For instance, at the university in Nigeria, there is limited access to the Internet from 8am to 4pm, while

at the university in South Africa, students have unlimited (24/7) access to the network but with restriction to educational sites. This regulation is due to specific guidelines given in the form of offences and fines regarding downloading of non-educational materials. For example, it was stipulated in Unizulu that YouTube and non-academic purpose videos are prohibited. Other violations like viewing pornography, burning and downloading music, and playing games on PC attract some stipulated fines and, in some cases, the loss of access privilege. Unfortunately, most students now access the network of the university on their various hand-held devices which have no visible conditions before they could gain access.

The situation is different at FUNAAB, where there is a clear ICT policy draft (2016) stipulating conducts on acceptable use of cybertechnology. Among others things, the policy states that Internet access through the university network is not a right but a privilege. The ICTREC section is responsible for the implementation of appropriate filtering facilities for web-based and non-web-based internet traffic that may not have direct educational value, such as pornography and gaming sites. Another policy states that user's access on the university network is monitored and logged. However, these obvious stipulations do not deter cyberethics misuse behaviours and violations by undergraduate students, as affirmed by the results from the interview with ICTREC respondents. Furthermore, downloading of copyrighted items, pornography and the like can cause legal liabilities while also bringing in the risk of other threats to the university's network. It can therefore be deduced that universities that have adopted acceptable use policies may likely enjoy more productive educational usage than their counterparts.

The results from the South African university support the work of Cronan et al (2006), who found in their study of 516 students that undergraduates who have unrestricted access to computer technologies committed significantly more cybertechnology misuse behaviour. Thus, the assertion - that consistent access to cybertechnology without stipulated prohibited behaviours and practices in the university policy will influence students' misuse intention - is supported by this study. A similar pattern of results was obtained by Foltz, Cronan and Jones (2005) in their study where they concluded that mere presence of a computer usage policy does not make a difference in a university environment.

Furthermore, the findings of this study revealed that students from Nigeria received higher

orientation exercises in their first year in the university than students from South Africa. However, there is urgent need for the university managements to organise orientation and educational programmes on cyberethical issues with respect to responsible ethical behaviour and moral reasoning in cyberspace. This supports why Kortjan and von Solms (2012) and North et al. (2017) suggested the need for cyberethics education and awareness training for cybertechnology users. This would enhance awareness concerning the development of an understanding of moral reasoning and ethical use of cybertechnology and ethical behaviour in cyberspace. This is because the findings indicated some weaknesses in the current measures to checkmate cyberethical issues among students in the universities. This could be why Dadzie (2011) argues that the education of students is very paramount in enhancing the level of awareness of cyberethics behaviour.

Hence, the findings of this study also showed the need for institutions to review existing cyberethics policy to reflect clauses in cybertechnology ethics and behaviour expected from users of their networks. This observation is in line with findings from members of staff in the ICT sections in the two universities, who believe that the institutions' current policies are due for

review. This finding concurs with the works of Yamano (2014), Laughton (2008), and Chang and Lee (2011) that internet and/or ICT policy and code of ethics should be made very important in academic institutions to guide students in the utilisation of cyber technologies. This buttresses the work of Foltz, Schwager and Anderson (2008) that many university students do not use cybertechnology policies, which are supposed to guide them from unethical cybertechnology usage. This also supports the work of Livingstone et al. (2011), Sendag, Duran and Robert Fraser (2012) that lack of institutional policies and awareness of institutional guidelines were directly identified as reasons for the involvement of their study's respondents in e-dishonesty.

7.8 Summary

This chapter discussed the findings of the study in relation to the theoretical framework, literature review and results of similar studies in literature. The chapter attempted to elucidate possible consistency and inconsistency of the previous studies with the current context. The discussion pointed to demographic characteristics of the respondents and the first research question revealed that there is moderate relationship between demographic

characteristics and cyberethics misuse behaviour of students in the two universities.

The chapter also looked at the level of awareness of cyberethics misuse behaviour of the respondents, establishing that behaviour varies among the respondents from the two studied universities, but the general level of cyberethics misuse behaviour awareness is somewhat high. The types of cyberethics behaviour exhibited by the respondents were also discussed. Also included in the formulation is the determination of the influence of the Theory of Planned Behaviour (TPB) on the cyberethics behaviour of the subjects under investigation. The constructs of attitude, subjective norms and perceived behavioural control, which are the major variables in the applied theory, exacted some degree of significance and influence on cyberethics behaviour in the universities under investigation. Hence, the relevance of this theory to the study of cyberethics behaviour was substantiated. The challenges faced by undergraduate students in the attempt to act ethically correct in the cyberspace of their universities were also discussed. The

study established several personal and systemic factors that hinder students from acting ethically in their use of cybertechnology. The last discussion centred on the attempt to determine the impact of cyberethics policy in strengthening cyberethics in the studied universities.

The next chapter presents summary, conclusion and recommendations of the study.

CHAPTER EIGHT

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

8.1 Introduction

In the previous chapter, findings based on the data analysis from the quantitative and qualitative data were discussed. This concluding chapter provides answers to the research questions formulated in Chapter One. Recommendations from the study and suggestions for future studies are also presented.

The purpose of this study was to examine the cyberethical behaviour of undergraduate students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria. The specific objectives of the study were:

- To determine the relationship between demographic characteristic and cyberethics behaviour of undergraduate students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria;
- To determine undergraduate students' awareness of cyberethics indicators at the University of Zululand and the Federal University of Agriculture, Abeokuta, Nigeria;
- To identify the types of cyberethics behaviour that are prevalent in the studied universities;
- To verify the influence of the Theory of Planned Behaviour on cyberethical behaviour;
- To identify the challenges faced by undergraduate students in their efforts to act ethically correct in the cyberspaces of the two universities;
- To determine the impact of cyberethics policy in strengthening or promoting cyberethics in the two universities under consideration.

As pointed out in Chapter Six of this study, the pragmatic research paradigm was used to address the research problem. The study used the mixed-method approach with the

quantitative survey instrument of questionnaire and qualitative semi-structured interviews. The interview was used for the qualitative data collection in order to triangulate, complement and validate the

quantitative data. The respondents were drawn from two selected universities in Nigeria and South Africa. 380 valid questionnaires were returned out of the administered 450, with the Nigerian university having 192 (51%) respondents and the South African 188 (49%) respondents. 14 professional staff members in the information and communications technology (ICT) sections of the two selected universities were also interviewed to validate the responses from the questionnaire.

The reliability and validity of the research instruments (the questionnaire and the structured interview guide) were ascertained by academics and professionals in the Department of Information Studies at the University of Zululand. A pilot study was conducted among the undergraduate students of the University of Zululand to ascertain the dependability of the research instruments. 45 students responded to the research instruments with useful contributions. Cronbach's alpha technique was applied to further determine the good fit and reliability of the instrument.

8.2 Summary of Findings

This section presents the summary of the findings in line with the research objectives. The summary is subsequently used to establish conclusions and propose recommendations.

8.2.1 Characteristics of the respondents

Objective 1: To determine the relationship between students' demographic characteristics and cyberethics misuse behaviour.

In achieving this objective, this research question was asked: What is the relationship between students' demographic variables and their cyberethics misuse behaviour in the two universities?

One of the objectives of the present study was to discover the relationships between demographic characteristics of university undergraduate students and their cyberethical behaviour. Six demographic characteristics were investigated as potential variables affecting cyberethics behaviour. They were: course of study, gender, age, year of study,

cybertechnology skills and cybertechnology experience. The study found that, overall, the actual behaviour of undergraduate students in relation to cyberethics is influenced by demographic variables.

An assessment of the course of study and cyberethical behaviour characteristics or variables revealed that there was a significant association between the course of study and some specific variables of cyberethical behaviour like accessing inappropriate or illegal online material ($\chi = 29.431$, $P < 0.05$), identity theft ($\chi = 22.815$, $P < 0.05$), denial of service ($\chi = 37.472$, $P < 0.05$) in South Africa and in Nigeria, cyberpiracy ($\chi = 87.594$, $P < 0.05$), cybersex or pornography ($\chi = 52.530$, $P < 0.05$) and privacy violation ($\chi = 58.878$, $P < 0.05$). However, other variables on the list were not significantly associated ($P > 0.05$).

Furthermore, the relationship between gender and cyberethics behaviour revealed that in South Africa, there was significant associations between gender and cybersex or pornography ($\chi = 39.119$, $P < 0.05$), accessing inappropriate or illegal material ($\chi = 15.532$, $P < 0.05$), identity theft ($\chi = 16.533$, $P < 0.05$) and cyber smearing ($\chi = 20.609$, $P < 0.05$). In Nigeria, there was significant relationship between gender and cybersex or pornography ($\chi = 13.363$, $P < 0.05$); however, there was lack of association between gender and other cyberethics variables on the list.

The age of the respondents also established a moderate strength of association with cyberethical behaviour. The most significant variable that had a strong relationship with gender was hacking ($\chi = 15.769$, $P < 0.05$) in Nigeria, and no association between age and cyberethical behaviour in South Africa. The relationship between the year of study and cyberethical behaviour showed that the year of study is associated with cyberethics specific variables like cyberpiracy ($\chi = 33.770$, $P < 0.05$), accessing inappropriate illegal online material ($\chi = 26.470$, $P < 0.05$) in South Africa, while in Nigeria they was only cybersex or cyberpiracy ($\chi = 30.796$, $P < 0.05$).

Next was the relationship between cybertechnology skills and cyberethical behaviour, where the findings established that the more cybertechnology and internet experience the respondents reported having, the more likely it was that they would violate some specific cyberethical behaviours.

8.2.2 Awareness level of cyberethics indicators

Objective 2: To determine awareness level of cyberethics indicators among students at the University of Zululand and the Federal University of Agriculture, Abeokuta, Nigeria.

In achieving this objective, this research question was asked: What is the level of awareness of cyberethics misuse behaviour among students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria?

The information from the questionnaire showed that undergraduate students were mostly aware of cyberethical behaviour in the universities in South Africa and Nigeria. This was also corroborated by the interview results which established that students from both universities under investigation were mostly aware of cyberethical behaviour. The results on orientation and training revealed that most students had received training on the use of cyber technology for educational purposes in their first year in the universities.

A couple of the observations from this study are noteworthy. First, the respondents only received training on the application of computers, laptop and other hand-held devices for the purpose of learning. However, while this would help the students to understand the benefits of the devices, the implications of the negative applications of those devices to the network, which could have addressed the issues of cyberethics, were not included in the orientation programmes. The institutions' orientation programmes were too focused on technological skills and educational applications of those skills rather than give due consideration as well to the implications of the risks that could arise from cyberethical misuse behaviour: that is, the risk to the integrity of the cyber infrastructure and the image of the universities.

8.2.3 Types of cyberethics misuse behaviour

Objective 3: To identify the types of cyberethics misuse behaviour exhibited by undergraduate students in the two universities.

In achieving this objective, this research question was asked: What are the types of cyberethics behaviour exhibited by undergraduate students in the two universities?

The impressive and remarkable nature of cyber technology, which has served the students as a revolutionary medium of expression and access to globalised information, comes with new challenges. The increasingly limitless access to the Internet on university campuses has made cyberpiracy and other forms of cyber behaviour among students prevalent.

Studies have underscored the difficulty in identifying and policing cyberethics infringements, most especially where the policies and laws are flexible.

Thus, the study established the most prevalent forms of cyberethics misuse behaviour among undergraduate students in the studied universities. Cyberpiracy had the highest mean scores of $\bar{x} = 3.6$ and $SD = 1.5$ and $m = 3.6$, $SD = 1.3$ among students in Nigeria and South Africa, respectively. This is an indication that cyberpiracy is at an alarming rate in the two universities. Following this is cyber-sex behaviour, with $\bar{x} = 3.5$, $SD = 1.4$ for Nigeria and $\bar{x} = 3.2$, $SD = 1.5$ for South Africa. Next is cyber smearing with $\bar{x} = 3.6$, $SD = 1.4$ for Nigeria and $m = 3.7$, $SD = 1.3$ for South Africa. This is not surprising as several studies have underscored the prevalence of cyberpiracy and other forms of cyberethics violations among undergraduate students. It is also notable to mention that the use of cybertechnology, especially computers, smart devices and the Internet, has become a significant daily routine on most campuses of universities. The frequency of this usage has led to the escalating nature of ethical issues among students.

8.2.4 Applicability and impact of the Theory of Planned Behaviour (TPB) on cyberethics misuse behaviour

Objective 4: To verify the applicability and impact of the Theory of Planned Behaviour (TPB) on cyberethics misuse behaviour in the two universities.

In achieving this objective, this research question was asked:

8.1.1.1. What is the impact of the Theory of Planned Behaviour on the cyberethics misuse intention of undergraduate students in the two universities?

Overall, the significant levels of the results established that the three variables (attitude, subjective norms and perceived behavioural control) were individually statistically significant in influencing students' cyberethical behaviour. The regression results established an adjusted R-square value of 0.517 for Nigeria and 0.543 for South Africa. Table 5.4.2, and an F-ratio of 67.110 for Nigeria (Table 5.4.5) and F-ratio of 72.806 (Table 5.4.5). Both were significant at 0.05 level ($0.000 < 0.05$). These results indicate that the three independent variables (attitude, subjective norms and perceived behavioural control towards cyberethical behaviour) jointly (as

indicated by the R-square value) explained or predicted 51.7% of the variations on the influence of the Theory of Planned Behaviour on undergraduates' cyberethical behaviour in Nigeria, and 54.3% of the variations on the influence of the Theory of Planned Behaviour on undergraduates' cyberethical intention and eventual behaviour in South Africa.

Secondly, the standardised coefficients (Beta values), which indicated the relative strength of each factor in the prediction of cyberethical intention, showed that perceived behavioural control contributed most to the prediction of cyberethical intentions and eventual behaviour of undergraduate students in Nigeria (Beta value = .747) and in South Africa (Beta value = .601). These results implied that all the three constructs of the Theory of Planned Behaviour (TPB) exert significant contribution in predicting cyberethical intention and behaviour.

Subjective norms are important attributes when determining cyberethics intentions. Hence, it is logical to assume that reference groups, such as parents, friends or faculties that students perceive as important in their daily routines, have influential roles in their formation of cyberethics misuse behaviour. In other words, these significant others may represent the social pressure necessary to encourage either positive or negative intention towards cyberethics misuse behaviour of students. Accordingly, this research suggests targeting these important reference groups when planning a campaign strategy or creating a persuasive message against cyberethics misuse behaviour. Role models, such as parents in the home and staff members in the ICT sections or faculties in the universities, could represent a good starting point for effectively instilling negative attitudes toward cyberethics technology misuse by students.

8.2.5 Challenges faced by undergraduate students in their efforts to act ethically correct in cyberspace

Objective 5: To identify the challenges faced by undergraduate students in their efforts to act ethically correct in cyberspace at the two universities.

In achieving this objective, this research question was asked: What are the challenges faced by undergraduate students in their efforts to act ethically correct in cyberspace at the two universities?

The results established that the entire 21 challenges listed in the table are significant. The results established also that the addition of neutral, agree and strongly agree responses, when added to each of the challenges identified, result in a high percentage response for each item. The study further established that there were both systemic and personal challenges and barriers to students acting ethically correct in the cyberspaces of their universities, chief among which are: lack of appropriate structure to deal with cyberethics misuse behaviour, and lack of regulations and enforcement that will address these challenges. It was also claimed that the sections are in the learning process and often take reactive actions after violations. Other challenges mentioned by participants include lack of adequate working knowledge of cybertechnology, lack of experts or an organised and professional system for faculties to handle cyberethics teaching.

8.2.6 Impact of cyberethics policy

Objective 6: To determine the impact of cyberethics policy in strengthening or promoting cyberethics in the two universities.

In achieving this objective, this research question was asked: What is the impact of cyberethics policy in strengthening or promoting compliance to ethical conduct in cyberspace in the two universities?

The ICT policy or internet policy in Nigeria and South Africa include: the Promotion of Access to Information Act, 2000 (Act, 2 200), Copyright Amended Act (200), Protection of Personal Information (FOI) Act (2011), Cybercrime Policy (2013), Privacy and Personal

Information Protection Act (1998), Health Records and Information Policy Act (2002), Freedom of Information (FOI) Act (2011), Cybercrime Policy (2013), and the National ICT Policy (2012). These policy instruments, specifically the Policy and Procedure on Research Ethics (2013), Policy and Procedure on Managing and Preventing Acts of Plagiarism (2013), and Research Ethics Guide (2013) have been approved and supplemented by management to guide the conduct of research at the studied university in South Africa. Similarly, at the studied university in Nigeria, the university has an expanded the ICT policy. However, findings from this study indicated that the two universities do

not have a clear-cut and official code of conduct guiding ethical use of cybertechnology or cyberethics policy. Findings from the study have established the position of Da Veiga (2015:30) that policy implementation is hampered by the culture of non-compliance.

Despite the important functions of cybertechnology in the university community, the study established that the two universities under investigation provided access but with some restrictions. While the university of Zululand provided round-the-clock access, the Federal University of Agriculture, Abeokuta, had limited and regulated access for users on their network. Findings further showed the use of filtering and other software by the ICT sections of the two universities to monitor internet traffic and block inappropriate or unauthorised websites like pornography, gaming and gambling sites. However, some staff members at the university in South Africa stated that the section observes restraint in the full application of the filtration and blocking of some educational sites. For instance, while they employ control and regulations, they are at the same time conscious of the need for researchers to access different internet sites for some classified research topics bordering on sex or the study of pornography, because completely blocking such sites may impede the successful completion of such useful tasks. In other words, the researchers interested in such studies may request the information technology section (ITS) to unblock and enable access to such classified sites for the completion of such studies.

Furthermore, the findings also showed that the rules and ethics guiding the use of the university computer labs are provided to students on pop up pages at the University of Zululand, but policies on cyberethics need more articulation and implementation among the generality of students. This perhaps shows that the institution still lacks proper coordination on the implementation of ethical conduct when using the university cyberspace. One of the reasons might be that implementing such policies could be difficult considering the fact that users claim the right to access, freedom of information, right to privacy and other legal stipulations in the constitutions of the two countries. In addition, most students believe since they pay for internet services, they should have unfettered access to do whatever they want when connected to the IP and network of the university. They, therefore, view the monitoring, security and safety measures adopted by the university as violations of their right of access to digital knowledge.

8.3 Conclusions

In conclusion, though many similarities in the types of cyberethical behaviour of undergraduate students have been established between the two studied universities, there are variations in demographic characteristics, types, awareness levels and challenges regarding the nature of the phenomenon of cyberethics in the two universities. Generally, the study discovered a mild relationship between demographic characteristics and cyberethics behaviour of undergraduate students, but with some variations in the results obtained from the universities in South Africa and Nigeria. It was also found that undergraduate students, who are the major respondents in this study, are mostly aware of cyberethics behaviour indicators in the study. The study also revealed that undergraduate students are violators of some types of cyberethical behaviour.

It was further established that the constructs of the Theory of Planned Behaviour have significant

influence on the cyberethical behaviour of undergraduate students in this study. Specifically, the three variables were individually statistically significant in influencing students' cyberethical behaviour. The variables are: attitude, subjective norms and perceived behavioural control and intention. Also, numerous personal and systemic challenges were discovered as impeding students from acting ethically correct in the cyberspaces of the universities. The two universities have no supportive cyberethics policy as ethical guidelines that can be used to support the utilisation of cybertechnology on their campuses.

This study has its share of limitations. First, the study did not involve situational factors and, thus, did not fully explain why some moral philosophies did not impact ethical judgment and behavioural intentions in the ethical situations. Although most theories regard intention to commit behaviour as the most influential factor of actual behaviour, in the case of cyberethical behaviour, actual behaviour can be changed by situational factors. Therefore, future studies should include actual behaviour and situational factors in their research models. Second, the study was conducted with samples drawn from undergraduate university students. Some empirical ethical decision-making literature (O'Fallon and Butterfield, 2005) indicate that young adults give less ethical responses and that some responses may be influenced by social desirability. Lastly, the questionnaire was

worded in English, which is a second or third language for all the respondents in the study. Most of the sentences or phrases may well have been misinterpreted or interpreted in alternative ways. Some of the questions and their contexts and

subtleties may not have been fully understood and might have influenced the outcome of the study.

8.4 Theoretical Implication

The knowledge may be considered a public good when a perception of moral ethical conduct exists. This may help to expand the application of the Theory of Planned Behaviour in cyberethics research. Overall, the results of the current study emphasise the value of the Theory of Planned Behaviour in explaining different types of behaviours associated with cybertechnology users.

The findings of this study suggest a good fit of the overall model to the data. The Theory of Planned Behavior is useful for predicting different types of behaviours associated with cybertechnology use. All three of Ajzen's predictor constructs - attitude toward behaviour, subjective norms and perceived behavioural control - contribute to the predictive power of the theory. An intriguing theoretical finding was the strong role of Perceived Behavioural Control in the context of this study. While all three of Ajzen's (2006) main determinants had an influence on undergraduates' cyberethical behaviour, Perceived Behavioural Control provided the strongest prediction.

Even though a lot of research studies have been done among university undergraduate students and their ethical conducts in the use of computers, few studies have tested the efficacy of TPB in determining cyberethical behaviour among undergraduate students in the context of South Africa and Nigeria, as combined study. Therefore, this study seeks to close the gap in the literature. The study reveals that participants' attitudes toward cyberethics issues, subjective norms and perceived behavioral control significantly influence their intentions towards a given cyber behaviour. Since university undergraduate students have tendencies to engage in untoward cyber behavior, institution management should design educational programmes that would influence students' attitudes toward ethical conducts, subjective norms and perceived behavioral control. This may ultimately influence their intentions which could translate into actual cyberethics behaviour.

8.5 Originality and Contribution of the Study

The originality of this study can be viewed from the following angles of its contributions to the area of research:

1. Applying socio-psychology theory to determine cyberethical behaviour. This provides further evidence that the TPB can be applied to cyberethics research. More specifically, it shows that the TPB can be applied in the context of students from under-resourced universities, largely from rural environments and under-resourced domestic backgrounds. This is important because limited literature exists in which the TPB has been applied in such social environments and in the sampled universities in South Africa and Nigeria.
2. The study also contributes to literature by conceptualising the phenomenon of cyberethics within the context of South Africa and Nigeria, which can generate debate for further discussions on cyberethics among African scholars.

8.6 Recommendations

This section outlines the recommendations that could be implemented to bridge the gap identified in the study.

Objective 1: Relationship between students' demographic characteristics and cyberethics misuse behaviour.

The study established that there was limited association between demographic characteristics and cyberethics behaviour. Specifically, the course of study positively correlated with some specific cyberethical behaviour variables like cyberpiracy, accessing inappropriate or illegal online materials, cybersex or pornography, privacy violation in the university in South Africa, while cyberpiracy and cybersex or pornography were associated with course of study in Nigeria. Other variables were not significantly linked. Based on this, the institutions' managements should consider creating awareness.

Objective 2: Awareness level of cyberethics indicators among students at the University of Zululand and the Federal University of Agriculture, Abeokuta, Nigeria.

In order to minimise cyberethics misuse among university undergraduate students, proactive steps should be taken to increase awareness of the negative and harmful effects

of cyberethical violations. Unfortunately, it is much easier to raise awareness and educate people about cyberpiracy and intellectual property and other forms of cyberethical violations, than it is to change attitudes and beliefs. Changing attitudes is a long-term process and may require the re- evaluation of annual orientation programmes, in order to impact beliefs, opinions and attitudes. To become ethically aware, based on established finding, it is recommended that managements of the institutions ensure that ICT professionals and other knowledgeable stakeholders make students aware of security threats, negative ethical implications , the speed with which virus can spread through the institutions' cyber infrastructure, and the impact of all these on the overall image of the institutions.

It is also recommended that it should be emphasised to students that not only are cyberethics misuse behaviours becoming more frequent, but the severity with which they disrupt an institution's normal cybertechnology-dependent operations is increasing. Such persuasive indoctrination can be accomplished through cyberethics education and training. The need to educate students on cyberethics is clear, drawn from the established results of the study findings. The management of institutions should evaluate their priorities when introducing or revamping their course syllabus or curriculum, as the case may be, to include courses on ethical awareness, in order to instil a profound sense of ethical responsibility in students. University management should also strive to improve the variety of resources in order to inculcate positive and responsible use of cybertechnology by students. For example, in a situation where students share their passwords and other login details with strangers or friends, these have consequences, not only for the network of the institution, but also for the students themselves. Cyberethics education should focus on making it clear to students that such practices can lead to situations whereby malicious persons use these passwords to gain access.

Other strategies can also be used to train users on how to behave securely. Some staff participants in the study recommended using persuasive technology, such as interactive YouTube pre-recorded video designed to change users' or students' attitudes and behaviours, to educate users, rather than merely providing traditional information security instructions on creating memorable yet secure passwords.

Others have suggested the need for universities to evaluate and modify annual orientation

and cybertechnology training for students, including on cyberethics and cyberethical instructions, so that desired skills and attitudes regarding responsible and ethical use of cybertechnology on and beyond the campus can be achieved. New measures on a general education course are needed to stir or develop the proper ethical attitude, knowledge and skills in students.

Objective 3: Types of cyberethics misuse behaviour exhibited by undergraduate students. Academic institutions around the world make extensive use of cybertechnology, and often try to keep their network secure by deploying technical cybersecurity measures and policies that specify acceptable behaviour of students. The findings from this study have established that many users do not often comply with specified acceptable behaviours on the cyberspace of the university, probably because students do not know the difference between risky and acceptable behaviour. This study indicated the types of cyberethics violations engaged in by students as cyberpiracy and cyber smearing, among others. Thus, the study recommends that the institutions should educate their users on the implications of cyberpiracy and other aberrant cyber behaviours. The institutions need to adopt a more severe strategy against illegal and inappropriate digital contents on their networks.

Objective 4: Theory of Planned Behaviour (TPB) on cyberethics misuse behaviour of undergraduate students

The findings from this study identify a significant relationship between the Theory of Planned Behaviour and undergraduate cyberethical behaviour in the studied universities.

This finding implied that students engaged more with those activities that are easier to perform with their cybertechnology. The strong impact of perceived behavioural control (PBC) on cyberethical intention was observed in the results obtained from the two universities in South Africa and Nigeria. PBC, in this study, is defined as the perceived ease of a certain cyberethics behaviour, which reflects the ability of an individual to use and manipulate cybertechnology.

Since most universities aim to develop a high level of cybertechnology literacy skills in their students, such endeavour comes with a price. Although having a community of cyber-savvy and high-level ICT literates has its benefits, it could also result in the rise of cyberethical misuse of cybertechnology. Thus, some institutions have started blocking off some of the free access to all available contents in order to solve the issue of illegal access

that could bring litigation to the institutions.

Cyberethics education is particularly germane to acceptable conduct, if made campus-wide, where students can have positive influence on one another. Cyberethics awareness will be more effective if it can account for the factor of self-efficacy of cybertechnology users and provide some reward to those who adhere to ethical conduct on the university network.

The ICT sections of the universities must improve cybersecurity since the awareness of secure connection may allow students to observe cyberethics. Lastly, institutions' managements, through the ICT section, must guide critical media consumption by students, including the use of social media, because in reality most social networks do not live up to established ethical principles such as fairness or accountability, and only to a certain extent do they comply with corporate ethics (Weber, 2016:s8).

Objective 5: Challenges faced by undergraduate students in their attempts to act ethically correct in cyberspace at the two universities.

In this study, numerous challenges in the effort by undergraduate students to act ethically correct in the cyberspaces of the universities were identified. These include lack of appropriate structure to deal with cyberethics misuse behaviour, lack of regulations and enforcement to address these various challenges, inexperienced sections who often take reactive actions after violations, lack of adequate working knowledge of cybertechnology, lack of experts and professional systems for faculties to handle cyberethics teaching.

Cybertechnological innovations within the university campus have enabled access to a huge amount of information on the Internet, which has its blessings and drawbacks for both institutions and students. As a result of this, numerous ethical issues surrounding the use of cybertechnology have become a cause for concern for institutions and students. In the light of this, the study recommends that institutions should make greater effort to educate users of cybertechnology on ethical issues in cyberethics by finding room in their syllabus/curriculum to teach ethical conduct. Considering the inconsistencies in available policies, a dialogue on cyberethics among the stakeholders in the academic community is one step to overcome the identified challenges in this study. In other words, making cyberethics discussion an integral part of institutional values will likely promote ethical

development among the generality of students.

Objective 6: The role of cyberethics policy in strengthening or promoting cyberethics in the studied universities.

The institutions under investigation need to review existing policies to reflect clauses in ethical cybertechnology use and the behaviours expected from users of their networks. Such policies should also be made visible and accessible to the generality of students. Students should be informed of relevant national legislation and university policies regarding the use of cybertechnology. Institutions can adopt technological measures that can be used to prevent obvious cybertechnology breaches on their campuses. Internet traffic could be monitored by the university. Filtering certain types of data, illegal internet traffic and piracy websites may help to reduce cyberpiracy and other violations among the institution's community of young adults. Universities should create an acceptable use policy with dos and don'ts for students. Computer lab management must not only raise fines but also adopt proactive strategies to discourage unethical use of cybertechnology. A code of ethics should be provided, read and accepted by each student before surfing on the networks of the university. Internet use ethics should be taught in all faculties, especially to first year students. The technology portions of Acceptable Use Policies and other allied code of conduct should be made available to students during the annual orientation exercise. Such handbooks need to be updated yearly. Instructional contents need to be updated to reflect best practices and lessons learned. However, if these were distributed in printed form, budgets would be strained to the breaking point. Instead, updating digital formats of policy, procedure and content would allow for more frequent update. Incorporating comments and appraisal, blogs and social media forums can enrich the dialogue and provide additional strategies to address unethical cyber violations by students. This could add value to the performance of the ICT sections of the universities. Creating this dynamic digital information space may be critical to keeping up with technological changes. Policies need to be reviewed to ensure that all levels of students (postgraduate and undergraduate) understand them. The topics need to be covered more thoroughly than having a quick overview at the beginning of the year, when so many other things are distracting from the contents. It is imperative that consequences of violations are included and enforced by management.

8.7 Recommendations for Further Studies

The study on cyberethical behaviour of undergraduate students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria, was the first of its kind in Nigeria. The following research issues emerged during the study and require further investigation:

- There is need to explore factors accounting for the disproportionate use of cybertechnology by students in both universities in South Africa and Nigeria with the aim of mitigating them.
- There is need for continuous and comparative research on the impact of cybertechnology (mobile devices, laptops, etc) on users' behaviours. These behaviours are better understood if they are studied over time. A longitudinal research is recommended in order to establish patterns, behaviours and underlying implications.
- This study was based in two selected institutions in Nigeria and South Africa. A similar study should be replicated in other countries or nations in Africa.
- Analysis of available research and initiatives and/or comparative research on adolescents' ethical use of digital technology in developing and emerging countries will be a worthwhile research area to explore.
- Investigations are required to find ways of mitigating the cultural factors which stand out as key inhibitors to ethical behaviour in cyberspace and use of cybertechnology among young adults.

This study should be replicated in three to five years' time to determine if similar results would be obtained using the same research population. This is necessary due to the rapid changes in cybertechnology.

8.8 Summary

The objective of this last chapter was to elucidate on the research questions that have guided the research for the past few years. Answers to the six research questions were provided with varying degrees of fulfilment. It is intended that the purpose of this study, which is the promotion of cyberethics in cyberspace in university environments, will provide the management of the institutions involved in the study with various intervention

strategies. It is also hoped that many other further studies on cyberethics and information ethics will arise to initiate further discovery soon. Hence, it is suggested that future studies should involve situational factors, as an extension of the Theory of Planned Behaviour and empirically test the model. In the ethics literature, situational factors include moral intensity (Jones, 1991), ego strength (Trevino, 1990). Studies should not be limited to just identifying behaviours of students in cyberspace but rather to all users of cybertechnology within the academic environment. Hence, further research to examine cyberethical behaviour of postgraduate students and staff of the university should be conducted. Empirical research and evidence on cyberethics and its allied behaviours and the suitability of various cyberethics policies and training are needed to enrich the body of knowledge.

Lastly, more qualitative studies are needed to examine, at a more intimate level, how best to inform individuals in ethical and prosocial cyber behaviour. Such studies could include both observed behaviours of users and in-depth interviews of ICT staff of the institutions and cybertechnology users, which could contribute greatly to the development of useful strategies and tools for educational administrators.

REFERENCES

- Abdullah, K. U. Z. U. (2009). Problems Related to Computer Ethics: Origins of the Problems and Suggested Solutions. *TOJET: The Turkish Online Journal of Educational Technology*, 8(2).
- Abolarinwa, L. O., Tihamiyu, M. A. & Eluwa, S. E. (2015). Computer Ethics and Security Awareness Behaviour of Tertiary Institution Students in South-Western Nigeria. *Engineering Science and Technology: An International Journal (ESTIJ)*, 260-265.
- Acilar, A. & Aydemir, M. (2010). An Empirical Study on Attitudes of Future Managers and Employees toward Ethical Use of Computers. *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, 11(1).
- Acılar, A. & Aydemir, M. (2010). Students' Attitudes towards Software Piracy - The Gender Factor: A Case of a Public University in an Emerging Country.
- Acilar, A. & Aydemir, M. (2012). Exploring Gender Differences in Attitudes toward Software Piracy among Undergraduate Students in a Developing Country. *International Journal of Information Communication Technologies and Human Development (IJICTHD)*, 4(4), 1-9.
- Acilar, A. & Yoruk, D. (2010). Gender Differences in Computer Ethics among Business Administration Students. *Annals of Dunarea De Jos University of Galatic. Journal of Economics and Applied Informatics*. Xvi(2)
- Acılar, A., & Aydemir, M. (2010, April). Students' Attitudes towards Software Piracy - The Gender Factor: A Case of a Public University in an Emerging Country. In *The Eleventh ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communication Technology*, Universitat Rovira i Virgili, Tarragona, Spain, 14th April to (pp. 2-8).
- Ackermann, M. F. & Britz, H. (2006). *Information, Ethics and the Law: A Guide for Information Practitioners, Students and the Corporate Environment*. Van Schaik Publishers.
- Adam, A. (2008). Ethics for Things. *Ethics and Information Technology*, 10(2-3), 149-154.

- Adebayo, J.O & Mabawonku, I (2017). Perception and Practice of Information Ethics by Librarians in Four Higher Institutions in Oyo State, Nigeria. *Library Philosophy and Practice (e-journal)*.1574.<http://digitalcommons.unl.edu/libphilprac/1574>
- Adekola, A. & Eze, S. C. (2015). The Intellectual Property Rights in Nigeria: A Critical Examination of the Activities of the Nigerian Copyright Commission. *Journal of Law, Policy and Globalization*, 35, 56-63.
- Adeoye, A. A. & Adeoye, B. J. (2017). Digital Literacy Skills of Undergraduate Students in Nigeria Universities. *Library Philosophy and Practice*. (e-journal). 1665. <https://digitalcommons.unl.edu/libphilprac/1665>
- Aderonmu, O., Aasheim, C. L. & Rutner, P. (2013). Development and Testing of a Survey Instrument to Assess Ethical Perceptions of IT and IS Students. 2013 South-eastern INFORMS Conference Proceedings: 217-241: Southeast Institute for Operations Research and the Management Sciences. Source: <http://seinformatics.org/> <https://digitalcommons.georgiasouthern.edu/information-tech-facpubs/9>
- Adetimirin, A. (2017). Awareness and Knowledge of Cyber Ethics by Library and Information Science Doctoral Students in Two Nigerian Universities. *International Journal of Technology Policy and Law*, 3(1), 43-55.
- Agarwal, N. K., Xu, Y. & Poo, D. C. (2011). A Context-based Investigation into Source Use by Information Seekers. *Journal of the American Society for Information Science and Technology*, 62(6), 1087-1104.
- Aggarwal, C. C. (2015). Outlier Analysis. In *Data Mining* (pp. 237-263). Springer, Cham.
- Aiken, M. & Mc Mahon, C. (2014). A Primer on Research in Mediated Environments: Reflections on Cybermethodology. *Available at SSRN 2462700*.
- Ajzen, I. & Fishbein, M. (1977). Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research. *Psychological Bulletin*, 84(5), 888.
- Ajzen, I. & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behaviour.
- Ajzen, I. & Sheikh, S. (2013). Action Versus Inaction: Anticipated Affect in the Theory of

Planned Behavior. *Journal of Applied Social Psychology*, 43(1), 155–162.
[Http://Doi.Org/10.1111/J.1559-1816.2012.00989.X](http://doi.org/10.1111/J.1559-1816.2012.00989.X)

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In *Action Control* (pp. 11-39). Springer, Berlin, Heidelberg.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Ajzen, I. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior 1. *Journal of Applied Social Psychology*, 32(4), 665-683.

Ajzen, I. (2005). *Attitudes, Personality, and Behavior*. McGraw-Hill Education (UK).

Ajzen, I. (2006). Behavioral Interventions Based on the Theory of Planned Behavior. Retrieved: <http://www.heybradford.com/FormativeResearchInstructionalUnit/Ajzen%201991.pdf>

Ajzen, I. (2011). The Theory of Planned Behaviour: Reactions and Reflections. *Psychology and Health*, 26(9), 1113-1127.

Ajzen, I. (2013). Theory of Planned Behaviour Questionnaire. *Measurement Instrument Database for the Social Science*. Retrieved from www.midss.ie

Ajzen, I. (2015). The Theory of Planned Behaviour Is Alive and Well, and not Ready to Retire: A Commentary on Sniehotka, Penseau, and Araújo-Soares. *Health Psychology Review*, 9(2), 131-137.

Ajzen, I. & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice Hall.

Ajzen, I. & Fishbein, M. (2005). The Influence of Attitudes on Behavior. *The Handbook of Attitudes*, 173(221), 31.

Ajzen, I., Joyce, N., Sheikh, S. & Cote, N. G. (2011). Knowledge and the Prediction of Behavior: The Role of Information Accuracy in the Theory of Planned Behavior. *Basic and Applied Social Psychology*, 33(2), 101-117.

Ajzen, I., Joyce, N., Sheikh, S. & Cote, N. G. (2011). Knowledge and the Prediction of

Behavior: The Role of Information Accuracy in the Theory of Planned Behavior. *Basic and Applied Social Psychology*, 33(2), 101-117.

Akbulut, Y., Şendağ, S., Birinci, G., Kılıçer, K., Şahin, M. C. & Odabaşı, H. F. (2008). Exploring the Types and Reasons of Internet-Triggered Academic Dishonesty among Turkish Undergraduate Students: Development of Internet-Triggered Academic Dishonesty Scale (ITADS). *Computers & Education*, 51(1), 463-473.

Akman, I. & Mishra, A. (2009). Ethical Behavior Issues in Software Use: An Analysis of Public and Private Sectors. *Computers in Human Behavior*, 25(6), 1251-1257.

Akpome, A. (2015). What Is Nigeria? Unsettling the Myth of Exceptionalism. *Africa Spectrum*, 50(1), 65-78.

Alhaleem, A., Eltayeb, R. & Osman, I. M. (2010). Computer Ethics Awareness. Dspace Repository. Retrieved from <http://www.repository.sustech.edu/handle/123456789/3693>

Aliyu, A. A., Rosmain, T. & Takala, J. (2014). Online Banking and Customer Service Delivery in Malaysia: Data Screening and Preliminary Findings. *Procedia-Social and Behavioral Sciences*, 129, 562-570.

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D. & Zeki, A. M. (2010, December). Computer Security and Ethics Awareness among IIUM Students: An Empirical Study. In *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010* (pp. A52-A56). IEEE.

Al-Jabri, I. M. & Abdul-Gader, A. H. (1997). Software Copyright Infringements: An Exploratory Study of the Effects of Individual and Peer Beliefs. *Omega*, 25(3), 35- 344.

Alleyne, P., Soleyn, S. & Harris, T. (2015). Predicting Accounting Students' Intentions to Engage in Software and Music Piracy. *Journal of Academic Ethics*, 13(4), 291-309.

Almualla, S. (2012). Towards a Pedagogy for Teaching Computer Ethics in Universities in Bahrain. Retrieved from:

<https://pdfs.semanticscholar.org/f712/abe93cf6fcfcb8095a015303a70b63bfd8bf.pdf>

Al-Rafee, S. & Cronan, T. P. (2006). Digital Piracy: Factors That Influence Attitude toward Behavior. *Journal of Business Ethics*, 63(3), 237-259.

Al-Rafee, S. & Dashti, A. E. (2012). A Cross Cultural Comparison of the Extended TPB: The Case of Digital Piracy. *Journal of Global Information Technology Management*, 15(1), 5-24.

Anistel, I, Anistel, M. & Elmore, R. (2009). Academic Dishonesty and Intention to Cheat: A Model on Active versus Passive Academic Dishonesty as Perceived by Business Students. *Academy of Educational Leadership Journal*. 13(2), 17-25

Amirkhani, A., Vahdat, D. & Khezrian, S. (2010). The Connection between Internet Ethic and Character Pattern of Five Students. *Ethics in Science and Technology*, 5(3), 4.

Anderson, C. L. & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS quarterly*, 34(3),

Andrews, F. M. & Withey, S. B. (2012). *Social Indicators of Well-being: Americans' Perceptions of Life Quality*. Springer Science & Business Media.

Anfara Jr, V. A. & Mertz, N. T. (Eds.). (2014). *Theoretical Frameworks in Qualitative Research*. Sage Publications.

Argandoña, A. (2012). Another Definition of Social Responsibility. *Chair "La Caixa" Social Responsibility of the Company and Corporate Governance*. IESE Business School. University of Navarra .

Armitage, C. J. & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A Meta Analytic Review. *British Journal of Social Psychology*, 40(4), 471-499.

Attuquayefio, S. & Addo, H. (2014). Using the UTAUT Model to Analyze Students' ICT Adoption. *International Journal of Education and Development Using ICT*, 10(3).

Austin, M. J. & Brown, L. D. (1999). Internet Plagiarism: Developing Strategies to Curb

- Student academic Dishonesty. *The Internet and Higher Education*, 2(1), 21-33.
- Avais, M., Wassan, A., Narejo, H. & Khan, J. (2014). Awareness Regarding Cyber Victimization among Students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, 4(5), 632-641.
- Ayooluwa, K. P. (2016). Use of Web 2.0 Technologies for Teaching and Learning in Selected Federal Universities in Southwest Nigeria (Doctoral Dissertation, University of Kwazulu-Natal, Pietermaritzburg).
- Aziz, A. A., Lokman, A. M. & Yusof, Z. M. (2011). Information Technology Ethics: The Conceptual Model of Constructs, Actions and Control Measure. *International Journal on Computer Science and Engineering*, 3(6), 2580-2588.
- Baase, S. (2003). A Gift of Fire. *Social, Legal and Ethical Issues in Computing*. Prentice-Hall.
- Babbie, E. (2010). The Practice of Social Research (ed.). Wadsworth: Nelson Education Ltd.
- Bairaktarova, D. & Woodcock, A. (2017). Engineering Student's Ethical Awareness and Behavior: A New Motivational Model. *Science and Engineering Ethics*, 23(4), 1129-1157.
- Baker, R. K. & White, K. M. (2010). Predicting Adolescents' Use of Social Networking Sites from an Extended Theory of Planned Behaviour Perspective. *Computers in Human Behavior*, 26(6), 1591-1597
- Bandura, A. (1998). Personal and Collective Efficacy in Human Adaptation and Change. *Advances in Psychological Science*, 1, 51-71.
- Bandura, A. (1991). Social Cognitive Theory of Self-Regulation. *Organizational Behavior and Human Decision Processes*, 50(2), 248-287.
- Banerjee, D., Cronan, T. P. & Jones, T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics. *MIS Quarterly*, 31-60.
- Barnes, C. M., Schaubroeck, J., Huth, M. & Ghumman, S. (2011). Lack of Sleep and Unethical Conduct. *Organizational Behavior and Human Decision Processes*, 115(2), 169-180.

Baase, S. (2012). *A Gift of Fire*. Pearson Education Limited.

Bawa, D. S. & Marwah, A. (2011). Cyber Ethics – A New Evolving Area 1, 1(6), 369–381.

Bazerman, C. (2003). Intertextuality: How Texts Rely on other Texts. In *What Writing Does and How It Does It* (pp. 89-102). Routledge.

Bebetsosi, I. I. (2012). E. & Antoniou, P.(2009). Gender Differences on Attitudes, Computer Use and Physical Activity among Greek University Students. *The Turkish Online Journal of Educational Technology*, Volume 8, Issue 2, Article 6, 63-67. Accessed on Sep 01st 2016

Bear, L. (2014). 3 For Labour: A Jeet's Accident and the Ethics of Technological Fixes in Time. *Journal of the Royal Anthropological Institute*, 20, 71-88.

Beck, L. & Ajzen, I. (1991). Predicting Dishonest Actions Using the Theory of Planned Behavior. *Journal of Research in Personality*, 25(3), 285-301.

Bellamy, C. (2012). *Principles of Methodology: Research Design in Social Science*. Sage.

Berkowitz, A. D. (2005). An Overview of the Social Norms Approach. *Changing the Culture of College Drinking: A Socially Situated Health Communication Campaign*, 193-214.

Beycioglu, K. (Ed.). (2012). *Ethical Technology Use, Policy, and Reactions in Educational Settings*. IGI Global.

Blaj, E. C. (2017). On Cyber-ethical Challenges. *Agathos*, 8(1), 161.

Bloomberg, B., Cooper, D. R. & Schindler, P. S., (2011). *Business Research Methods*. 3rd ed.

London: McGraw-Hill Higher Education.

Bouhnik, D. & Deshen, M. (2014). WhatsApp Goes to School: Mobile Instant Messaging

- between Teachers and Students. *Journal of Information Technology Education: Research*, 13(1), 217-231.
- Boynton, R. S. (2004). The Tyranny of Copyright? *The New York Times*, 25.
- Brandtzæg, P. B. (2010). Towards a Unified Media-User Typology (MUT): A Meta-Analysis and Review of the Research Literature on Media-User Typologies. *Computers in Human*
- Brey, P. (2000). Disclosive Computer Ethics. *ACM Sigcas Computers and Society*, 30(4), 10- 16.
- Brey, P. (2000). Method in Computer Ethics: Towards a Multi-Level Interdisciplinary Approach. *Ethics and Information Technology*, 2(2), 125-129.
- Brey, P. (2009). Chapter Twenty Five Computer Ethics in (Higher) Education. *Computation, Information, Cognition: The Nexus and the Liminal*, 341.
- Brey, P. A. (2007). Computer Ethics in (Higher) Education. In *Computation, Information Cognition: the Nexus and the Liminal* (pp. 341-363). Cambridge Scholars Press.
- Briggle, A. & Mitcham, C. (2012). *Ethics and Science: An Introduction*. Cambridge University Press.
- Britz, H. & Ackermann, M. (2006). Information, Ethics and the Law. *Pretoria: Van Schaik*.
- Britz, J. (2013). Understanding Information Ethics. *Information Ethics in Africa: Crosscutting Themes*, 7, 1-6.
- Bryan Foltz, C., Schwager, P. H. & Anderson, J. E. (2008). Why Users (Fail to) Read Computer Usage Policies. *Industrial Management & Data Systems*, 108(6), 701-712.
- Bryman, A. & Bell, E. (2011). Ethics in Business Research. *Business Research Methods*, 7(5), 23-56.
- Bryman, A. (2012). *Social Research Methods*, 4th ed. Oxford: Oxford University Press.

- Butterfield, K. D., Trevin, L. K. & Weaver, G. R. (2000). Moral Awareness in Business Organizations: Influences of Issue-related and Social Context Factors. *Human Relations*, 53(7), 981-1018.
- Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective* (Vol. 63). Oxford: Oxford University Press.
- Bynum, T. (2008). Computer and Information Ethics. Available: <https://plato.stanford.edu/entries/ethics-computer/> Accessed 16/04/2016
- Bynum, T. W. (2006). Flourishing Ethics. *Ethics and Information Technology*, 8(4), 157-173.
- Bynum, T. W. (2008). Milestones in the History of Information and Computer Ethics. *The Handbook of Information and Computer Ethics*, 25.
- Bynum, T. W. (2011). A Very Short History of Computer Ethics. *APA Newsletters on Philosophy and Computers*, 99(2). Retrieved from <http://rccs.southernct.edu/a-very-short-history-of-computer-ethics>
- Calvani, A., Fini, A., Ranieri, M. & Picci, P. (2012). Are Young Generations in Secondary School Digitally Competent? A Study on Italian Teenagers. *Computers & Education*, 58(2), 797- 807.
- Cameron, R., Ginsburg, H., Westhoff, M. & Mendez, R. V. (2012). Ajzen's Theory of Planned Behavior and Social Media. *American Journal of Psychological Research*, 8(1).
- Capurro, R. (2008). Intercultural Information Ethics: Foundations and Applications. *Journal of Information, Communication and Ethics in Society*, 6(2), 116-126.
- Caputi, P., Hunter, M. G. & Tan, F. B. (2009). Personal Construct Theory. In *Handbook of Research on Contemporary Theoretical Models in Information Systems* (Pp. 496-515). IGI Global.
- Cargan, L. (2007). *Doing Social Research*. Rowman & Littlefield.

- Case, C. J., & Young, K. S. (2002). Employee Internet Management: Current Business Practices and Outcomes. *CyberPsychology & Behavior*, 5(4), 355-361.
- Cate, F. H. (1999). The Changing Face of Privacy Protections in the European Union and the United States. *Ind. L. Rev.*, 33, 173.
- Cavana, R. Y., Delahaye, B. L., & Sekaran, U. (2001). *Applied Business Research: Qualitative and Quantitative Methods*. John Wiley & Sons Inc.
- Cesareo, L., & Pastore, A. (2014). Consumers' Attitude and Behavior Towards Online Music Piracy and Subscription-based Services. *Journal of Consumer Marketing*, 31(6/7), 515- 525.
- Chaabane, A., Manils, P. & Kaafar, M. A. (2010, September). Digging into Anonymous Traffic: A Deep Analysis of the tor Anonymizing Network. In *2010 Fourth International Conference on Network and System Security* (pp. 167-174). IEEE.
- Chadwick, A. & Howard, P. N. (Eds.). (2010). *Routledge Handbook of Internet Politics*. Taylor & Francis.
- Chan, H. C. O. & Wong, D. S. (2015). The Overlap between School Bullying Perpetration and Victimization: Assessing the Psychological, Familial, and School Factors of Chinese Adolescents in Hong Kong. *Journal of Child and Family Studies*, 24(11), 3224-3234.
- Chandarman, R., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, 2017(20), 133-155.
- Charlesworth, M. & Sewry, D. (2009). Ethical Theories and Computer Ethics. In *Handbook of Research on Technoethics* (pp. 186-204). IGI Global.
- Chatterjee, S., Sarker, S. & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems*, 31(4), 49-87.

- Chatterjee, S., Valacich, J. S. & Sarker, S. (2012, January). Unethical Use of Information Technology: A Two-country Study. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3071-3080). IEEE.
- Chele, G. E., Lucinschi, D. L. & Stefanescu, C. (2014). Ethical Aspects of Internet Derived Information Utilization in Adolescents: The Role of Family and Education. *Procedia- Social and Behavioral Sciences*, 149, 164-168.
- Cherryholmes, C. H. (1994). More Notes on Pragmatism. *Educational Researcher*, 23(1), 16- 18.
- Chiang, L. & Lee, B. (2011). Ethical Attitude and Behaviors Regarding Computer Use. *Ethics & Behavior*, 21(6), 481-497.
- Chiasson, M., Germonprez, M. & Mathiassen, L. (2009). Pluralist Action Research: A Review of the Information Systems Literature. *Information Systems Journal*, 19(1), 31-54.
- Chiou, J. S. (1998). The Effects of Attitude, Subjective Norm, and Perceived Behavioral Control on Consumers' Purchase Intentions: The Moderating Effects of Product Knowledge and Attention to Social Comparison Information. *Proc. Natl. Sci. Counc. ROC (C)*, 9(2), 298- 308.
- Chiou, J. S., Huang, C. Y. & Lee, H. H. (2005). The Antecedents of Music Piracy Attitudes and Intentions. *Journal of Business Ethics*, 57(2), 161-174.
- Cilliers, L. (2017). Evaluation of Information Ethical Issues among Undergraduate Students: An Exploratory Study. *South African Journal of Information Management*, 19(1), 1-6.
- Clariana, M., Badia, M., Cladellas, R. & Gotzens, C. (2013). Academic Cheating and Gender Differences in Barcel. *Summa psicológica UST (En línea)*, 10(1), 65-72.
- Clarke, C. & Reed, J., (2006). Case Study Research. In: Gerrish, K., Lacey, A. (Eds.), *The Research Process in Nursing*. 5th ed. Blackwell, Sydney, pp. 302–315
- Claudy, M. C., Peterson, M. & O'Driscoll, A. (2013). Understanding the Attitude-Behavior Gap for Renewable Energy Systems Using Behavioral Reasoning

- Theory. *Journal of Macromarketing*, 33(4), 273-287.
- Clough, J. (2015). Possession of Extreme Pornography: Where's the Harm? *Canadian Journal of Law and Technology*, 13(2).
- Cohen, L., Manion, L. & Morrison, K. (2011). Surveys, Longitudinal, Cross-sectional and Trend Studies. *Research Methods in Education*, 7th edition. Abingdon: Routledge, 261-4.
- Collins, K. M., Onwuegbuzie, A. J. & Jiao, Q. G. (2007). A Mixed Methods Investigation of Mixed Methods Sampling Designs in Social and Health Science Research. *Journal of Mixed Methods Research*, 1(3), 267-294.
- Collins, K. M., Onwuegbuzie, A. J., Johnson, R. B. & Frels, R. K. (2013). Practice Note: Using Debriefing Interviews to Promote Authenticity and Transparency in Mixed Research. *International Journal of Multiple Research Approaches*, 7(2), 271-284.
- Conger, S., Pratt, J. H. & Loch, K. D. (2013). Personal Information Privacy and Emerging Technologies. *Information Systems Journal*, 23(5), 401-417
- Conner, M. & Sparks, P. (2005). Theory of Planned Behaviour and Health Behaviour. *Predicting Health Behaviour*, 2(1), 121-162.
- Conner, M., Godin, G., Sheeran, P. & Germain, M. (2013). Some Feelings Are More Important: Cognitive Attitudes, Affective Attitudes, Anticipated Affect, and Blood Donation. *Health Psychology*, 32(3), 264.
- Conner, M., Smith, N. & McMillan, B. (2003). Examining Normative Pressure in the Theory of Planned Behaviour: Impact of Gender and Passengers on Intentions to Break the Speed Limit. *Current Psychology*, 22(3), 252-263.
- Coombes, B. (2009). Generation Y: Are They Really Digital Natives or More like Digital Refugees. *Synergy*, 7(1), 31-40.
- Cooper, D. R., & Schindler, P. S. (2008). International Edition: Business Research Methods. New Delhi: McGraw-Hill.
- Corbetta, P. (2003). *Social Research: Theory, Methods and Techniques*. Sage.

- Coreil, J. (2010). Behavioural and Social Science Theory. *Social and Behavioural Foundations of Public Health*, 69-90.
- Council of the European Union (2015): Evaluation Report on the Seventh Round of Mutual Evaluations –The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime —Report on Slovakia, Brussels, 22 September 2015, 9761/1/15 REV 1 DCL 1
- Creswell, J. W. (2014). *A Concise Introduction to Mixed Methods Research*. Sage Publications.
- Creswell, J. W. (2002). *Educational Research: Planning, Conducting, and Evaluating Quantitative* (Pp. 146-166). Upper Saddle River, NJ: Prentice Hall.
- Creswell, J. W. (2008). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage Publications.
- Creswell, J. W. (2008). Qualitative, Quantitative, and Mixed Methods Approaches.
- Creswell, J. W. (2013). *Educational Research: Planning, Conducting, and Evaluating*. W. Ross MacDonald School Resource Services Library.
- Creswell, J. W. & Plano Clark, V. L. (2011). Choosing a Mixed Methods Design. *Designing and Conducting Mixed Methods Research*, 2, 53-106.
- Cronan, T. P. & Al-Rafee, S. (2008). Factors That Influence the Intention to Pirate Software and Media. *Journal of Business Ethics*, 78(4), 527-545.
- Crossman, A. (2012). Cluster Sample. Available: <http://sociology.about.com/od/Types-of-Samples/a/Cluster-Sample.htm> [2016, May 20].
- Da Veiga, A. (2015). The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*

- Dadzie, P. S. (2011). Rethinking Information Ethics Education in Ghana: Is It Adequate? *The International Information & Library Review*, 43(2), 63-69.
- Dahlstrom, Eden, and Jacqueline Bichsel. (2014). ECAR Study of Undergraduate Students and Information Technology, 2014. Research Report. Louisville, CO: ECAR, October. Available from <http://www.educause.edu/ecar>.
- D'arcy, J. & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *European Journal of Information Systems*, 20(6), 643-658.
- D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79-98.
- Davidson, J. & Gottschalk, P. (Eds.). (2010). *Internet Child Abuse: Current Research and Policy*. Routledge.
- Davies, C. B. & McKittrick, K. (2015). Sylvia Wynter: On Being Human as Praxis.
- Davinson, N. & Sillence, E. (2010). It Won't Happen to Me: Promoting Secure Behaviour among Internet Users. *Computers in Human Behavior*, 26(6), 1739-1747.
- Davis, F. D. (1993). User Acceptance of Information Technology: System Characteristics, User Perceptions and Behavioral Impacts. *International Journal of Man-machine Studies*, 38(3), 475-487.
- Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. (1992). Extrinsic and Intrinsic Motivation to Use Computers in the Workplace. *Journal of Applied Social Psychology*, 22(14), 1111- 1132.
- De Bruyn, M. (2014). The Protection of Personal Information (POPI) Act: Impact on South Africa. *International Business & Economics Research Journal* – November/December Volume 13, Number 6
- Del Rosario, M. B., Lovell, N. H. & Redmond, S. J. (2016). Quaternion-based Complementary Filter for Attitude Determination of a Smartphone. *IEEE Sensors Journal*, 16(15), 6008- 6017.

- DeWall, C. N., Baumeister, R. F., Chester, D. S. & Bushman, B. J. (2016). How Often Does Currently Felt Emotion Predict Social Behavior and Judgment? A Meta-analytic Test of Two Theories. *Emotion Review*, 8(2), 136-143.
- Dika, A. & Hamiti, M. (2011). Challenges of Implementing the Ethics through the Use of Information Technologies in the University. *Procedia-Social and Behavioral Sciences*, 15, 1110-1114.
- Dill, D. D. (2005). Are Public Research Universities Effective Communities of Learning? The Collective Action Dilemma of Assuring Academic Standards. In *Symposium: Future of the American Public Research University, Penn State University* (Vol. 25).
- Dinev, T. & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, 8(7), 23.
- Discala, J. & Weeks, A. C. (2013). Access Denied: School Librarians' Responses to School District Policies on the Use of Social Media Tools. *School Library Research*, 16.
- Disoloane, V. P. P. (2010). Enhancing Ethical Conduct in the South African Public Service. *Journal of Public Administration*, 45(3), 436-446.
- Dolliver, D. S. & Poorman, K. (2018). Understanding Cybercrime. P. Reichel, & R. Randa, *Transnational Crime and Global Security*, 139-160.
- Dömeová, L. & Jindrová, A. (2013). Unethical Behavior of the Students of the Czech University of Life Sciences. *International Education Studies*, 6(11), 77.
- Donnelly, J. (2013). *Universal Human Rights in Theory and Practice*. Cornell University Press.
- Dowell, E. B., Burgess, A. W. & Cavanaugh, D. J. (2009). Clustering of Internet Risk Behaviors in a Middle School Student Population. *Journal of School Health*, 79(11), 547-553.

- Dyck, B. & Wong, K. (2010). Corporate Spiritual Disciplines and the Quest for Organizational Virtue. *Journal of Management, Spirituality and Religion*, 7(1), 7-29.
- Dwivedi, Y. K. (Ed.). (2009). *Handbook of Research on Contemporary Theoretical Models in Information Systems*. IGI Global.
- Echebarria-Echabe, A. (2013). Mortality Salience and Uncertainty: Similar Effects but Different Processes? *European Journal of Social Psychology*, 43(3), 185-191.
- Jegade, A. E. (2014). Cyber Fraud, Global Trade and Youth Crime Burden: Nigerian Experience. *Afro-Asian Journal of Social Sciences*, 5(4).
- Edmonds, W. A. & Kennedy, T. D. (2016). *An Applied Guide to Research Designs: Quantitative, Qualitative and Mixed Methods*. Sage Publications.
- Eldakak, S. (2010). Does Applying Ethics in Education Have an Effective Impact in the Classroom? *Online Submission*.
- Ellahi, A. Mushtaq, R & Mohammed, B. K. (2013). Multi-Campus Investigation of Academic Dishonesty in Higher Education of Pakistan. *International Journal of Educational Management*, 27(6) 647-666.
- Ellis, T. J. & Levy, Y. (2009). Towards a Guide for Novice Researchers on Research Methodology: Review and Proposed Methods. *Issues in Informing Science & Information Technology*, 6.
- Engen, B. K., Giæver, T. H. & Mifsud, L. (2015). Guidelines and Regulations for Teaching Digital Competence in Schools and Teacher Education: A Weak Link? *Nordic Journal of Digital Literacy*, 10(02), 69-83.
- Ercegovac, Z. & Richardson, J. V. J. (2004). Academic Dishonesty, Plagiarism Included, in the Digital Age: A Literature Review. *Coll. Res. Libr.*, 65(4), 301–318. Retrieved from [Http://Crl.Acrl.Org/Content/65/4/301.Short](http://Crl.Acrl.Org/Content/65/4/301.Short)
- Ernst and Young (Firm) Great Britain. Office of the Deputy Prime Minister (ODPM). (2004). Evidence-based Review of Skills for Sustainable Communities. Office of the Deputy Prime Minister, London, England.

Evans, J. S. B. & Over, D. E. (2013). *Rationality and Reasoning*. Psychology Press.

Evans, J., Over, D. (1996). *Rationality and Reasoning*. London: Psychology Press,
<https://doi.org/10.4324/9780203027677>

Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*,

Falconi, T. M. (2014). Global Stakeholder Relationships Governance: An Infrastructure.
In *Global Stakeholder Relationships Governance: An Infrastructure* (pp. 1-55).
Palgrave Pivot, London

Federal Government of Nigeria. (1999). Constitution of the Federal Republic of Nigeria
1999.

Federal University of Agriculture, Abeokuta (2013). *Funaab ICT Policy*. Retrieved from:
<https://ceadese.unaab.edu.ng/download/FUNAAB%20ICT%20POLICY.pdf>

Festl, R. & Quandt, T. (2013). Social Relations and Cyberbullying: The Influence of
Individual and Structural Attributes on Victimization and Perpetration via the
Internet. *Human Communication Research*, 39(1), 101-126.

Fieser, J. (2009). Ethics. In James Fieser, Bradley Dowden. *The Internet Encyclopedia of
Philosophy*.

Fink, A. (2010). *Conducting Research Literature Reviews: From the Internet to Paper*.
Sage Publications.

Fishbein, M. & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction
to Theory and Research*.

Fishbein, M. & Ajzen, I. (2005). Theory-Based Behavior Change Interventions:
Comments on Hobbis and Sutton. *Journal of Health Psychology*, 10(1), 27-31.

Flinders, D. J. & Mills, G. E. (Eds.). (1993). *Theory and Concepts in Qualitative Research:
Perspectives from the Field*. Teachers College Press.

Floridi, L. (2010). Information Ethics. *The Cambridge Handbook of Information and*

Computer Ethics, 77-99.

Floridi, L. (Ed.). (2011). *The Blackwell Guide to the Philosophy of Computing and Information*. John Wiley & Sons.

Fodorean, D. (2018). Ethics and Law - The Role of Legal Ethics Course in the Formation of Future Romanian Juridical Professionals. *Scientia Moralitas-International Journal of Multidisciplinary Research*, 3(2), 43-50.

Folorunso, O., Vincent, R. O., Adekoya, A. F. & Ogunde, A. O. (2010). Diffusion of Innovation in Social Networking Sites among University Students. *International Journal of Computer Science and Security*, 4(3), 361-372.

Foltz, C., Schwager, P. & Anderson, J. (2008). Por qué los usuarios (no) leen las directivas de uso del equipo. *Gestión industrial y sistemas de datos*, 108(6), 701-712.

Forester, T. & Morrison, P. (1994). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press.

Fosnacht, K., Sarraf, S., Howe, E. & Peck, L. K. (2017). How Important Are High Response Rates for College Surveys? *The Review of Higher Education*, 40(2), 245-265.

Fox, M. J. & Reece, A. (2012). Which Ethics? Whose Morality? An Analysis of Ethical Standards for Information Organization. *Ko Knowledge Organization*, 39(5), 377-383.

Fraenkel, J. R. & Wallen, N. E. (2009). The Nature of Qualitative Research. *How to Design and Evaluate Research in Education, Seventh Edition*. Boston: McGraw-Hill, 420.

Frangos, C. C., Frangos, C. C. & Sotiropoulos, I. (2011). Problematic Internet Use among Greek University Students: An Ordinal Logistic Regression with Risk Factors of Negative Psychological Beliefs, Pornographic Sites, and Online Games. *Cyberpsychology, Behavior, and Social Networking*, 14(1-2), 51-58.

Frize, M. (2012). Electronic Medical Records (EMRs): Patient Safety and Ethical Considerations. *Ethics in Biology, Engineering and Medicine: An International Journal*, 3(1-3).

- Froehlich, Thomas (2005). A Brief History of Information Ethics. Computer Society of India (CSI)11e13, Available Online. [www. capurro.de/csi June2005infoeth.pdf](http://www.capurro.de/csi_June2005infoeth.pdf). Accessed 16 Nov, 2015
- Gaffar, K., Singh, L. & Thomas, T. (2011). Are We Ready for Web 2.0? Evidence from a Caribbean University. *The Caribbean Teaching Scholar*, 1(2).
- Gagne, P. & Hancock, G. R. (2006). Measurement Model Quality, Sample Size, and Solution Propriety in Confirmatory Factor Models. *Multivariate Behavioral Research*, 41(1), 65-83.
- Gallivan, M. J., Spitler, V. K. & Koufaris, M. (2005). Does Information Technology Training Really Matter? A Social Information Processing Analysis of Coworkers' Influence on IT Usage in the Workplace. *Journal of Management Information Systems*, 22(1), 153-192.
- Galvez, S. M. & Guzman, I. R. (2009). Identifying Factors That Influence Corporate Information Security Behavior. *AMCIS 2009 Proceedings*, 765.
- Gan, L. L. & Koh, H. C. (2006). An Empirical Study of Software Piracy among Tertiary Institutions in Singapore. *Information & Management*, 43(5), 640-649.
- Gattiker, U. E. & Kelley, H. (1999). Morality and Computers: Attitudes and Differences in Moral Judgments. *Information Systems Research*, 10(3), 233-254.
- Gelso, C. J. (2006). Working Alliance: Current Status and Future Directions: Editor's Introduction. *Psychotherapy: Theory, Research, Practice, Training*, 43(3), 257.
- Gikenye, W. (2012). The Diffusion of Mobile Phones for Business and Information Management in Kenya. *Journal of Gender, Information and Development in Africa (JGIDA)*, 1(1), 43- 56.
- Glanz, K. & Bishop, D. B. (2010). The Role of Behavioral Science Theory in Development and Implementation of Public Health Interventions. *Annual Review of Public Health*, 31, 399-418.
- Godin, G., Conner, M. & Sheeran, P. (2005). Bridging the Intention–Behaviour Gap: The Role of Moral Norm. *British Journal of Social Psychology*, 44(4), 497-512.

- Goel, N., Kaur, A. & Vaidya, M. (2012). Indian Youth Inclination towards Unethical Practices in the Use of Information and Communication Technology. *Pertanika Journal of Social Sciences & Humanities*, 20(4).
- Goessl, L. (2008). How Computer Ethics Impact Society. Retrieved from <http://www.helium.com/items/845336-howcomputer-ethics-impact-society>
- Goles, T., Jayatilaka, B., George, B., Parsons, L., Chambers, V., Taylor, D. & Brune, R. (2008). Softlifting: Exploring Determinants of Attitude. *Journal of Business Ethics*, 77(4), 481-499.
- Gopal, R. D., Sanders, G. L., Bhattacharjee, S., Agrawal, M. & Wagner, S. C. (2004). A Behavioral Model of Digital Music Piracy. *Journal of Organizational Computing and Electronic Commerce*, 14(2), 89-105.
- Göritz, A. S., Singh, R. K. & Voggeser, B. J. (2012). Human Behavior on the WWW. In *Encyclopedia of Cyber Behavior* (pp. 117-131). IGI Global.
- Gotterbarn, D. & Rogerson, S. (2005). Responsible Risk Assessment with Software Development: Creating the Software Development Impact Statement. *Communications of the Association for Information Systems*, 15(1), 40.
- Gotterbarn, D., Miller, K. & Impagliazzo, J. (2006). Plagiarism and Scholarly Publications: An Ethical Analysis. *Proceedings - Frontiers in Education Conference, FIE*, 22-27. [Http://Doi.Org/10.1109/FIE.2006.322365](http://doi.org/10.1109/FIE.2006.322365)
- Gotterbarn, D. (1991). Computer Ethics: Responsibility Regained. In *National Forum* (Vol. 71, No. 3, p. 26). Honor Society of Phi Kappa Phi.
- Gottfredson, M. R. & Hirschi, T. (1990). *A General Theory of Crime*. Stanford University Press.
- Granitz, N. & Loewy, D. (2007). Applying Ethical Theories: Interpreting and Responding to Student Plagiarism. *Journal of Business Ethics*, 72(3), 293-306.
- Grant, C. & Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your House. *Administrative Issues Journal*, 4(2), 4.

- Gray, E. D. (2014). *Doing Research in the Real World* (2014th Ed.). London: Sage.
- Graziano, M.A. & Raulin, L.M. (2010). *Research Methods: A Process of Inquiry* (7th ed.), Allyn & Bacon, Boston, MA.
- Greene, J. C. (2007). *Mixed Methods in Social Inquiry* (Vol. 9). John Wiley & Sons.
- Greene, J. C. & Caracelli, V. J. (2003). Making Paradigmatic Sense of Mixed Methods Practice.
Handbook of Mixed Methods in Social and Behavioral Research, 9, 91-110.
- Greening, T., Kay, J. & Kummerfield, B. (2006). Integrating Ethical Content into Computing Curricula. Retrieved February 20, 2016, from www.acs.org.au/documents/public/crpit/CRPITV30Greening.pdf
- Grube, J. W., Morgan, M. & McGree, S. T. (1986). Attitudes and Normative Beliefs as Predictors of Smoking Intentions and Behaviours: A Test of Three Models. *British Journal of Social Psychology*, 25(2), 81-93.
- Grunwald, A. (2000). Against Over-Estimating the Role of Ethics in Technology Development. *Science and Engineering Ethics*, 6(2), 181-196.
- Haines, R. & Leonard, L. N. (2007). Individual Characteristics and Ethical Decision-Making in an IT Context. *Industrial Management & Data Systems*, 107(1), 5-20.
- Halder, D., Jaishankar, K., Periyar, E. & Sivakumar, R. (2011). Cyber Victimization in India: An Empirical Analysis. In *First International Conference of the South Asian Society of Criminology and Victimology (SASCV)*, 15-17 January 2011, Jaipur, Rajasthan, India: SASCV 2011 Conference Proceedings (p. 77). K. Jaishankar
- Hamiti, M. & Dika, A. (2011, June). Challenges of Computers and IT in the Coming Decade, Case Study: SEE-University in Macedonia. In *Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces* (pp. 65-70).

IEEE.

Hamiti, M., Reka, B. & Baloghová, A. (2014). Ethical Use of Information Technology in High Education. *Procedia-Social and Behavioral Sciences*, 116, 4411-4415.

Hamsi, A. S., Bahry, F. D. S., Tobi, S. N. M. & Masrom, M. (2015). Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem. *Journal of Management Research*, 7(2), 169.

Hardigan, P. C., Popovici, I. & Carvajal, M. J. (2016). Response Rate, Response Time, and Economic Costs of Survey Research: A Randomized Trial of Practicing Pharmacists. *Research in Social and Administrative Pharmacy*, 12(1), 141-148.

Harding, D. J. (2007). Cultural Context, Sexual Behavior, and Romantic Relationships in Disadvantaged Neighborhoods. *American Sociological Review*, 72(3), 341-364.

Harding, T. S., Mayhew, M. J., Finelli, C. J. & Carpenter, D. D. (2007). The Theory of Planned Behavior as a Model of Academic Dishonesty in Engineering and Humanities Undergraduates. *Ethics & Behavior*, 17(3), 255-279.

Harris, M. & Furnell, S. (2012). Routes to Security Compliance: Be Good or Be Shamed? *Computer Fraud & Security*, 2012(12), 12-20.

Hart, C. (2018). *Doing a Literature Review: Releasing the Research Imagination*. Sage.

Hartrick Doane, G. (2003). Through Pragmatic Eyes: Philosophy and the Re-Sourcing Of Family Nursing. *Nursing Philosophy*, 4(1), 25-32.

Haughton, N. A., Yeh, K. C., Nworie, J. & Romero, L. (2013). Digital Disturbances, Disorders, and Pathologies: A Discussion of Some Unintended Consequences of Technology in Higher Education. *Educational Technology*, 3-16.

Hauptman, R. (2011). *Authorial Ethics: How Writers Abuse Their Calling*. Rowman & Littlefield.

Hayes, N. & Introna, L. D. (2005). Cultural Values, Plagiarism, and Fairness: When Plagiarism Gets in the Way of Learning. *Ethics & Behavior*, 15(3), 213-231.

- Heersmink, R., van den Hoven, J., van Eck, N. J. & van den Berg, J. (2011). Bibliometric Mapping of Computer and Information Ethics. *Ethics and Information Technology*, 13(3), 241.
- Henderson-Redmond, A. N., Guindon, J. & Morgan, D. J. (2016). Roles for the Endocannabinoid System in Ethanol-Motivated Behavior. *Progress in Neuro-Psychopharmacology and Biological Psychiatry*, 65, 330-339.
- Herath, H. M. P. S. & Wijayanayake, W. M. J. I. (2009). Computer Misuse in the Workplace. *Journal of Business Continuity & Emergency Planning*, 3(3), 259-270.
- Hikwa, L. & Maisiri, E. (2013). Information Ethics and Use of Social Media in Higher Education: Faculty Members' Perspectives. *Innovation: Journal of Appropriate Librarianship and Information Work in Southern Africa*, 2013(47), 43-69.
- Himma, K. E. & Tavani, H. T. (Eds.). (2008). *The Handbook of Information and Computer Ethics*. John Wiley & Sons.
- Holt, T. J., Bossler, A. M. & May, D. C. (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, 37(3), 378-395.
- Houser, N. (2005). Peirce in the 21st Century. *Transactions of the Charles S. Peirce Society: A Quarterly Journal in American Philosophy*, 41(4), 729-739.
- Howe, K. R. (1998). The Interpretive Turn and the New Debate in Education. *Educational Researcher*, 27(8), 13-20.
- Hoyle, R. H., Harris, M. J. & Judd, C. M. (2002). *Research Methods in Social Relations*. <https://doi.org/10.4337/9781783473250.00017>
- Hu, G. & Lei, J. (2015). Chinese University Students' Perceptions of Plagiarism. *Ethics & Behavior*, 25(3), 233-255.
- Hu, Q., Xu, Z. & Yayla, A. A. (2013). Why College Students Commit Computer Hacks: Insights from a Cross Culture Analysis. In *PACIS* (P. 104).
- Hunt, S. D. & Vitell, S. J. (2006). The General Theory of Marketing Ethics: A Revision and Three Questions. *Journal of Macromarketing*, 26(2), 143-153.

- Ibrahim, S. (2016). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44-57.
- Igwe, K. N. & Ibegwam, A. (2014). Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria. *International Journal of ICT and Management*, 2(2), 102-113.
- Imenda, S. (2014). Is There a Conceptual Difference between Theoretical and Conceptual Frameworks? *Sosyal Bilimler Dergisi/Journal of Social Sciences*, 38(2).
- Innis, H. A. (2008). *The Bias of Communication*. Toronto: University of Toronto Press.
- International Telecommunication Union (2018). *Measuring the Information Society Report 2018*. Volume 1. Geneva: ITU. Retrieved December 19, 2018 from <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf>
- Iorga, M. & Sztankovszky, L-Z. (2013). Contextual and Personal Reasons for Unethical Behaviours among University Students. *European Journal of Science and Theology*, 9, 5, 243-254.
- Isa, P. M., Samah, S. A. A. & Jusoff, K. (2008). Inculcating Values and Ethics in Higher Education E-Learning Drive: UiTM i-learn User Policy. In *World Academy of Science, Engineering and Technology Conference* (pp. 452-455).
- Iyadat, W., Iyadat, Y., Ashour, R. & Khasawneh, S. (2012). University Students and Ethics of Computer Technology Usage: Human Resource Development. *E-Learning and Digital Media*, 9(1), 43-49.
- Jackman, M. & Lorde, T. (2014). Why Buy When We Can Pirate? The Role of Intentions and Willingness to Pay in Predicting Piracy Behavior. *International Journal of Social Economics*, 41(9), 801-819.
- Jambon, M. M. & Smetana, J. G. (2012). College Students' Moral Evaluations of Illegal Music Downloading. *Journal of Applied Developmental Psychology*, 33(1), 31-39.
- Jamil, M. & Shah, J. H. (2014). Perception of Undergraduates about Computer and Internet

- Ethics in Pakistan. *Nigerian Journal of Technology*, 33(4), 512-522.
- Jamil, M., Hussain, J. & Tariq, R. (2013) IT Ethics: Undergraduates' Perception Based on Their Awareness. *Journal of Education and Practice* 4(12), 110–122.
- Jamwal, S. S. & Gupta, N. (2012). Software Piracy among IT Students of J & K: Ethical or Unethical. In *International Conference on Recent Advances and Future Trends in Information Technology* (pp. 33-36).
- Jawahar, I. M., Kisamore, J. L., Stone, T. H. & Rahn, D. L. (2012). Differential Effect of Inter- Role Conflict on Proactive Individual's Experience of Burnout. *Journal of Business and Psychology*, 27(2), 243-254.
- Johnson, D. P. (2017). How Attitude toward Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention. (Dissertation). Retrieved from:
<https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.co.z a/&httpsredir=1&article=5557&context=dissertations>
- Johnson, D. (2001). Computer Ethics, 3rd. Edition, Prentice Hall, 112-118. Johnson, D. G. (1985). Computer Ethics. Englewood Cliffs (NJ).
- Johnson, R. B., Onwuegbuzie, A. J. & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research*, 1(2), 112-133.
- Jones, D. L. R. (2011). Academic Dishonesty: Are More Students Cheating? *Business Communication Quarterly*, 74(2), 141–150.
[Http://Doi.Org/10.1177/1080569911404059](http://doi.org/10.1177/1080569911404059)
- Jones, T. M. & Wicks, A. C. (1999). Convergent Stakeholder Theory. *Academy of Management Review*, 24(2), 206-221.
- Jones, T. M. (1991). Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model. *Academy of Management Review*, 16(2), 366-395.
- Jonker, J. & Pennink, B. (2010). *The Essence of Research Methodology: A Concise Guide for Master and PhD Students in Management Science*. Springer Science & Business Media.

- Jung, I. (2009). Ethical judgments and Behaviors: Applying a Multidimensional Ethics Scale to Measuring ICT Ethics of College Students. *Computers & Education*, 53, 940–949.
- Kafai, Y., Nixon, A. & Burnam, B. (2007). Digital Dilemmas: How Elementary Preservice Teachers Reason about Appropriate Computer and Internet Use and Their Predictions of Students' Judgments and Justifications. *Journal of Technology and Teacher Education*, 15(3), 409-424.
- Karabag, S. F. & Berggren, C. (2012). Retraction, Dishonesty and Plagiarism : Analysis of a Crucial Issue for Academic Publishing, and the Inadequate Responses from Leading Journals in Economics and Management Disciplines. *Journal of Applied Economics and Business Research*, 2(3), 172–183.
- Karim, N. S. A., Zamzuri, N. H. A. & Nor, Y. M. (2009). Exploring the Relationship between Internet Ethics in University Students and the Big Five Models of Personality. *Computers & Education*, 53(1), 86-93.
- .Kasiulevičius, V., Šapoka, V. & Filipavičiūtė, R. (2006). Sample Size Calculation in Epidemiological Studies. *Gerontologija*, 7(4), 225-231.
- Kaufman, L. M. (2011). How Private is the Internet. *IEEE Security & Privacy*, January/February, pp. 73-75
- Kavuk, M., Keser, H. & Teker, N. (2011). Reviewing Unethical Behaviors of Primary Education Students' Internet Usage. *Procedia-Social and Behavioral Sciences*, 28, 1043-1052.
- Kelly, M., Lyng, C., McGrath, M. & Cannon, G. (2009). A Multi-Method Study to Determine the Effectiveness of, and Student Attitudes to, Online Instructional Videos for Teaching Clinical Nursing Skills. *Nurse Education Today*, 29(3), 292-300.
- Kerlinger, F. N. (1980). Analysis of Covariance Structure Tests of a Criterial Referents Theory of Attitudes. *Multivariate Behavioral Research*, 15(4), 403-422.
- Khalil, O. E. & Seleim, A. A. (2012). Attitudes towards Information Ethics: A View from Egypt.

- Journal of Information, Communication and Ethics in Society*, 10(4), 240-261.
- Kidwell, L. A. & Kent, J. (2008). Integrity at a Distance: A Study of Academic Misconduct among University Students on and off Campus. *Accounting Education: An International Journal*, 17(S1), S3-S16.
- Kim, S. & Park, H. (2014). Intrinsic and Extrinsic Factors Impacting Individuals' Cyber Ethics Awareness and Behavior Intention. *The Journal of Information Systems*, 23(1), 111-138.
- Verecio, R. L. (2016). Computer Ethics Awareness: Implication to Responsible Computing. *International Journal of Education and Research*, 4(3), 195-204.
- Kini, R. B., Rominger, A. & Vijayaraman, B. S. (2000). An Empirical Study of Software Piracy and Moral Intensity among University Students. *Journal of Computer Information Systems*, 40(3), 62-72.
- Kirby, C. & Slevin, O. (2003). Ethical Knowing the Moral Ground of Nursing. *Theory and Practice of Nursing: An Integrated Approach to Caring Practice*, 209.
- Kisamore, J. L., Jawahar, I. M., Liguori, E. W., Mharapara, T. L. & Stone, T. H. (2010). Conflict and Abusive Workplace Behaviors: The Moderating Effects of Social Competencies. *Career Development International*, 15(6), 583-600.
- Kizza, J. M. (2013). Africa's Indigenous Technologies Making Footprint on the World Stage. *Int J Comput ICT Res [Serial Online]*, 7(1), 6-11.
- Kizza, J. M. (2013). Ethics and Ethical Analysis. In *Ethical and Social Issues in the Information Age* (Pp. 29-51). Springer, London.
- Kizza, J. M. (2013). New Frontiers for Computer Ethics: Virtualization and Virtual Reality. In *Ethical and Social Issues in the Information Age* (Pp. 211-229). Springer, London.
- Kizza, J. M. (2015). Security Motives and Threats to Computer Networks. In *Guide to Computer Network Security* (pp. 61-86). Springer, London.
- Knabe, A. (2012). Applying Ajzen's Theory of Planned Behavior to a Study of Online Course Adoption in Public Relations Education.
(Dissertation) Retrieved from:

https://epublications.marquette.edu/cgi/viewcontent.cgi?article=1186&context=dissertations_mu

- Kling, R. & Courtright, C. (2003). Group Behavior and Learning in Electronic Forums: A Sociotechnical Approach. *The Information Society*, 19(3), 221-235.
- Kollmuss, A. & Agyeman, J. (2002). Mind the Gap: Why Do People Act Environmentally and What Are the Barriers to Pro-Environmental Behavior? *Environmental Education Research*, 8(3), 239-260.
- Korte, R. & Mercurio, Z. A. (2017). Pragmatism and Human Resource Development: Practical Foundations for Research, Theory, and Practice. *Human Resource Development Review*, 16(1), 60-84.
- Kortjan, N. & von Solms, R. (2012). Cyber Security Education In Developing Countries: A South African Perspective. In *International Conference on E-Infrastructure and E-Services for Developing Countries* (pp. 289-297). Springer, Berlin, Heidelberg.
- Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International
- Krejcie, R. V. & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, 30(3), 607-610.
- Krishnaswami, O. I. & Ranganathan, M. (2010). *Methodology of Research in Social Sciences*.
Mumbai: Himalaya Publication House.
- Kuan, L. H., Idrus, R. & Muton, N. A. R. Cyberethics Awareness Using Defining Issues Test: A Preliminary Findings.
- Kukafka, R., Johnson, S. B., Linfante, A. & Allegrante, J. P. (2003). Grounding a New Information Technology Implementation Framework in Behavioral Science: A Systematic Analysis of the Literature on IT Use. *Journal of Biomedical Informatics*, 36(3), 218-227.

- Kumar, R. (2017). Ethics and its High Valued in Business World. *Journal of Public Policy & Environmental Management*, 1(1), 1-7.
- Kuo, F. Y. & Hsu, M. H. (2001). Development and Validation of Ethical Computer Self-Efficacy Measure: The Case of Softlifting. *Journal of Business Ethics*, 32(4), 299-315.
- Kuzu, A. (2009). Problems Related to Computer Ethics: Origins of the Problems and Suggested Solutions. *Online Submission*, Turkish Online Journal of Educational Technology - TOJET 8(2).
- Lalonde, P. L., Bourgault, M. & Findeli, A. (2010). Building Pragmatist Theories of PM Practice: Theorizing the Act of Project Management. *Project Management Journal*, 41(5), 21-36.
- Langford, D. (Ed.). (2000). *Internet Ethics*. New York: Macmillan.
- Lau, G. K., Yuen, A. H. & Park, J. (2013). Toward an Analytical Model of Ethical Decision Making in Plagiarism. *Ethics & Behavior*, 23(5), 360-377.
- Lau, W. W. & Yuen, A. H. (2014). Internet Ethics of Adolescents: Understanding Demographic Differences. *Computers & Education*, 72, 378-385.
- Laughton, P. A. (2008). Hierarchical Analysis of Acceptable Use Policies. *South African Journal of Information Management*, 10(4), 2-6.
- Lee, A. (2010). *Cyberethics in Action: Copyright, Privacy, and Media Awareness Teachers' Guides* (Doctoral dissertation). Retrieved from:
https://qspace.library.queensu.ca/bitstream/handle/1974/6064/Lee_Arthur_P_201009_MEd.pdf?sequence=1
- Lee, J., Cerreto, F. A. & Lee, J. (2010). Theory of Planned Behavior and Teachers' Decisions Regarding Use of Educational Technology. *Journal of Educational Technology & Society*, 13(1), 152-164.
- Lee, M. J. & McLoughlin, C. (2010). Beyond Distance and Time Constraints: Applying Social Networking Tools and Web 2.0 Approaches in Distance Education.

- Lee, W. W. & Chan, K. C. (2008). Computer Ethics: A Potent Weapon for Information Security Management. *Information Systems Control Journal*.
- Leedy, P.D. & Ormrod, J.E. (2014). Practical Research: Planning and Design. 10th ed. London: Pearson.
- Lennie, S. (2013). *Ethical Complexities in the Virtual World: Teacher Perspectives of ICT Based Issues and Conflicts* (Doctoral dissertation). Retrieved from: https://tspace.library.utoronto.ca/bitstream/1807/35879/7/Lennie_Shawn_SD_201306_PhD_thesis.pdf
- Leonard, L. N. & Paul Cronan, T. (2005). Attitude toward Ethical Behavior in Computer Use: A Shifting Model. *Industrial Management & Data Systems*, 105(9), 1150-1171.
- Leonard, L. N. & Cronan, T. P. (2001). Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences. *Journal of the Association for Information Systems*, 1(1), 12.
- Levy, Y. & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: The International Journal of an Emerging Transdiscipline*, 9, 181-213.
- Lewis, J. M., Ross, S. & Holden, T. (2012). The How and Why of Academic Collaboration: Disciplinary Differences and Policy Implications. *Higher Education*, 64(5), 693-708.
- Liao, C., Lin, H. N. & Liu, Y. P. (2010). Predicting the Use of Pirated Software: A Contingency Model Integrating Perceived Risk with the Theory of Planned Behavior. *Journal of Business Ethics*, 91(2), 237-252.
- Litt, E. (2013). Measuring Users' Internet Skills: A Review of Past Assessments and a Look toward the Future. *New Media & Society*, 15(4), 612-630.
- Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011). Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16 Year Olds and Their Parents

in 25 Countries.

Liyanagunawardena, T. R. & Samarasinghe, K. (2008). Acceptable Use Policy and Misuse of Work Computers: Case from Sri Lankan Software Development Industry. In *Proceedings of International Conference on Business Management* (Vol. 5).

Loch, K. D. & Conger, S. (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM*, 39(7), 74-84.

Lowry, P. B., Posey, C., Bennett, R. B. J. & Roberts, T. L. (2015). Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust. *Information Systems Journal*, 25(3), 193-273.

Lysaght, Z. (2011). Epistemological and Paradigmatic Ecumenism In Pasteur's Quadrant: Tales from Doctoral Research. In *The Third Asian Conference on Education, Osaka, Japan, Official Conference Proceedings* (pp. 567-579).

Lysonski, S. & Durvasula, S. (2008). Digital Piracy of MP3s: Consumer and Ethical Predispositions. *Journal of Consumer Marketing*, 25(3), 167-178.

MacCord, A. (2015). Infringing a Standard-Essential Patent Or Not. *IEEE Power Electron. Mag.*, 2(4), 14-62.

MacDonald, R. (2008). Professional Development for Information and Communication Technology Integration: Identifying and Supporting a Community of Practice through Design Based Research. *Journal of Research on Technology in Education*, 40(4), 429-446.

MacKinnon, B. & Fiala, A. (2014). *Ethics: Theory and Contemporary Issues*. Nelson Education.

Majumdar, P.K. (2005). *Research Methods in Social Science*. New Delhi: Viva Books Private Limited.

Mäkinen, O. (2008). Philosophy of Web-Based Mediation. In *Handbook of Research on*

Digital Information Technologies: Innovations, Methods, and Ethical Issues (pp. 465-481). IGI Global.

Marks, A. & Rezgui, Y. (2009). A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing. In *2009 International Conference on Management and Service Science* (pp. 1-7). IEEE.

Martin, D. E., Rao, A. & Sloan, L. R. (2009). Plagiarism, Integrity, and Workplace Deviance: A Criterion Study. *Ethics & Behavior*, 19(1), 36-50.

Martin, K. D. & Cullen, J. B. (2006). Continuities and Extensions of Ethical Climate Theory: A Meta-Analytic Review. *Journal of Business Ethics*, 69(2), 175-194.
(Two authors not one)

Martin, N. L. & Woodward, B. S. (2011). Computer Ethics of American and European Information Technology Students: A Cross-Cultural Comparison. *Issues in Information Systems*, 12(1), 78-87.

Martin, R. J., Usdan, S., Nelson, S., Umstattd, M. R., Laplante, D., Perko, M. & Shaffer, H. (2010). Using the Theory of Planned Behavior to Predict Gambling Behavior. *Psychology of Addictive Behaviors*, 24(1), 89.

Martz Jr, W. B. & Shepherd, M. (2007). The Influence of Media Factors on Ethical Behavior. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference On* (Pp. 247a-247a). IEEE.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, 5-12.

Masrom, M. & Ismail, Z. (2008). Computer Security and Computer Ethics Awareness: A Component of Management Information System. In *Information Technology, 2008. Itsim 2008. International Symposium on* (Vol. 3, Pp. 1-7). IEEE.

Masrom, M., Ismail, Z. & Hussein, R. (2009). Ethical Awareness of Computer Use among Undergraduate Students. *ACM SIGCAS Computers and Society*, 39(1), 27-40.

Masrom, M., Ismail, Z., Hussein, R. & Mohamed, N. (2010). An Ethical Assessment of Computer Ethics Using Scenario Approach. *International Journal of Electronic Commerce Studies*, 1(1), 25-36.

- Masrom, M., Mahmood, N. H. N. & Zainon, O. (2013). Cyberethics and Internet Behaviour of Malaysian Primary Education Students. *Journal of Emerging Trends in Educational Research and Policy Studies*, 4(1), 105-111.
- Mathieu, E., Barratt, A., Carter, S. M. & Jamtvedt, G. (2012). Internet Trials: Participant Experiences and Perspectives. *BMC Medical Research Methodology*, 12(1), 162.
- Mayer, D. M., Kuenzi, M., Greenbaum, R., Bardes, M., & Salvador, R. B. (2009). How Low Does Ethical Leadership Flow? Test of a Trickle-Down Model. *Organizational Behavior and Human Decision Processes*, 108(1), 1-13.
- Mayer, J. R. & Mitchell, J. C. (2012). Third-party Web Tracking: Policy and Technology. In *2012 IEEE Symposium on Security and Privacy* (pp. 413-427). IEEE.
- Mayisela, T. (2013). The Potential Use of Mobile Technology: Enhancing Accessibility and Communication in a Blended Learning Course. *South African Journal of Education*, 33(1).
- McCabe, D. L., & Trevino, L. K. (1997). Individual and Contextual Influences on Academic Dishonesty: A Multicampus Investigation. *Research in Higher Education*, 38(3), 379-396.
- McCabe, D. L., Butterfield, K. D. & Trevino, L. K. (2006). Academic Dishonesty in Graduate Business Programs: Prevalence, Causes, and Proposed Action. *Academy of Management Learning & Education*, 5(3), 294-305.
- McEachan, R. R. C., Conner, M., Taylor, N. J. & Lawton, R. J. (2011). Prospective Prediction of Health-Related Behaviours with the Theory of Planned Behaviour: A Meta-Analysis. *Health Psychology Review*, 5(2), 97-144.
- Mcloughlin, C. & Lee, M. J. (2010). Personalised and Self-Regulated Learning in the Web 2.0 Era: International Exemplars of Innovative Pedagogy Using Social Software. *Australasian Journal of Educational Technology*, 26(1).
- Mcquade, S. & Sampat, N. (2008). Survey of Internet and At-Risk Behaviors. *Rochester Institute of Technology*.
- Melo, C. D. O. & de Sousa, T. C. (2017, May). Reflections on Cyberethics Education for Millennial Software Engineers. In *2017 IEEE/ACM 1st International Workshop on*

Software Engineering Curricula for Millennials (SECM) (pp. 40-46). IEEE.

- Mohamed, N., Shahriza Abdul Karim, N. & Hussein, R. (2012). Computer Use Ethics among University Students and Staffs: The Influence of Gender, Religious Work Value and Organizational Level. *Campus-Wide Information Systems*, 29(5), 328-343.
- Mihelic, K. K., Lipicnik, B. & Tekavcic, M. (2010). Ethical Leadership. *International Journal of Management & Information Systems (Online)*, 14(5). Accessed
- Miliany, K. (2014). The Displacement Effect of Internet Use among Saudi Students. *Journal of Arab & Muslim Media Research*, 7(2-3), 185-204.
- Miller, B. & Record, I. (2013). Justified Belief in a Digital Age: On the Epistemic Implications of Secret Internet Technologies. *Episteme*, 10(2), 117-134.
- Mintzberg, H. (2017). Developing Theory about the Development of Theory. In *Handbook of Middle Management Strategy Process Research*. Edward Elgar Publishing. DOI:
- Mishna, F., Cook, C., Gadalla, T., Daciuk, J. & Solomon, S. (2010). Cyber Bullying Behaviors among Middle and High School Students. *American Journal of Orthopsychiatry*, 80(3), 362-374.
- Mitchell, K. J., Finkelhor, D. & Wolak, J. (2007). Youth Internet Users at Risk for the Most Serious Online Sexual Solicitations. *American Journal of Preventive Medicine*, 32(6), 532- 537.
- Molluzzo, J. C. & Lawler, J. (2012). A Study of the Perceptions of College Students on Cyberbullying. *Information Systems Education Journal*, 10(4), 84.
- Molnar, K. K., Kletke, M. G. & Chongwatpol, J. (2008). Ethics vs. IT Ethics: Do Undergraduate Students Perceive a Difference? *Journal of Business Ethics*, 83(4), 657-671.
- Monahan, K. (2012). A Review of the Literature Concerning Ethical Leadership in Organizations. *Emerging Leadership Journeys*, 5(1), 56-66.
- Moor, J. H. (1985). What Is Computer Ethics? *Metaphilosophy*, 16(4), 266-275.

- Moor, J. H. (1998). Reason, Relativity and Responsibility in Computer Ethics. *ACM SIGCAS Computers and Society*, 28(1), 14–21.
[Http://Doi.Org/10.1145/277351.277355](http://doi.org/10.1145/277351.277355)
- Moor, J. H. (1999). Just Consequentialism and Computing. *Ethics and Information Technology*, 1(1), 61-65.
- Moor, J. H. (2001). The Future of Computer Ethics: You Ain't Seen Nothin' Yet! *Ethics and Information Technology*, 3(2), 89-91.
- Moor, J. H. (2004). Reason, Relativity, and Responsibility in Computer Ethics. *Readings in Cyber Ethics, 2nd edition. Jones and Bartlett, Sudbury, MA*, 40-54.
- Moor, J. H. (2006). The Nature, Importance, and Difficulty of Machine Ethics. *IEEE Intelligent Systems*, 21(4), 18-21.
- Moore, T. T. & Chang, J. C. J. (2006). Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model. *MIS Quarterly*, 167-180.
- Moorthy, A. L. & Ramaiah, C. K. (2014). Copyright in Open Access Era: Dealing with Plagiarism. *Scholarly Communication and Intellectual Property Rights*, 103.
- Moross, K. (2017). *Cyberbullying: Youth's Perceptions in a Johannesburg School Context* (Doctoral dissertation).
- Morrow, A. & Downey, C. A. (2013). Perceptions of Adolescent Bullying: Attributions of Blame and Responsibility in Cases of Cyber-Bullying. *Scandinavian Journal of Psychology*, 54(6), 536-540.
- Moskowitz, S. (2017). *Cybercrime and Business: Strategies for Global Corporate Security*. Butterworth-Heinemann.
- Moss, N. D., O'Connor, E. L. & White, K. M. (2010). Psychosocial Predictors of the Use of Enhanced Podcasting in Student Learning. *Computers in Human Behavior*, 26(3), 302-309.
- Mouton, J. (1996). *Understanding Social Research*. Van Schaik Publishers.
- Mukherjee, T. (2013). (Ed) How Digital Media is Changing Corporate Communication. *Amity Journal of Media & Communications Studies (AJMCS)*, 3(1).

- Mutula, S. M. (2013). Ethical Dimension of the Information Society: Implications for Africa. *Information Ethics in Africa: Cross-Cutting Themes, Pretoria: AC*, 29-42.
- Myers, M. D. (1999). Investigating Information Systems with Ethnographic Research. *Communications of the Association for Information Systems*, 2(1), 23
- Mykytyn Jr, P. P. & Harrison, D. A. (1993). The Application of the Theory of Reasoned Action to Senior Management and Strategic Information Systems. *Information Resources Management Journal (IRMJ)*, 6(2), 15-26.
- Namlu, A. G. & Odabasi, H. F. (2007). Unethical Computer Using Behavior Scale: A Study of Reliability and Validity on Turkish University Students. *Computers & Education*, 48(2), 205-215.
- Narayan, V. & Baglow, L. (2010). New Beginnings: Facilitating Effective Learning through the Use of Web 2.0 Tools. *Curriculum, Technology & Transformation for an Unknown Future*, 658-667.
- National Cyber Security Alliance (2009) National Cyberethics, Cybersafety, Cybersecurity Baseline Study
<http://staysafeonline.mediaroom.com/index.php?s=67&item=44>
- Ndubueze, P. N., Igbo, E. U. M. & Okoye, U. O. (2013). Cyber Crime Victimization among Internet Active Nigerians: An Analysis of Socio-Demographic Correlates. *International Journal of Criminal Justice Sciences*, 8(2), 225.
- Neuman, W. L. & Kreuger, L. (2003). *Social Work Research Methods: Qualitative and Quantitative Approaches*. Allyn and Bacon.
- Neuman, W. L. & Robson, K. (2014). *Basics of Social Research*. Toronto: Pearson Canada.
- Newman, D. (2006). The Lines That Continue to Separate Us: Borders in Our Borderless World. *Progress in Human Geography*, 30(2), 143-161.
- Ngoqo, B. & Flowerday, S. (2014). Linking Student Information Security Awareness and Behavioural Intent. In *HAISA* (Pp. 162-173).
- Ngulube, P. (2015). Trends in Research Methodological Procedures Used in Knowledge Management Studies. *African Journal of Library, Archives and Information Science*, 25(2), 125-143.

- Nguyen, T., Nham, P. & Hoang, V. (2019). The Theory of Planned Behavior and Knowledge Sharing: A Systematic Review and Meta-Analytic Structural Equation Modelling, *VINE Journal of Information and Knowledge Management Systems*, Vol. 49 No. 1, pp. 76-94. <https://doi.org/10.1108/VJIKMS-10-2018-0086>
- Ni, X., Yan, H., Chen, S. & Liu, Z. (2009). Factors Influencing Internet Addiction in a Sample of Freshmen University Students In China. *Cyberpsychology & Behavior*, 12(3), 327-330.
- Nkhungulu, C. F. & Deda, F. (2013). An Investigation of Academic Dishonesty in a South African Institution, 2(2), 1294–1300.
- North, M. M., George, R. & North, S. M. (2007, March). A Brief Study of Information Security and Ethics Awareness as an Imperative Component of Management Information Systems. In *Proceedings of the 45th Annual Southeast Regional Conference*(pp. 515-516). ACM.
- North, M. M., Richardson, R. & North, S. M. (2017). Information Security and Ethics Awareness: A Concise Comparative Investigation. *Calitatea*, 18(160), 141.
- Nwogu, M. I. O. (2015). Copyright Law and the Menace of Piracy in Nigeria. *JL Pol'y & Globalization*, 34, 113.
- O'Fallon, M. J. & Butterfield, K. D. (2005). A Review of the Empirical Ethical Decision-Making Literature: 1996–2003. *Journal of Business Ethics*, 59(4), 375-413.
- Oakley, R. L. & Salam, A. F. (2012). Cyber Citizens and Cyber Deviance: Exploring Social and Technical Factors as Antecedents to Cyber Deviance and the Implications for Cyber Citizenship. *SIGHCI2012 Proceedings*. 7.<https://aisel.aisnet.org/sighci2012/7>
- Obar, J. A., Zube, P. & Lampe, C. (2012). Advocacy 2.0: An Analysis of How Advocacy Groups in the United States Perceive and Use Social Media as Tools for Facilitating Civic Engagement and Collective Action. *Journal of Information Policy*, 2, 1-25.
- Ocholla, D. (2009). Information Ethics Education in Africa. Where Do We Stand? *The International Information & Library Review*, 41(2), 79-88.
- Odo, C. R. & Odo, A. I. (2015). The Extent of Involvement in Cybercrime Activities

among Students in Tertiary Institutions in Enugu State of Nigeria. *Global Journal of Computer Science and Technology*.15(3), 1-6

Okoli, C. & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. Available at SSRN 1954824.
<https://pdfs.semanticscholar.org/31dc/753345d5230e421ea817dd7dcdd352e87ea2.pdf>

Onyancha, O. B. (2015). An Infometrics View of the Relationship between Internet Ethics, Computer Ethics and Cyberethics. *Library Hi Tech*, 33(3), 387-408.

Orbell, S. & Sheeran, P. (1998). Inclined Abstainers: A Problem for Predicting Health-Related Behaviour. *British Journal of Social Psychology*, 37(2), 151-165.

Osborne, H. (2017). Digital Piracy, Digital Practices: Changing Discourse on Young People and Downloading in Canadian Newspapers. *Jeunesse: Young People, Texts, Cultures*, 9(2), 112-139.

Oyewole, O. (2017). Awareness and Perception of Computer Ethics by Undergraduates of a Nigerian University. *Journal of Information Science, Theory and Practice*, 5(4), 68-80.

Pahuja, S. (2011). *Decolonising International Law: Development, Economic Growth and the Politics of Universality*(Vol. 86). Cambridge University Press

Pallant, J. (2013). *SPSS Survival Manual*. McGraw-Hill Education (UK).

Passow, H. J., Mayhew, M. J., Finelli, C. J., Harding, T. S. & Carpenter, D. D. (2006). Factors Influencing Engineering Students' Decisions to Cheat by Type of Assessment. *Research in Higher Education*, 47(6), 643-684.

Patton, M. Q. (2002). Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective. *Qualitative Social Work*, 1(3), 261-283.

Peace, A. G., Galletta, D. F. & Thong, J. Y. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, 20(1),

- Peng, T. Q., Zhu, J. J., Tong, J. J. & Jiang, S. J. (2012). Predicting Internet Non-Users' Adoption Intention and Adoption Behavior: A Panel Study of Theory of Planned Behavior. *Information, Communication & Society*, 15(8), 1236-1257.
- Peslak, A. R. (2008). Current Information Technology Issues and Moral Intensity Influences. *Journal of Computer Information Systems*, 48(4), 77-86.
- Phyo, A. H., Furnell, S.M. & Phippen, A.D. (2007). Prerequisites for Monitoring Insider IT Misuse, In Bleimann, U.G., Dowland, P.S. & Furnell, S.M. (Eds.): Proceedings of the Third Collaborative Research Symposium Security, E-Learning, Internet and Networking (SEIN 2007), Pp.41–52.
- Plaisance, P. L. (2007). Transparency: An assessment of the Kantian Roots of a Key Element in Media Ethics Practice. *Journal of Mass Media Ethics*, 22(2-3), 187-207.
- Plaisance, P. L. (2013). *Media Ethics: Key Principles for Responsible Practice*. Sage Publications.
- PriceWaterHouse Coopers, L. L. C. (2017). “Key Findings from the 2013 US State Of Cybercrime Survey.” Retrieved February, 13, 2017.
- Prosser, B. T. & Ward, A. (2000). Kierkegaard and the Internet: Existential Reflections on Education and Community. *Ethics and Information Technology*, 2(3), 167-180.
- Quarshie, H. O. (2012). Ethical Challenges in a Computerized Society, 3(11), 1495–1497.
- Quigley, M. (Ed.). (2005). *Information Security and Ethics: Social and Organizational Issues*. IGI Global.
- Quigley, M. (Ed.). (2007). *Encyclopedia of Information Ethics and Security*. IGI Global.
- Quinn, M. J. (2014). *Ethics for the Information Age*. New Jersey: Pearson.
- Radcliffe, E. S. (1997). Kantian Tunes on a Humean Instrument: Why Hume Is Not Really a Skeptic about Practical Reasoning. *Canadian Journal of Philosophy*, 27(2), 247-269.

- Ramadhan, A., Sensuse, D. I. & Arymurthy, A. M. (2011). E-Government Ethics: A Synergy of Computer Ethics, Information Ethics and Cyber Ethics. *International Journal of Advanced Computer Science and Applications*, 2(8), 82–86.
- Randolph, J. J. (2009). A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research & Evaluation*, 14(13), 1-13.
- Rathinasabapathy, G. & Rajendran, L. (2007). Cyber Crimes and Information Frauds: Emerging Challenges for LIS Professionals. In *Information to Knowledge: Technology and Professionals. Proceedings of the Conference on Recent Advances in Information Science and Technology (READIT 2007)*, MALA & IGCAR, Kalpakkam (pp. 131-142).
- Renee Taylor, K., Won Whang, E. & Tettegah, S. Y. (2006). Acceptable Use Policies in School Districts: Myth or Reality? In *Technology and Education: Issues in Administration, Policy, and Applications in K12 Schools* (pp. 115-123). Emerald Group Publishing Limited.
- Rensburg, A. J. (2018, Oct 30). Malusi Gigaba Sex Scandal: Should We Care about Politicians' Private Lives? The Herald. Retrieved from <http://www.herald.co.zw>
- Republic of South Africa (2003). *Health Records and Information Policy Act*. Retrieved from: http://www.samed.org.za/Filemanager/userfiles/national-health-act-61-2003-norms-and-standards-regulations-applicable-to-different-categories-of-health-establishments_20170104-GGN-40539-00010.pdf
- Republic of South Africa (2011). *Freedom of Information (FOI) Act*. Retrieved from: https://www.saps.gov.za/resource_centre/acts/downloads/promotion_of_access_act2_2000.pdf
- Republic of South Africa (2013) *Protection of Personal Information*. Retrieved from: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinfoforcorrect.pdf

Republic of South Africa (2013). *Cybercrime Policy*. Retrieved from:
<http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf>

Republic of South Africa (2017) *Copyright Amended Act*. Retrieved
from: [https://www.gov.za/sites/default/files/gcis_document/201705/b13-
2017copyright170516.pdf](https://www.gov.za/sites/default/files/gcis_document/201705/b13-2017copyright170516.pdf),

Republic of South Africa (2017). *Cybercrime Bill*.
Retrieved from:
<http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf>

Republic of South Africa (2016). South African Higher Education Reviewed: Two
Decades of Democracy. Retrieved January 17,2019, from
[https://www.ch.ac.za/sites/default/files/publications/CHE_South%20African%2
0higher
%20education%20reviewed%20-%20electronic.pdf](https://www.ch.ac.za/sites/default/files/publications/CHE_South%20African%20higher%20education%20reviewed%20-%20electronic.pdf)

Rettinger, D. A. & Kramer, Y. (2009). Situational and Personal Causes of Student
Cheating. *Research in Higher Education*, 50(3), 293-313.

Reynolds, E. O. R. (1971). Effect of Alterations in Mechanical Ventilator Settings on
Pulmonary Gas Exchange in Hyaline Membrane Disease. *Archives of Disease in
Childhood*, 46(246), 152-159.

Reynolds, G. (2015). *Ethics in Information Technology*. Nelson Education.

Ridley, D. (2008). *The Literature Review: A Step-by-Step Guide for Students*. London: Sage.

Riemenschneider, C. K., Harrison, D. A. & Mykytyn, P. P. (2003). Understanding IT
Adoption Decisions in Small Business: Integrating Current Theories. *Information
& Management*, 40(4), 269-285.

Ritchie, J., Lewis, J., Nicholls, C. M. & Ormston, R. (2013). *Qual Res Practice: A Guide
for Soc Sci Students and Researchers*.

Ritchie, J. & Lewis, J. 2012. *Qualitative Research Practice: A Guide for Social Science
Students and Researchers*. Los Angeles: Sage.

- Robertson, K., McNeill, L., Green, J. & Roberts, C. (2012). Illegal Downloading, Ethical Concern, and Illegal Behavior. *Journal of Business Ethics*, 108(2), 215-227.
- Roblyer, M. D., McDaniel, M., Webb, M., Herman, J. & Witty, J. V. (2010). Findings on Facebook in Higher Education: A Comparison of College Faculty and Student Uses and Perceptions of Social Networking Sites. *The Internet and Higher Education*, 13(3), 134- 140.
- Robson, C., (2011). Real World Research. John Wiley & Sons.
- Rocco, T. S. & Plakhotnik, M. S. (2009). Literature Reviews, Conceptual Frameworks, and Theoretical Frameworks: Terms, Functions, and Distinctions. *Human Resource Development Review*, 8(1), 120-130.
- Rujoiu, O. & Rujoiu, V. (2014). Academic Dishonesty and Workplace Dishonesty: An Overview. In *Proc. Int. Manage. Conf* (Vol. 8, pp. 928-938).
- Rychlak, J. F. (1968). A Philosophy of Science for Personality Theory.
- Sabatier, P. A. & Weible, C. M. (Eds.). (2014). *Theories of the Policy Process*. Westview Press.
- Saias, M. A. (2014). Unlawful Acquisition of Trade Secrets by Cyber Theft: Between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks. *Journal of Intellectual Property Law & Practice*, 9(9), 721-729.
- Salkind, N. J. (2003). Exploring Research. United States of America: Prentice Hall
- Sampson, M., McGowan, J., Cogo, E., Grimshaw, J., Moher, D. & Lefebvre, C. (2009). An Evidence-Based Practice Guideline for the Peer Review of Electronic Search Strategies. *Journal of Clinical Epidemiology*, 62(9), 944-952.
- Sargolzaei, E. & Nikbakht, M. (2017). The Ethical and Social Issues of Information Technology: A Case Study. *International Journal of Advanced Computer Science and Applications*, 8(10), 138-146.
- Saunders, M. N. & Lewis, P. (2012). *Doing Research in Business & Management: An Essential Guide to Planning Your Project*. Pearson.

- Schepers, P., Hagenzieker, M., Methorst, R., Van Wee, B. & Wegman, F. (2014). A Conceptual Framework for Road Safety and Mobility Applied to Cycling Safety. *Accident Analysis & Prevention*, 62, 331-340.
- Scheuermann, L. E. & Langford, H. P. (1997). Perceptions of Internet Abuse, Liability, and Fair Use. *Perceptual and Motor Skills*, 85(3), 847-850.
- Schulman, A. (2001). The Extent of Systematic Monitoring of Employee E-Mail and Internet Use. *The Privacy Project*, July, 9.
- Schultz, R. A. (Ed.). (2005). *Contemporary Issues in Ethics and Information Technology*. IGI Global.
- Schweitzer, D., Gibson, D., Bibighaus, D. & Boleng, J. (2009). Preparing Our Undergraduates to Enter a Cyber World. In *IFIP World Conference on Information Security Education* (pp. 123-130). Springer, Berlin, Heidelberg.
- Scotland, J. (2012). Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to the Methodology and Methods of the Scientific, Interpretive, and Critical Research Paradigms. *English Language Teaching*, 5(9), 9-16.
- Seider, S., Novick, S. & Gomez, J. (2013). Cultivating the Academic Integrity of Urban Adolescents with Ethical Philosophy Programming. *Peabody Journal of Education*, 88(2), 142–158. [Http://Doi.Org/10.1080/0161956X.2013.775864](http://doi.org/10.1080/0161956X.2013.775864)
- Sekaran, U. & Bougie, R. (2010). *Research Methods for Business: A Skill Building Approach*, 5th ed. UK: John Wiley & Sons.
- Şendağ, S., Duran, M. & Fraser, M. R. (2012). Surveying the Extent of Involvement in Online Academic Dishonesty (E-Dishonesty) Related Practices among University Students and the Rationale Students Provide: One University's Experience. *Computers in Human Behavior*, 28(3), 849-860.
- Sharma, M., Mittal, S. & Verma, A. (2015). Cyber Ethics in Security Application in the Modern Era of Internet. *IITM Journal of Management and IT*, 6(1), 140-143.
- Sheeran, P., Gollwitzer, P. M. & Bargh, J. A. (2013). Nonconscious Processes and Health.

Health Psychology, 32(5), 460.

Shemroske, K. (2011). *The Ethical Use of IT: A Study of Two Models for Explaining Online File Sharing Behavior* (Doctoral dissertation). Retrieved from: <https://uh-ir.tdl.org/handle/10657/429>

Shinde, S. M. (2013). Cyber Ethics and Laws - Pros and Cons : A Study of IT Act, 25–29.

Siegfried, R. M. (2004). Student Attitudes on Software Piracy and Related Issues of Computer Ethics. *Ethics and Information Technology*, 6(4), 215–222.

Sidani, Y., Zbib, I., Rawwas, M. & Moussawer, T. (2009). Gender, Age, and Ethical Sensitivity: The Case of Lebanese Workers. *Gender in Management: An International Journal*, 24(3), 211-227

Sidani, Y. (2005). Women, Work, and Islam in Arab Societies. *Women in Management Review*, 20(7), 498-512

Simonson, M., Smaldino, S. & Zvacek, S. M. (Eds.). (2014). *Teaching and Learning at a Distance: Foundations of Distance Education*. IAP.

Singer, P. (2011). *Practical Ethics*. Cambridge University Press.

Singh, A. K. & Siddiqui, A. T. (2011). New Face of Terror: Cyber Threats, Emails Containing Viruses. *Asian Journal of Technology & Management Research* [ISSN: 2249– 0892], 1(01).

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 487-502.

Smith, N., Allhoff, F. & Vaidya, A. J. (2008). *Ancient Philosophy*. Blackwell Publishing Ltd.

Sniehotta, F. F., Presseau, J. & Araújo-Soares, V. (2014). Time to Retire the Theory of Planned Behaviour. *Health Psychology Review*, 8(1), 1.

Snyder, I., Jones, A. & Lo Bianco, J. (2005). *Using Information and Communication*

- Technologies in Adult Literacy Education: New Practices, New Challenges. An Adult Literacy National Project Report.* National Centre for Vocational Education Research Ltd. PO Box 8288, Stational Arcade, Adelaide, SA 5000, Australia.
- Sommer, L. (2011). The Theory of Planned Behaviour and the Impact of Past Behaviour. *International Business & Economics Research Journal*, 10(1), 91-110.
- Spangenberg, L. (2016). *An Exploration of the Ethics of Scam Advertising and Advertising Awards Shows in South Africa* (Doctoral Dissertation, University of Pretoria).
- Spence, E. H. & Quinn, A. (2008). Information Ethics as a Guide for New Media. *Journal of Mass Media Ethics*, 23(4), 264-279.
- Spinello, R. (2011). *Cyberethics: Morality and Law in Cyberspace*. Jones & Bartlett Learning.
- Spinello, R. A. & Tavani, H. T. (Eds.). (2004). *Readings in Cyberethics*. Jones & Bartlett Learning.
- Sponaule, A. D. (2008). *Assessing Undergraduate Students' Perceptions of Ethics Instruction in a Computing Curriculum* (Doctoral Dissertation, University of Maryland, Baltimore County).
- SPSS version 25 (2017), IBM Software Group, ATTN: Licensing, 200 W. Madison St. Chicago, IL; 60606, U.S.A
- Srivastava, A. & Thomson, S. B. (2009). Framework Analysis: A Qualitative Methodology for Applied Policy Research.
- Stahl, B. C. & Flick, C. (2010). ETICA Workshop on Computer Ethics: Exploring Normative Issues. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (pp. 64-77). Springer, Berlin, Heidelberg. (Not 2011)
- Stahl, B. C. & Rogerson, S. (2009). Landscapes of Ethical Issues of Emerging ICT Applications in Europe. In *8th International Conference Computer Ethics: Philosophical Enquiry* (pp. 719-737).

- Stahl, B. C., Eden, G. & Jirotko, M. (2013). Responsible Research and Innovation in Information and Communication Technology: Identifying and Engaging with the Ethical Implications of ICTs. *Responsible Innovation*, 199-218.
- Stahl, B. C., Eden, G., Jirotko, M. & Coeckelbergh, M. (2014). From Computer Ethics to Responsible Research and Innovation in ICT: The Transition of Reference Discourses Informing Ethics-Related Research in Information Systems. *Information & Management*, 51(6), 810-818.
- Stahl, B. C., Heersmink, R., Goujon, P., Flick, C., Van Den Hoven, J., Wakunuma, K. & Rader, M. (2010). Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method. *International Journal of Technoethics (IJT)*, 1(4), 20-38.
- Stahl, B. C., Rogerson, S. & Wakunuma, K. J. (2009), November). Future Technologies: The Matter of Emergent Ethical Issues in Their Development. In *Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, 2009.Computation World'09. Computation World*: (pp. 603-607). IEEE.
- Stake, R. E. (2000). Case Studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (2nd ed., pp. 435-454). Thousand Oaks, CA: Sage.
- Stamatellos, G. (2007). *Computer Ethics: A Global Perspective*. Jones & Bartlett Learning.
- Staub, E. (2013). *Positive Social Behavior and Morality: Social and Personal Influences*. Elsevier.
- Statista (2014) *Distribution of Daily Media Consumption among 15-24 Year-Olds in the United Kingdom (UK) in 2014*. Retrieved from:
<https://www.statista.com/statistics/486125/daily-media-diet-of-young-people-uk/>

- Stone, T. H., Jawahar, I. M. & Kisamore, J. L. (2010). Predicting Academic Misconduct Intentions and Behavior Using the Theory of Planned Behavior and Personality. *Basic and Applied Social Psychology*, 32(1), 35-45. B
- Stylianou, A. C., Winter, S., Niu, Y., Giacalone, R. A. & Campbell, M. (2013). Understanding the Behavioral Intention to Report Unethical Information Technology Practices: The Role of Machiavellianism, Gender and Computer Expertise. *Journal of Business Ethics*, 117(2), 333-343.
- Sumner, W. G. (2013). *Folkways - A Study of the Sociological Importance of Usages, Manners, Customs, Mores and Morals*. Read Books Ltd.
- Supavai, E. (2014). *Measuring Online Moral Reasoning: The Development and Psychometric Properties of the Cyberethics Scale* (Doctoral Dissertation, Boston University).
- Sutton, S. (1994). The Past Predicts the Future: Interpreting Behaviour–Behaviour Relationships in Social Psychological Models of Health Behaviour. In DR Rutter & L. Quine (Eds.), *Social Psychology and Health: European Perspectives* (pp. 71-88). Brookfield, VT, US: Avebury/Ashgate Publishing
- Szabo, A. & Underwood, J. (2004). Cybercheats: Is Information and Communication Technology Fuelling Academic Dishonesty? *Active Learning in Higher Education*, 5(2), 180-199.
- Tade, O. & Aliyu, I. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2).
- Tadele, B. (2013). Motivations behind Software Piracy: From the Viewpoint of Computer Ethics Theories. (Masters' Dissertation). Retrieved from: <http://jultika.oulu.fi/files/nbnfioulu-201405241494.pdf>
- Tahat, L., Elia, M. I., Sawalha, N. N. & Al-Shaikh, F. N. (2014). The Ethical Attitudes of Information Technology Professionals: A Comparative Study between the USA and the Middle East. *Ethics and Information Technology*, 16(3), 241-249.

- Taherdoost, H., Namayandeh, M. & Jalaliyoon, N. (2011). Information Security and Ethics in Educational Context: Propose a Conceptual Framework to Examine Their Impact. *International Journal of Computer Science and Information Security*, 9(1), Pp.134-138.
- Tarafdar, M., DArcy, J., Turel, O. & Gupta, A. (2015). The Dark Side of Information Technology. *MIT Sloan Management Review*, 56(2), 61.
- Tarkang, E. E. & Zotor, F. B. (2015). Application of the Health Belief Model (HBM) In HIV Prevention: A Literature Review. *Central African Journal of Public Health*, 1(1), 1-8.
- Tashakkori, A. & Teddlie, C. (2008). Quality of Inferences in Mixed Methods Research: Calling for an Integrative Framework. *Advances in Mixed Methods Research*, 101-119.
- Tavani, H. T. (2013). Cyberethics. In: Runehov A.L.C., Oviedo L. (eds). *Encyclopedia of Sciences and Religions*. Springer, Dordrecht
- Tavani, H. T. (2011). *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*. John Wiley & Sons.
- Tavani, H. T. (2001). The State of Computer Ethics as a Philosophical Field of Inquiry: Some Contemporary Perspectives, Future Projections, and Current Resources. *Ethics and Information Technology*, 3(2), 97-108.
- Taylor, S. & Todd, P. A. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, 6(2), 144-176.
- Teddlie, C. & Tashakkori, A. (2009). *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. Sage.
- Tella, A. & Mutula, S. M. (2008). Gender Differences in Computer Literacy among Undergraduate Students at the University of Botswana: Implications for Library

- Use. *Malaysian Journal of Library & Information Science*, 13(1), 59-76.
- Tenbrunsel, A. E. (2007). Today's Ethical Issues: A Perspective from Accounting, Finance, Management and Marketing. *Journal of Business Ethics*, 70(1), 1-3.
- Thelwall, M. (2002, April). An Initial Exploration of the Link Relationship between UK University Websites. In *ASLIB Proceedings* (Vol. 54, No. 2, pp. 118-126). MCB UP Ltd.
- Thomas, T. & Ahyick, M. (2010). Can We Help Information Systems Students Improve Their Ethical Decision Making? *Interdisciplinary Journal of Information, Knowledge & Management*, 5.
- Thomas, T. D., Singh, L. & Gaffar, K. (2013). The Utility of the UTAUT Model in Explaining Mobile Learning Adoption in Higher Education in Guyana. *International Journal of Education and Development Using Information and Communication Technology*, 9(3), 71.
- Thompson, J. D. (2017). *Organizations in Action: Social Science Bases of Administrative Theory*.
Routledge.
- Thompson, R. L., Higgins, C. A. & Howell, J. M. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly*, 125-143.
- Thomson, K. L., Von Solms, R. & Louw, L. (2006). Cultivating an Organizational Information Security Culture. *Computer Fraud & Security*, 2006(10), 7-11.
- Time Live (2017) *South Africans Easy Meat for Hackers*. Retrieved from: <https://www.bizcommunity.com/Article/196/661/167877.html>
- Trevino, L. K. & Youngblood, S. A. (1990). Bad Apples in Bad Barrels: A Causal Analysis of Ethical Decision-Making Behavior. *Journal of Applied Psychology*, 75(4), 378.
- Tu, C. H. & McIsaac, M. (2002). The Relationship of Social Presence and Interaction in Online Classes. *The American Journal of Distance Education*, 16(3), 131-150.

- Udo-Akang, D. (2012). Theoretical Constructs, Concepts, and Applications. *American International Journal of Contemporary Research*, 2(9), 89-97.
- Udo-Akang, D. (2013). Ethical Orientation for New and Prospective Researchers. *American International Journal of Social Science*, 2(1), 54-64.
- Udris, R. (2016). Cyber Deviance among Adolescents and the Role of Family, School, and Neighborhood: A Cross-National Study. *International Journal of Cyber Criminology*, 10(2), 127.
- Underwood, J. D., Banyard, P. E. & Davies, M. N. (2007). Students in Digital Worlds: Lost in Sin City Or Reaching Treasure Island? In *BJEP Monograph Series II, Number 5- Learning Through Digital Technologies* (Vol. 83, No. 99, Pp. 83-99). British Psychological Society.
- United Kingdom Office of National Statistics (2018) Overview of Fraud and Computer Misuse Statistics for England and Wales. Retrieved From: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice>
- University of North Carolina (2014). General Administration. *Student Services: Responding to Issues and Challenges: The Fifth Compendium of Papers*. University of North Carolina General Administration.
- University of Zululand (2013). *Policy and Procedure on Research Ethics*. Retrieved from: <http://uzsite.unizulu.ac.za/research-and-innovation/policies-and-guidelines/>
- University of Zululand (2013). *Policy and Procedure on Managing and Preventing Acts of Plagiarism*. Retrieved from: <http://www.unizulu.ac.za/wp-content/uploads/2017/08/RI-P4.pdf>
- University of Zululand (2013). *Research Ethics Guide*. Retrieved from : <http://www.unizulu.ac.za/wp-content/uploads/2017/08/RI-P3.pdf>
- University of Zululand (2014). <http://www.unizulu.ac.za/wp-content/uploads/2014/08/Plagiarism-Policy-Council-Approved-20121207.pdf>
- University of Zululand Annual Report available: <http://www.unizulu.ac.za/wp-content/uploads/2018/12/UNIZULU-2017-2018-Annual-Report.pdf>

- Upshaw, D. & Babin, L. A. (2010). Music Downloading: Competing against Online Piracy. *International Journal of Business and Public Administration*, 7(1), 14-26.
- Vallor, S. (2010). Social Networking Technology and the Virtues. *Ethics and Information Technology*, 12(2), 157-170.
- Van den Hoven, J. (2008). Moral Methodology and Information Technology. *The Handbook of Information and Computer Ethics*, 49.
- Van Niekerk, J. & Von Solms, R. (2013). A Theory Based Approach to Information Security Culture Change. *Information (Japan)*, 16(6B), 3907-3930.
- Vanclay, F., Baines, J. T. & Taylor, C. N. (2013). Principles for Ethical Research Involving Humans: Ethical Professional Practice In Impact Assessment Part I. *Impact Assessment and Project Appraisal*, 31(4), 243-253.
- Varga, C. (2016). From the Ontology of Social Being to the Law's Ontology. *Millennium*, 45(3), 29
- Vedder, A. (2008). Responsibilities for Information on the Internet. *The Handbook of Information and Computer Ethics*, 339.
- Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 425-478.
- Verecio, R. L. (2016). Computer Ethics Awareness: Implication to Responsible Computing. *International Journal of Education and Research*, 4(3), 195-204.
- Vining, J. & Ebreo, A. (1990). What Makes a Recycler? A Comparison of Recyclers and Nonrecyclers. *Environment and Behavior*, 22(1), 55-73.
- Vitell, S. J. & Muncy, J. (2005). The Muncy-Vitell Consumer Ethics Scale: A Modification and Application. *Journal of Business Ethics*, 62(3), 267-275.
- Voiskounsky, A. E. (2009). Web Plagiarism: Empirical Study. *Psychology in Russia*, 2, 277

Von Schomberg, R. (2012). Prospects for Technology Assessment in a Framework of Responsible Research and Innovation. In *Technikfolgen abschätzen lehren* (pp. 39-61). VS Verlag für Sozialwissenschaften.

Von Solms, R. & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.

Wacker, J. G. (1998). A Definition of Theory: Research Guidelines for Different Theory-Building Research Methods in Operations Management. *Journal of Operations Management*, 16(4), 361-385.

Wagner, S. C. & Sanders, G. L. (2001). Considerations in Ethical Decision-Making and Software Piracy. *Journal of Business Ethics*, 29(1-2), 161-167.

Walczak, K., Finelli, C., Holsapple, M., Sutkus, J., Harding, T. & Carpenter, D. (2010). Institutional Obstacles to Integrating Ethics into the Curriculum and Strategies for Overcoming Them.

Walden, I. (2013). Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent.

In *Privacy and Security for Cloud Computing* (pp. 45-71). Springer, London.

Walker, D. H. & Sinclair, F. L. (1998). Acquiring Qualitative Knowledge about Complex Agroecosystems. Part 2: Formal Representation. *Agricultural Systems*, 56(3), 365-386.

Warschauer, M. & Matuchniak, T. (2010). New Technology and Digital Worlds: Analyzing Evidence of Equity in Access, Use, and Outcomes. *Review of Research in Education*, 34(1), 179-225.

Weaver, K. & Olson, J. K. (2006). Understanding Paradigms Used for Nursing Research. *Journal of Advanced Nursing*, 53(4), 459-469.

Webb, T. L. & Sheeran, P. (2006). Does Changing Behavioral Intentions Engender

- Behavior Change? A Meta-Analysis of the Experimental Evidence. *Psychological Bulletin*, 132(2), 249.
- Weber, R. H. (2016). CHAPTER SIX: ETHICS IN THE INTERNET ENVIRONMENT. *Designing Digital Freedom*, 113.
- Welman, Kruger, Mitchell (2012). *Research Methodology*. Oxford University Press: Southern
- Weulen Kranenbarg, M., Holt, T. J. & van Gelder, J. L. (2017). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, 1-16.
- Whitley, B. E. Jr. (1998). Factors Associated with Cheating among College Students: A Review. *Research in Higher Education*, 39(3), 235–274.
- Whittier, D. B. (2013). Cyberethics: Envisioning Character Education in Cyberspace. *Peabody Journal of Education*, 88(2), 225-242.
- Williams, M. D., Rana, N. P., Dwivedi, Y. K. & Lal, B. (2011, June). Is UTAUT Really Used or Just Cited for the Sake of It? A Systematic Review of Citations of UTAUT's Originating Article. In *ECIS* (P. 231).
- Williamson, S., Clow, K. E., Walker, B. C. & Ellis, T. S. (2011). Ethical Issues in the Age of the Internet: A Study of Students' Perceptions Using the Multidimensional Ethics Scale. *Journal of Internet Commerce*, 10(2), 128-143.
- Wolak, J., Mitchell, K. & Finkelhor, D. (2007). Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. *Pediatrics*, 119(2), 247-257.
- Wood, A. W. (2007). *Kantian Ethics*. Cambridge University Press.
- Woodward, B., Martin, N. L. & Imboden, T. (2011). Expansion and Validation of the PAPA Framework. *Information Systems Education Journal*, 9(3), 28.

- Xu, Z., Hu, Q. & Zhang, C. (2013). Why Computer Talents Become Computer Hackers. *Communications of the ACM*, 56(4), 64-74.
- Yamano, P. (2006, March). Cyberethics in the Elementary Classroom: Teaching Responsible Use of Technology In *Society for Information Technology & Teacher Education International Conference* (Pp. 3667-3670). Association for the Advancement of Computing in Education (AACE).
- Yan, Z. (Ed.). (2012). *Encyclopedia of Cyber Behavior* (Vol. 1). IGI Global.
- Yin, R. K. (2003). Case Study Research: Design and Methods: Vol. 5. Applied Social Research Methods Series. Thousand Oaks, CA: Sage
- Yoon, C. (2010). Ethical Decision-Making in the Internet Context: Development and Test of an Initial Model Based on Moral Philosophy. *Computers in Human Behavior*, 27(6), 2401- 2409.
- Yoon, C. (2011). Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model. *Journal of Business Ethics*, 100(3), 405-417.
- Young, K. S. & Case, C. J. (2004). Internet Abuse in the Workplace: New Trends in Risk Management. *Cyber Psychology & Behavior*, 7(1), 105-111.
- Yousafzai, S. Y., Foxall, G. R. & Pallister, J. G. (2010). Explaining Internet Banking Behavior: Theory of Reasoned Action, Theory of Planned Behavior, or Technology Acceptance Model? *Journal of Applied Social Psychology*, 40(5), 1172-1202.
- Zachariadis, M., Scott, S. & Barrett, M. (2013). Methodological Implications of Critical Realism for Mixed-Methods Research. *MIS Quarterly*, 855-879.
- Zetter, K. (2007) Is Your Boss Spying on You? It's Legal, It's Happening and It Can Get You Fired. *Reader's Digest* - November, 97 - 103.
- Zhang, A. T. (2010). Key Influences of Cyberbullying for University Students. Retrieved September 22, 2016, from <http://www.pacis-net.org/file/2010/S01-01.pdf>
- Zuidema, W. (2007). Parsimonious Data-Oriented Parsing. In *Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning (EMNLP-CoNLL)*.

APPENDIX

Appendix 1: Ethical Clearance Certificate: Reg No UZREC 171110-030



ETHICAL CLEARANCE CERTIFICATE

Certificate Number	UZREC 171110-030 PGD 2016/116						
Project Title	Cyberethical behavior of undergraduate students of University of Zululand South Africa and federal University of Agriculture Abeokutu Nigeria						
Principal Researcher/ Investigator	NA Adeniyi						
Supervisor and Co-supervisor	Prof DN Ocholla						
Department	Information Studies						
Nature of Project	Honours/4 th Year		Master's		Doctoral	x	Departmental

The University of Zululand's Research Ethics Committee (UZREC) hereby gives ethical approval in respect of the undertakings contained in the above-mentioned project proposal and the documents listed on page 2 of this Certificate.

Special conditions:

- (1) The Principal Researcher must report to the UZREC in the prescribed format, where applicable, annually and at the end of the project, in respect of ethical compliance.
- (2) Documents marked "To be submitted" (see page 2) must be presented for ethical clearance before any data collection can commence.

The Researcher may therefore commence with the research as from the date of this Certificate, using the reference number indicated above, but may not conduct any data collection using research instruments that are yet to be approved.

Please note that the UZREC must be informed immediately of

- Any material change in the conditions or undertakings mentioned in the documents that were presented to the UZREC
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research

Classification:

Data collection	Animals	Human Health	Children	Vulnerable pp.	Other
X					
Low Risk		Medium Risk		High Risk	
		X			

The table below indicates which documents the UZREC considered in granting this Certificate and which documents, if any, still require ethical clearance. (Please note that this is not a closed list and should new instruments be developed, these would require approval.)

Documents	Considered	To be submitted	Not required
Faculty Research Ethics Committee recommendation	X		
Animal Research Ethics Committee recommendation			X
Health Research Ethics Committee recommendation			X
Ethical clearance application form	X		
Project registration proposal	X		
Informed consent from participants	X		
Informed consent from parent/guardian			X
Permission for access to sites/information/participants	X		
Permission to use documents/copyright clearance			X
Data collection/survey instrument/questionnaire	X		
Data collection instrument in appropriate language		Only if necessary	
Other data collection instruments		Only if used	

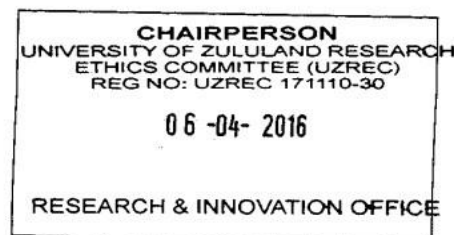
The UZREC retains the right to

- Withdraw or amend this Certificate if
 - Any unethical principles or practices are revealed or suspected
 - Relevant information has been withheld or misrepresented
 - Regulatory changes of whatsoever nature so require
 - The conditions contained in this Certificate have not been adhered to
- Request access to any information or data at any time during the course or after completion of the project

The UZREC wishes the researcher well in conducting the research



Professor Nokuthula Kunene
Chairperson: University Research Ethics Committee
 06 April 2016
 NA Adeniyi - PGM 2016/116



Appendix 2: Access letter requesting permission to conduct research work at FUNAAB

ANNEXURE G: ACCESS LETTER REQUESTING PERMISSION TO CONDUCT RESEARCH

University of Zululand
Private Bag X1001,
KwaDlangezwa, 3886
South Africa.

The Registrar
Federal University of Agriculture
Abeokuta, Ogun State
Nigeria

.....
Date 10, September 2016

Dear Sir,

REQUEST FOR PERMISSION TO CONDUCT RESEARCH

I am a registered PhD student in the Department of Information Studies, Faculty of Arts at the University of Zululand. My supervisors are Professor Dennis Ocholla and Professor Johannes Britz.

The proposed topic of my research is: **Cyberethical Behaviour of Undergraduate Students in University of Zululand South Africa and Federal University of Agriculture Abeokuta Nigeria**

The objectives of the study are:

1. To determine the relationships between students' demographic characteristics and cyberethics behaviour.
2. To determine undergraduate students' awareness of cyberethics in the University of Zululand, South Africa, and the Federal University of Agriculture Abeokuta, Nigeria;
3. To identify the types of cyberethics behaviour exhibited by undergraduate students in the two universities;
4. To verify the applicability and impact of the theory of planned behaviour TPB on cyberethics behaviour in the two institutions;
5. To identify the challenges faced by undergraduate students in the attempt to act ethically correct in cyberspace at the two universities;

I am hereby seeking your consent for the success of this exercise. To assist you in reaching a decision, I have attached to this letter:

- (a) A copy of an ethical clearance certificate issued by the University
- (b) A copy of the research instruments which I intend using in my research

Should you require any further information, please do not hesitate to contact me or my supervisor. Our contact details are as follows:

(+27633948676 or 08056446353 Email: rabshittu@yahoo.com)

Upon completion of the study, I undertake to provide you with a bound copy of the dissertation. Your permission to conduct this study will be greatly appreciated.

Yours sincerely,
Aderibigbe N A.



Signature



FEDERAL UNIVERSITY OF AGRICULTURE ABEOKUTA, NIGERIA

OFFICE OF THE REGISTRAR
Registrar: Mr. M. O. Ayoola, JP.
P.M.B. 2240, Abeokuta, Ogun State, Nigeria
e-mail: registrar@funaab.edu.ng
ayoolamo@funaab.edu.ng
Website: www.funaab.edu.ng
Tel: 234-803-391-8405

FUNAAB/REG.40A/VOL.IV/16/244

November 16, 2016

Mr. N. A. Aderibigbe,
University of Zululand,
Private Bag X1001,
KwaDlangezwa, 3886,
South Africa.

Dear Mr. Aderibigbe,

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH

Your letter dated September 10, 2016 on the above subject matter refers, please.

I write to convey the approval of the Vice-Chancellor, Professor Olusola Bandele Oyewole for you to conduct your Ph.D Research titled: "**Cyberethical Behaviour of Undergraduate Students in University of Zululand South Africa and Federal University of Agriculture, Abeokuta, Nigeria**" in the Federal University of Agriculture, Abeokuta.

Kindly liaise with Professor O. D. Akinyemi, Director, Academic Planning and Dr. O. Folorunsho, Head, Webometric Unit for briefing and other necessary information.

It is hoped that your research work will be beneficial to knowledge advancement.

Yours sincerely,

M. O. Ayoola, JP.
Registrar

Our Vision:
To be a Centre of Excellence in Knowledge generation for global development and the sustenance of an environmentally friendly society.

Our Mission:
To build future leaders and generate knowledge through research and intellectually stimulating environment for teaching, learning and community outreach towards sustainable development.

Appendix 3: Approval for the conduct of research field work at FUNAAB

Appendix 4: Notification of completion of research field work

	FEDERAL UNIVERSITY OF AGRICULTURE ABEOKUTA, NIGERIA
	OFFICE OF THE REGISTRAR Registrar: Dr. Hakeem 'Bola ADEKOLA P.M.B. 2240, Abeokuta, Ogun State, Nigeria e-mail: registrar@funaab.edu.ng bola.adekola@gmail.com Website: www.funaab.edu.ng Tel: +234 805 524 9564
	May 25, 2018
FUNAAB/REG.40A/VOL.IV/300	
Mr. N. A. Aderibigbe, University of Zululand, Private Bag X1001, KwaDlangezwa, 3886, South Africa.	
Dear Mr. Aderibigbe,	
NOTIFICATION OF COMPLETION OF PH.D RESEARCH WORK	
This is to confirm the completion of the research work in respect of the Ph.D thesis titled: <i>"Cyberethical Behaviour of Undergraduate Students in University of Zululand South Africa and Federal University of Agriculture, Abeokuta, Nigeria"</i> in the Federal University of Agriculture, Abeokuta.	
It is hoped that the research work will be beneficial to knowledge advancement.	
Thank you.	
Yours sincerely,	
 'Bola Adekola, Ph.D, FCIDA, FCIA Registrar	
Our Vision: To be a Centre of Excellence in Knowledge generation for global development and the sustenance of an environmentally friendly society.	Our Mission: To build future great leaders and generate Knowledge through research and intellectually stimulating environment for teaching, learning and community outreach towards Sustainable development.

Appendix 5: Survey Research Questionnaire

University of Zululand



Faculty of Arts

Department of Information
Studies

Dear respondent,

**REQUEST TO PARTICIPATE IN THE SURVEY ON CYBERETHICAL BEHAVIOUR OF
UNDERGRADUATE STUDENTS AT THE UNIVERSITY OF ZULULAND,
KWADLANGEZWA, AND THE FEDERAL UNIVERSITY OF AGRICULTURE,
ABEOKUTA.**

I am a Doctor of Literature and Philosophy student in the Department of Information Studies at the University of Zululand, and I am conducting a research on *Cyberethical Behaviour of Undergraduate Students at the University of Zululand*.

I am requesting your participation in my study by answering the attached questionnaire. Kindly respond to all questions as indicated.

The information provided will inform the institution's requisite measures and strategies to advance the purpose of cybertechnology provisions within the university.

Kindly note that there are no wrong answers from the choices given. Your honest opinion will be very much appreciated. You are not required to write your name on the questionnaire. The information collected in this questionnaire will be used strictly for the purpose of this research and will be treated with utmost confidentiality. Feel free to ask for clarification where necessary.

I kindly ask for your time to complete the questionnaire based on your knowledge and experience, and return at your earliest convenience. Your frank feedback will be taken as an important

contribution to this study.

Note: Some terms in this questionnaire are explained for clarity and understanding to aid your response.

Thanking you in advance for
your time.

Yours sincerely



Aderibigbe Nurudeen Adeniyi 201445518@stu.unizulu.ac.za

0604317046 Department of Information Studies

University of Zululand

QUESTIONNAIRE ON CYBERETHICAL BEHAVIOUR OF UNDERGRADUATE STUDENTS AT THE UNIVERSITY OF ZULULAND, KWANDLANGEZWA, AND THE FEDERAL UNIVERSITY OF AGRICULTURE, ABEOKUTA

Dear respondent,

Thank you for participating in this survey for a PhD study on cyberethical behaviour of undergraduate students at the University of Zululand, KwaDlangezwa. I solicit your support in completion of the questionnaire. All information provided will be treated with utmost confidentiality and used only for the purpose of the research.

Cyberethical behaviour is a term related to cyberethics, which is the study of users' behaviour and the choices they make while using the computer, smartphone and other devices that are connected to the Internet: e.g downloading of music, films, online porn, privacy violation, hacking, software piracy, identity theft, disseminating junk email, writing and disseminating viruses and worms, etc.

Cybertechnology includes the computer, laptop, smartphone (mobile phone) and the World Wide Web (internet, intranet connectivity, etc).

You are requested to choose the best option from the alternatives provided in each case.

Section A: Demographic data of respondents

Please mark with (×) one of the options that best applies to you.

1. Faculty:

Arts [] Education [] Science and Agriculture [] Commerce, Administration and Law []

2. Gender

Male [] Female [] Non-conforming []

3. Age

17 – 20 [] 21 – 25 [] 26 above []

4. Current year of study: 100 level [] 200 level [] 300 level [] 400 []

5. Cybertechnology skills: Beginning [] Intermediate [] Advanced []

6. How long have you been using cybertechnology?

Less than a year [] 1-2 [] 3-4 [] 5-6 [] 7 years and above []

Section B: Awareness and types of cyberethical behaviour

7a. The table below contains a list of cyberethical behaviours. Please mark (x) for any of the cyber behaviours you are familiar with, using the following scales: 1= Not Aware, 2= Somehow Aware, 3= Not Sure, 4= Aware, 5= Fully Aware

NO.	Cyberethical behaviour	FA	A	NS	SA	NA
1	Cyberpiracy (software piracy: music and film downloading)					
2	Cybersex (online porn or pornography)					
3	Privacy violation					
4	Blackmailing and disseminating junk mail					
5	Disseminating fake news					
6	Cybercrime					
7	Cyberstalking					
8	Cyberfraud (i.e fraudulent online banking)					
9	Cyberbullying					
10	Hacking/carding/phreaking/cracking					
11	Cyber vandalism					
12	Accessing inappropriate or illegal online material					
13	Identity theft					
14	Denial of service attack					
15	Data mining (indirect gathering of personal information)					
16	Cybersquatting					
17	Spoofing and phishing					
18	Violating intellectual property					
19	Violating software licence agreement					
20	Using another user's password					
21	Unleashing worms and viruses					
22	Cybersquatting					
23	Cyber libel (false statements that harm people's reputation)					
24	Cyberterrorism					
25	Spoofing and phishing					

26	Cyberespionage					
27	Copyright violation					
28	Plagiarism					
29	Cyber smearing (embarrassment or humiliation on social media network)					
30	Worms and viruses (malicious programs shared with the intent of shutting down the network)					
31	Others please specify.....					

7b. The following is a list of some cybertechnologies. Please identify and mark (X) for any or all that you use and are familiar with.

1	Computer, PC, Laptop	FA	A	NS	SA	NA
2	Tablet, smartphone, mobile phone					
3	World Wide Web (intranet, internet)					
4	Others (Please specify.....)					

7c. Have you personally received orientation on ethical use of cybertechnology at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta?

Yes [] No []

If yes to question 7c, kindly specify which form of training or orientation.

.....
.....
.....
.....
.....
.....

7d. Please indicate your level of agreement with the following items or statements as applicable elements of cybertechnology behaviour awareness.

Scale: 1= Strongly Disagree, 2= Disagree, 3= Neutral, 4=Agree, 5=Strongly Agree

		SA	A	N	D	SD
1	User awareness of the appropriate use of cybertechnology can influence cyber behaviour.					
2	Being a student, I follow news and developments about cybertechnology.					
3	I sometimes read about problems of unethical use of cybertechnology.					
4	I seek advice on different forum on the Internet about uses of cybertechnology.					
5	As a student, I am aware of the problems and consequences of cybertechnology behaviour.					
6	Being able to recognise ethical issues has no influence on cyberethical behaviour.					
7	Cyberethical behaviour is affected by skills and knowledge of cybertechnology.					
8	The ability to make decision based on previous knowledge has an effect on cyber behaviour.					
9	The ability to resolve conflicts between educational goals and unethical desire can impact on cyberethical behaviour.					
10	Awareness of consequences of ethical decisions influences cyberethical behaviour.					
11	Education has an impact on cyberethical behaviour.					
12	I discuss with friends and people around me about cybertechnology behaviour issues.					

Any additional comments

.....

.....

.....

8. Undergraduate students' understanding of what constitutes cyberethical behaviour

		SA	A	N	D	SD
1	It is easy for me to spreading the wrong information about other people by means of cybertechnology.					
2	It is acceptable for me to download music and films from the Internet for free.					
3	Spreading false malicious programmes with the intent to shut down a network system is an easy task to perform with cybertechnology.					
4	It is acceptable for me to take on a different identity on the Internet for fun or profit.					
5	It is acceptable for me to use someone else's bank identity to make purchase or order items.					
6	It is acceptable for me to access and download copyrighted material from the Internet.					
7	It is acceptable for me to make copies of illegal software for friends.					
8	It is acceptable for me to distribute pirated software by means of cybertechnology.					
9	It is acceptable for me to gain illegal and unauthorised access to Cybertechnology (hacking) with the understanding that it is illegal.					
10	It is acceptable for me to read someone's email without their consent.					
11	It is acceptable for me to arranging to meet an individual for paid friendship with the likelihood that it will lead to sexual act.					
12	It is acceptable for me to use cybertechnology for gaming and gambling.					
13	It is acceptable for me to obtain someone's private details by means of cybertechnology.					
14	It is acceptable for me to wilfully use another person's password to access their social network account.					
15	It is acceptable to use cybertechnology as a means of cyberbullying.					
16	It is acceptable to visit cites with questionable antisocial gathering (e.g. religious cults, hate groups, terrorist groups).					
17	It is acceptable for me to appropriate other people's intellectual property through cybertechnology.					

Any additional comments

.....

9. Influence of attitude, subjective norm and perceived behavioural control on cyberethical behavioural intention

Use the scales given below to indicate how much you agree with or differ from each statement. Scale: 1= Strongly Disagree, 2= Disagree, 3= Not Sure, 4=Agree, 5=Strongly Agree

9a. Attitude toward cybertechnology behaviour

N o.	Attitude towards Cybertechnology Behaviour	SA	A	N	D	SD
1.	Incidents of cyberethical violation are viewed as good behaviour by students.					
2.	Reporting the incidences of cyberethical violations is not necessary.					
3.	Students should be allowed to engage in unethical use of cybertechnology if they can get away with it.					
4.	Unethical cybertechnology behaviour is attractive.					
5.	I will encourage another student to use cybertechnology unethically.					
6.	I consider cyberethical violation as a wise action to engage in.					
7.	It is rewarding to engage in cyberethical behaviour violation.					
8.	I consider carrying out the action as favourable.					

9b. Subjective norm

N o.	Influence of Subjective Norm on the Use of Cybertechnology	SA	A	N	D	SD
1.	I will have the support of my fellow students if I were to use cybertechnology unethically.					
2.	I have often observed other students in the habit of unethical use of cybertechnology on campus.					
3.	The university environment makes it easy to engage in unethical					

	cybertechnology behaviour.					
4.	My fellow students have the tendency to carry out this action.					
5.	As students we often encourage and support ourselves to carry out unethical use of cybertechnology.					
6.	My religious group will support me to engage in unethical cybertechnology behaviour.					
7.	My family will be happy to see me engage in unethical cybertechnology violations.					
8.	My faculty will want me to carry out the action.					

9c. Perceived behavioural control

No.	Influence of PBC on Unauthorised Use of Cybertechnology	SA	A	N	D	SD
1.	It is easy for me as a student to engage in unethical cyber behaviour.					
2.	In this university, it would be fairly easy for student to use cybertechnology unethically.					
3.	I rate the difficulty in engaging in cyberethical violation act easily.					
4.	It would feel comfortable engaging in unethical use of cybertechnology.					
5.	I could easily carry out unethical use of cybertechnology and not get caught.					
6.	As a student, I have the skill and resources to engage in unethical cybertechnology behaviours.					
7.	Whether or not, the university cybertechnology policy does not control or prevent my cybertechnology behaviour.					
8.	I would be able to carry out the act even when there was no one to show me.					

9d. Influence of Behavioural Intention towards Cybertechnology Behaviour

No.	Influence of BI towards Cybertechnology Acts	SA	A	N	D	SD
1.	Ethical guidance provided to students by the university is an effective method of achieving desired cybertechnology behaviour.					
2.	Depending on the situation, rewards and punishments are effective means of realising compliance with my institution's cyberethical behaviour expectation.					
3.	The actions of system administrators have no influence on whether students conform to university's cyberethics policy or not.					
4.	The students' opinion of what is acceptable behaviour in cyberspace is influence by their cultural background.					
5.	Some cyberethical intentions and behaviour may be determined by the religious background of the student.					
6.	Personal factors and variables like age, gender and skills contribute very little to students' concept of right cybertechnology behaviour.					
7.	Friends and peers impact a person's right and wrong cybertechnology behaviour.					
8.	Sometimes, the event in a student's personal life can influence their cybertechnology behaviour.					
9.	Students' personal beliefs also play a role in how they react to the university's policy on ethical cybertechnology behaviour.					
10.	The morale level of the university does not influence students' cybertechnology behaviour.					
11.	Students' cybertechnology ethical foundation is unaffected by their participation in the university's social organisation.					

Any additional

comments.....

.....

.....

10. Challenges of cyberethical behaviour on university campus

No.	Challenges of cyberethical behaviour on university campus	SA	A	N	D	SD
1.	Social negative influence					
2.	Brings about ease of performing illegal activities (cybercrimes)					
3.	Lack of adequate security measures to ensure compliance with cyberethics policy					
4.	Lack of enough orientation and education on implications of ethical violations of cybertechnology use					
5.	Lack of policy guidance on use and appropriate cyber behaviour					
6.	Appropriate knowledge of cyber behaviour is very poor					
7.	Contradiction between copyright and freedom of information					
8.	Lack of cyber morality and ethical conduct in the use of cybertechnology					
9.	Negative violations of the integrity of the institution's cyber infrastructure					
10.	Exposure of the institution's network to virus and malware					
11.	Misuse of institution's license software and hardware					
12.	Lack of moral or ethical responsibility in the use of cybertechnology					
13.	Breaches in confidentiality and network security					
14.	Lack of knowledge of users' identity by network administrator					
15.	Lack of publicised policies about the ethical use of cybertechnology in students' handbooks					
16.	Lack of ethical consideration and consequence of violations					
17.	Data theft and loss of sensitive private, institution information					
18.	Compromised accounts or passwords					
19.	Privacy violations					
20.	Risk to anonymity of users					
21.	Theft of copyrighted materials					

Any additional

comment.....

.....

.....

Thank you for your time!

Appendix 6: Interview Schedule



University of Zululand Faculty of Arts

Department of Information Studies

Interview Schedule

Cyberethical Behaviour of Undergraduate Students at the University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta

Note: *Cyberethical behaviour is a term related to cyberethics, which is the study of users' behaviour and the choices they make while using the computer, smartphone and other devices connected to the Internet: e.g, downloading of music, films, online porn, privacy violation, hacking, software piracy, identity theft, disseminating junk email, writing and disseminating viruses and worms, etc. Cybertechnology includes the computer, laptop, smartphone (mobile phone) and the World Wide Web (internet, intranet connectivity, etc).*

RQ. Awareness of cyberethics at the University of Zululand

1a. Have you encountered any unethical cyber behaviour incidents during your professional work experience with students?

a) No b) Occasionally c) Frequently d) Frequently

1b. Which unethical or antisocial cyber behaviour incidents are occurring as a result of students' use of cybertechnology on the computers of the University of Zululand?.....

.....

.....

.....

.....

.....

.....
.....

2 Are there orientations or specific lessons for students on ethical use of cybertechnology and the Internet?.....

.....
.....
.....
.....
.....
.....
.....

3 How is cyberethics being addressed with students?

.....
.....
.....
.....
.....
.....

4 Who talks to students about cyber hacking, music and films download and other illegal use of the university's network as an ethical issue?.....

.....
.....
.....
.....
.....

5 Do you as administrators feel that cybertechnology-related ethical issues have increased in the University of Zululand campuses and, if so, why?.....

.....
.....300.....

.....

.....

.....

6a. Do you as administrators feel that cybertechnology-related ethical issues have increased in the University of Zululand campuses and if so, why?.....

.....

.....

.....

.....

.....

6b. Is there any effect or implication of unethical cybertechnology-related issues on the overall performance of the university's technology infrastructure?

a) Has decisive effect b) Has slight effect c) Has no effect

6c. What are the difficulties of developing a strong cyberethical awareness among undergraduate students in Unizulu?

a) Lack of support from management b) prevailing trend within the institution c) Negative effect on institution's finances

RQ. Cyberethics policy at the University of Zululand

7. What steps or precautions have been taken to resolve ethical problems?.....

.....

.....

.....

.....

.....

.....
.....

8. Does the university have written policies regarding appropriate use of cyber technology by students on campus

.....
.....
.....
.....
.....
.....
.....

9. What are limiting factors contributing to a lack of cyberethics policy at the University of Zululand?.....

.....
.....
.....
.....
.....
.....

10. How do you as an administrator believe a cyberethics policy should be aligned with the mission and purpose of higher education or the overall mission of the University of Zululand?.....

.....
.....
.....
.....

11. What do you consider the best way to communicate a cyberethics policy and encourage cyber technology users to believe in

it?.....
.....
.....
.....
.....
.....
.....
.....

12. **How does the University, through your section, monitor compliance with ethical use of cybertechnology?**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

13. **In what ways does your section enforce cybertechnology policy, and should this apply equally to students, staff and faculty?**

.....
.....
.....
.....
.....
.....
.....
.....

Thank you very much for your time!

Aderibigbe, N. A.

201445518@stu.uniz

ulu.ac.za

rabshittu@yahoo.co

m Researcher/PhD

student 0604317046.

Supervisor

Prof. Dennis Ocholla

ochollaD@unizulu.ac.za