10

CYBER ETHICAL BEHAVIOUR OF UNIVERSITY STUDENTS: AN OVERVIEW OF UNIVERSITY OF ZULULAND, SOUTH AFRICA AND FEDERAL UNIVERSITY OF AGRICULTURE, ABEOKUTA, OGUN STATE, NIGERIA

Nurudeen Adeniyi ***ADERIBIGBE[1] &*** Kehinde Abayomi, ***OWOLABI[2]***
'Nimbe Adedipe Library, Federal University of Agriculture, Abeokuta , Ogun State, Nigeria[12]
aderibigbena@funaab.edu.ng, rabshittu@yahoo.com[1], yomiowolabi2000@yahoo[2]

Abstract

Purpose: *The study aims to find out the cyber ethical behavior of undergraduates in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria.*

Design/Methodology/Approach: *The study adapted the Theory of planned Behaviour of Ajzen (1991; 2011) and adopts a triangulation method between quantitative and qualitative studies hence, information was obtained through the questionnaire and interview guide. The instruments were subjected to validity and reliability using the Cronbach alpha analysis and the results were provided in this study. A proportionate random sampling technique was used to select 380 students: 188 students from University of Zululand, SA and 192 students from Federal University of Agriculture, Abeokuta, Nigeria.*

Findings: *The findings of this study showed that students have intermediate cyber technology skills: higher in South Africa than in Nigeria and they have been using it for approximately 7 years. The findings of this study showed that attitude of students towards cyber ethical issues is of average in the two universities used. There are few significant differences in the subjective norms among students with respect to cyber ethical issues between South Africa and Nigeria and it implies that students are been controlled by their friends/peers, and university environment and management. Also, perception and awareness of students of cyber ethical issues is minimal. The findings of this study showed a significant difference in the prevalence of level of selected cyber ethical behaviour between South Africa and Nigeria with Nigeria having a higher level of prevalence. The findings also showed that attitude toward, perception and awareness of cyber ethical issues, subjective norms, and perceived behavioural control are all important factors that could influence actual cyber behavior among students in South Africa and Nigeria.*

Originality/Value: *The study has contributed to literature by conceptualizing the phenomenon of cyberethics from the context of South Africa and Nigeria, which can generate debates for further discussions on cyberethics among African scholars*

Keywords: *Cyberethics, Awareness, Theory of planned behavior, Policy, University of Zululand, Federal University of Agriculture, Abeokuta*

Introduction

The recent spates of technological innovations and dynamics where everyone have become social actors in the use of internet brought about the spirited debate about the need to investigate cyber-ethics behaviour. Cyber ethics refers to the code of responsible behavior on the Internet (Center for Internet Security, 2018). Since the inception of the internet, hackers have labored to exploit it for selfish interest such as sophomoric mischief, theft, espionage, among others (Olivier, 2013). Symantec (2013) noted that cyber-attacks are increasing and they are becoming increasingly complex in existence. To this regard, various cyber security methods and solutions have been introduced with time, but these had showed no signs of stopping the various activities of hackers on the internet. To this end, social behavior and appropriate use of the internet become more crucial with the increasingly interconnected cyber-physical-biological environment that links devices, systems, data, and people (Berman and Cerf, 2017).

The elastic potential of the internet creates an integrated ecosystem that respond to a wide spectrum of human needs and activities, thereby increasing efficiency and opportunity, and hence empowering people through

technology advancement, and also empowering technology through human intelligence. Howbeit, at its worst, the internet can introduce a Pandora's Box of wrong behavior, and bring about consequences that are not deliberate, and other vice habits that are not societal friendly among users. Omiunu (2017) noted that information and communication technologies such as the internet can be used and affect users negatively such as the social capital, community and national development. However, Wurst, Smarkola, & Gaffney (2008); Olson, Codde, deMaagd, Tarkleson, Sinclair, Yook and Egidio (2011); Ifijeh, Michael-Onuoha, Ilogho and Osinulu (2015); among others have noted its positive impact. According to Berman and Cerf (2017), the difference between an internet that enhances society and one that diminishes it will be determined by users' ability to create an effective model for its governance. The need to curtail the negative use of the internet among users towards leveraging its positive potentials in enjoying the benefits and contributing to personal, community and national development has call for the need for cyber ethical behavior.

As an information society, Wong (1995) noted that the internet have become indispensable in lives hence, Onyancha (2015) stated the society is becoming increasingly dependent on the internet to carry out various activities such as communication through the use of e-mails, the use of computers for organ transplants and heart surgeries in human beings, etc. To this end, ethical issues and problems have raised more concerns in recent information society due to the increasing number of internet use and dependency (Onyancha, 2015). The internet has become an essential tool for education and entertainment in the life of students (Wu and Yang, 2011). The use of internet has provided faster and easy information access, file sharing, and transfer among students in university (Lysonski and Durvasula, 2008; and Karim, Zamzuri and Nor, 2009). In addition, Aliyu, Abdallah, Lasisi, Diyar and Zeki (2010) noted that students are the major user of internet, hence different cyber behaviours occur among them. Various types of cyber behaviours that could be exhibited by them include cybersex or pornography, privacy violation, blackmailing and disseminating of junk mail, disseminating fake news, cyber-fraud, cyber-bully, hacking, identity theft, violating intellectual property, violating software license agreement, using another user's password, etc. In addition, Aliyu et al. (2010) stated that university students are the major violators of cyber ethics issues, because they are often reckless when posting content and browsing and are also frequently involved in illegal usage of files and documents through continuous sharing and downloading of counterfeit software, TV series, movies, among others. Aliyu et al. (2010) and Chandarman and Niekerk (2017) noted that a range of factors contribute to the violation of cyber ethics issues such as laziness, economic standing, lack of training and education of users, knowledge, awareness, self-perception of skills, actual skills, attitudes, among others.

Adapting the Theory of Planned Behaviour (TPB) by Ajzen (1991; 2011), attitude toward behavior, subjective norms, and perceived behavioral control are major factors that could influence humans' social behavior variables such as behavioral intentions and actual behaviors. In addition, behavioural intention is also observed to affect actual behavior in the theory of planned behavior. To this end, there are five major variables in the TPB, attitude toward behavior, subjective norms, and perceived behavioral control are clearly the independent variables, while on the one hand, behavioural intention stands as a dependent variable to attitude toward behavior, subjective norms, and perceived behavioral control. On the other hand, it serves as independent variable to actual behavior. Leonard, Cronan, &Kreie (2004); Lee &Kozar (2005); Ifinedo (2012); and Chandarman and Niekerk (2017) noted that the Theory of Planned Behaviour has been found to be suitable in investigating individuals' ethical behaviour. Adapting the TPB to cyber ethical behavior, it could be assumed that attitude toward cyber ethical behavior, subjective norms, and perceived behavioral control towards cyber ethical behavior are important variables to be considered in behavioural intention and also actual behavior

of various cyber ethical behavior. Attitude refers to the extent to which a person has a favorable or unfavorable appraisal of the behavior of interest. Subjective norm refers to the belief about whether peers within the immediate society of a particular user approve or disapprove of such behavior in question. Perceived behavioral control refers to someone's perception of how easy or difficult such behavior of interest can be performed. Behavioral intention refers to the motivational influence to perform such behavior of interest.

Adapting the TPB in this study is germane because according to Cassim (2011), cybercrimes are thriving in the African continent and the fight against it seems not to be effective. In addition, the lack of ICT literacy and the absence of suitable legal frameworks to deal with cybercrimes at national and regional levels have compounded the problem (Cassim, 2011). Nevertheless, various attempts are being made to curtail cybercrime in Africa. According to the Internet Crime Complaint Center (2012), the number of complaints with respect to cyber issues and problems have continued to grow with USA having the highest number of related issues (91.2%), followed by Canada (1.4%), the UK (0.9%), Australia (0.7%) and India (0.6%). In Africa, cyber problems and issues appeared to be higher the most in South Africa (0.18%), followed by Nigeria (0.08%). Cassim (2011) affirmed that Nigeria is one of the major sources of many cyber ethical issues. To this end, this provides the reason why this study focused on students in South Africa and Nigeria.

In South Africa, the government has introduced cyber legislation to tackle the various cyber-crimes in the country (Cassim, 2011). The South African common law to combat cyber-crime the Electronic Communications and Transactions Act 25 of 2002 (ECT), section 51(6) (g) of the draft Cybercrimes and Cybersecurity Bill of South Africa, the adapted Council of Europe's Convention on Cyber Crime CETS N0 185 (CECC), among others are some measures adapted in the country to curtail cyber-crimes behavior in South Africa (Cassim, 2011 and Chandarman & Van Niekerk, 2017). For example, section 51(6) (g) of the draft Cybercrimes and Cybersecurity Bill in South Africa as stated by Minister of Justice and Correctional Services (2015) specified that there is a need to (ii) promote and provide guidance in development and implementation of situational analysis and awareness campaigns concerning the risk environment of the South African cyberspace; and (vi) cybersecurity training, education, research and development programmes amongst other initiatives. In Nigeria, there is no specific legislation to combat cyber-crime and issues (Akomolede, 2008; Cassim, 2011). This has made Nigeria to receive worldwide attention and bad reputation because of the bad cyber ethical behaviours and the lack of proper law enforcement has compounded the problem (Cassim, 2011). Notwithstanding, the level of violation of cyber ethical behaviour is still higher in South Africa (0.18%), than in Nigeria (0.08%) as stated by Internet Crime Complaint Center (2012).

This could influence the appropriate use of internet among the population and could also hinder users to enjoy the benefits that such innovation provides both in the short and long run. Furthermore, the difference in the rate of prevalence of cyber issues and problems in South Africa and Nigeria shows that besides having a legislation that could address cyber ethical behavior, there could be other important factors that may contribute to users' violation of cyber ethical behavior between users in South Africa and Nigeria. To this end, this study adapted the TPB to investigate the rate of violation of cyber ethical behaviour and also selected factors that could contribute to the increasing rate of cyber ethical issues among undergraduates in South Africa and Nigeria. The following research questions re used to drive this study:

i. Do students in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria possess positive attitude toward and cyber ethical behavior?
ii. How do peers approve or disapprove cyber ethical behavior among students in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?
iii. What are the perceptions of students on how easy or difficult cyber ethical behavior is in University of Zululand,

South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

iv. Are students aware of cyber ethical behaviours in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

v. What is the level of cyber ethical behavior among students in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

Also, the following hypotheses of this study are subjected to test at 0.05 level of significance:

Ho1: There is no significant relationship between attitude toward and actual cyber ethical behavior

Ho2: There is no significant relationship between awareness and cyber ethical behavior between undergraduates from SA and Nigeria

Ho3: There is no significant relationship between subjective norms and actual cyber ethical behavior

Ho4: There is no significant relationship between perceived behavioral control and actual cyber ethical behavior

Ho5: There is no significant difference in the rate of cyber ethical behavior between undergraduates from SA and Nigeria

Literature Review

The various transformations in the global information society have introduced several challenges influencing the society (Onyancha, 2015) which calls for attention and urgency to be addressed. One of these major components of the information society is the use of internet. Studies such as Wong (1995); Campbell & Stylianou (2009); Wu and Yang (2011); Onyancha (2015); Omiunu (2017); among others have affirmed that the internet has become a major part of humans' lives. The use of internet varies with respect to the users' needs. For example, Campbell &Stylianou (2009) noted that in organization, internet access and use has become ubiquitous because of its effect on employee's management, performance and also in extension, organizational performance. With respect to students, Wu and Yang (2011) noted that internet is an essential tool for education and entertainment in the life of students. This increase use of internet has introduced another facet of challenge called cyber ethical behavior.

Froehlich (2005) cited by Onyancha (2015) noted that cyberethics is a particular branch of computer ethics that is concerned with ethical issues related to the use of internet or cyberspace. According to Spinello and Tavani (2004), cyberethics can be defined as the field of applied ethics that examines moral, legal, and social issues in the development and use of cyber technology such as the internet. Several studies such as Peits and Waelbroeck (2006); Lysonski and Durvasula (2008); Campbell &Stylianou (2009); Wu and Yang (2011); Onyancha (2015); among others have revealed the use of the internet has constituted major societal challenge such as negative cyber ethical behavior. Although, the effect of internet could be said to be felt across all aspects of human lives, such as work, home, education, etc. (Lysonski and Durvasula, 2008; Karim et al., 2009; Campbell &Stylianou, 2009). However, Wu and Yang (2011) have noted that it constitutes a big societal problem, and despite the magnitude of the problems, there has been little research exploring the internet users' behavior and ethical dimensions related cyber behavior especially among students. In addition, Wu and Yang (2011) noted that there is lack of research exploring users' cyber ethical behavior. Furthermore, while several studies have provided the level of the students' engagement in cyber ethical behaviours is important to emphasis that understanding the reason for student's engagement in such cyber ethical behavior is imminent (Peits and Waelbroeck, 2006; Lysonski and Durvasula, 2008).

According to Aliyu et al. (2010) university students are the culprit of cyber ethics issues and problems due to their daily involvement in thoughtless posting of content and evasive browsing and surfing the internet for several reason which is known to be equated to their life styles and peer exposure. They are also involved in the frequent illegal usage of files and documents through continuous sharing and downloading of counterfeit software such as games, apps. They most often use it to watch TV series, movies, listen to musics, among others.

Hence, the need to understand the factors that contribute to students' misuse of the internet and the continuous cyber ethical issues raised by several studies is germane to providing a necessary ground breaking knowledge that could set the pace into cushioning cyber ethical issues in Africa. Although, according to Aliyu et al. (2010) and Chandarman and Niekerk (2017), some range of factors have been noted to influence cyber ethical behavior, these are laziness, economic standing, lack of training and education of users, knowledge, awareness, self-perception of skills, actual skills, attitudes, among others. To extend the frontier of knowledge in the study of cyber ethical behavior, this study adapted the Theory of Planned Behaviour of Ajzen (1991; 2011) to provide a more elaborate and practical factors that could contribute to cyber ethical issues in Africa.

Research Framework

The study adapted the Theory of planned Behaviour of Ajzen (1991; 2011) (Figure 1). From figure 1, the theory of Planned Behaviour (TPB) by Ajzen (1991; 2011) has five major variables of interest which are: attitude toward behavior, subjective norms, perceived behavioral control, behavioral intentions and actual behaviors. Attitude toward behavior, subjective norms, and perceived behavioral control are the independent variables of TPB while actual behavior is the dependent variable. In the TPB, behavioral intention serves as a dependent variable when considering the relationship between in the IVs and behavioral intention on one part. On the other hand, it also serves as an independent variable to actual behaviour.

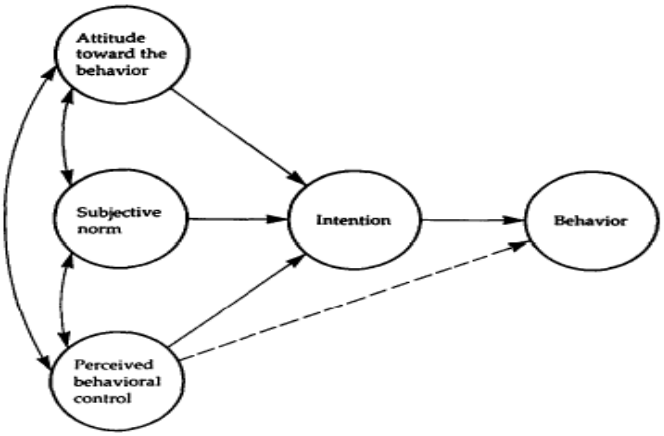

Figure 1: Theory of Planned Behaviour (Ajzen, 1991)

The figure 1 shows that, there is a significant relationship between each of the IVs (attitude toward behavior, subjective norms, and perceived behavioral control) and behavioral intentions. Also, behavioral intention is also shown to influence actual behavior of interest. However, behavioural intention was excluded from the TPB in the conceptual framework this study (figure 2) for several reasons. First, this study focuses on actual cyber ethical behaviours not the behavioural intention. Second, the relationship between behavioural intentions and actual behaviour is said to be complex and depends on several factors beyond the individual's control, such as the strength of the intention, and behaviour relation is also moderated by actual control over the behavior (Ajzen, 2011). Third, this study may not be interested in investigating and does not focus on the factors that affect the relationship between behavioural intention and actual behavior as it would be a distraction from the focus of this present study. Fourth, behavioural intention in the TPB framework holds two positions: in the first, it serves as a dependent variable for attitude, subjective norms and perceived control; second, it serves as independent variable for actual behavior. In this study, only one dependent variable is of interest: actual cyber ethical behavior among students. To this effect, behavioural intention was removed from this study hence, four major variables were adapted from the TPB and used to formulate a conceptual framework for this study (Figure 2).

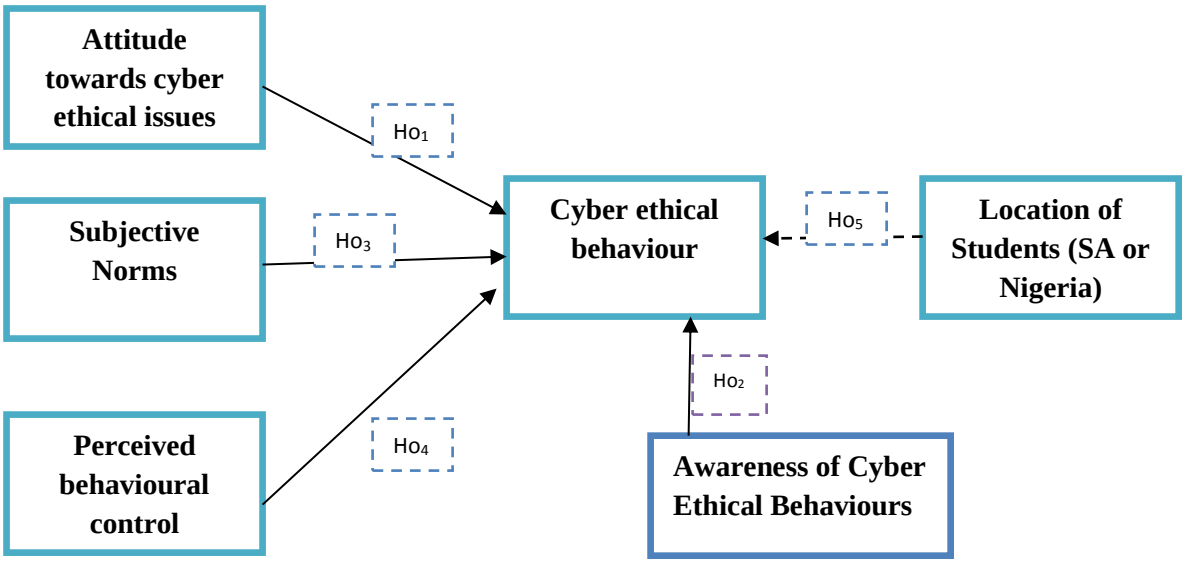

Figure 2: Conceptual Framework for the study: Correlates of Cyber ethical Behvaiour Framework

Source: The Author

From figure 2, attitudes towards ethical issues could be assumed to influence cyber ethical behaviours among student. Subjective norm is also assumed to influence cyber ethical behaviours among student. Also, perceived behavioural control is assumed to have significant influence on cyber ethical behaviours among student. In addition, students' location could also pose a significant difference in the rate of cyber ethical behaviours occurrence among students.

Research methods

The study adopts a triangulation method between quantitative and qualitative studies. The study population focuses on students from University of Zululand, SA and Federal University of Agriculture, Abeokuta, Nigeria. From the quantitative side, a correlational research design was adopted to explain the various factors that influence cyber ethical behaviours among students in universities in South Africa and Nigeria. To address this, the questionnaire was used to obtain information from the respondents. Adapting the TPB in figure 1, the questionnaire was divided into five sections namely demographic characteristics, attitude toward cyber ethical issues, subjective norms, perceived behavioral control and actual cyber ethical behavior with respect to the conceptual framework of this study in figure 2. The questions of the variables of interest in this study were captured through a five likert scale which the respondents are allowed to choose one from the options provided. The total number of undergraduate students in the University of Zululand is 15542 (Fact & figure, 2017) and the total number of undergraduate students in federal University of Agriculture Abeokuta is 15847. The total population of the two universities is 31,389. Using the formula below, a sample size of 38 was drawn.

$$n = \frac{N}{1 + \left[\frac{N\left(\frac{L}{100}\right)^2}{1.96^2 p(p-1)}\right]}$$

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% coincide 1.96; N is 31,389.

$$n = \frac{31389}{1 + \left[\frac{31389\left(\frac{5}{100}\right)^2}{1.96^2 \times 0.5(0.5-1)}\right]}$$

n=379.515

n = 380

The random sampling technique was used to select 380 students and a proportionate sampling technique was adopted to select 188 students from University of Zululand, SA and

192 students from Federal University of Agriculture, Abeokuta, Nigeria. The study used the Hoyle, Harris and Judd (2002) to get the sample size from each cluster, this is presented in table 1.

Table 1: Summary of sample size for undergraduate cyberethicalbehaviour

FACULTIES/UNIVERSITIES	STUDENT POPULATION	SAMPLE SIZE	PERCENT
Faculty of Art	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%**

Also, with respect to the qualitative aspect of the study, interview guide is used to obtain information from the respondents of this study and a total of 14 respondents were used for the study. The instrument (questionnaire) was subjected to psychometric property test using the validity and reliability test. The validity test was done using content and construct validity test where all the contents of the questionnaire was ensured that they capture the variables of interest in the study and in the research questions and the hypotheses of the study. Also, with respect to the reliability analysis, the Cronbach Alpha was used to test twenty administered questionnaires different from the 380-sample size. From the Cronbach alpha analysis, result shows that, attitude toward behavior has a reliability result of .73, subjective norms have a reliability result of .81, perceived behavioral control has a reliability result of .76, while actual cyber ethical behavior gave a reliability result of .79. As stated by Kaplan and Saccuzzo (2001), a reliability coefficient of 0.6 and above is considered good while Cohen and Swerdlik (2009) stated that a reliability result of 0.9 and above is too high and shows redundancy among the items in the instrument.

Given the importance of ethics to this study, ethical considerations were put into consideration. Such include obtaining a written introductory letter from the University of Zululand to major departments that would be used from the two selected universities. Also, participation in the study was voluntary, and participants were provided with the opportunity to withdraw at any time should they find it unfit for them to participate in the study. Also, the information provided by the respondents was treated as anonymous as their identities were treated as anonymous when providing the results of the study.

The information obtained was subjected to analysis. For the quantitative data, information obtained were coded into the SPSS version 20, and the descriptive statistics such as cross tabulation of frequency and percentage and mode are used while regression analysis and t-test were done to test the relationship between the variables of interest at 0.05 level of significance. For the qualitative analysis, the responses obtained was subjected to thematic analysis where responses are arranged with respect to major themes and objectives of the study, and interpretation is made to provide

answers to the research objectives and questions of the study.

Results

The results of this study is divided into three sections: demographic characteristics of respondents, research question analysis using cross tabulation of frequency and percentage, regression and t-test analysis to test the hypotheses of the study.

Demographic Characteristics of Respondents

The demographic characteristics of respondents of this study are provided in table 2.

Table 2: Demographic Characteristics of Respondents

		Nigeria	South Africa	Total
Gender	Male	112 (58.3%)	84 (44.7%)	196 (51.6%)
	Female	80 (41.7%)	101 (53.7%)	181 (47.6%)
	Non-conforming	0 (.0%)	3 (1.6%)	3 (.8%)
Total		192 (100.0%)	188 (100.0%)	380 (100.0%)
Colleges	COLMAS	44 (22.9%)	45 (23.9%)	89 (23.4%)
	COLBIOS	11 (5.7%)	62 (33.0%)	73 (19.2%)
	COLVET	4 (2.1%)	41 (21.8%)	45 (11.8%)
	COLENG	18 (9.4%)	39 (20.7%)	57 (15.0%)
	COLANIM	20 (10.4%)	1 (.5%)	21 (5.5%)
	COLPLANT	16 (8.3%)	0 (.0%)	16 (4.2%)
	COLERM	21 (10.9%)	0 (.0%)	21 (5.5%)
	COLFHEC	7 (3.6%)	0 (.0%)	7 (1.8%)
	COLAMRUD	29 (15.1%)	0 (.0%)	29 (7.6%)
	COLPHYS	22 (11.5%)	0 (.0%)	22 (5.8%)
Total		192 (100.0%)	188 (100.0%)	380 (100.0%)
Age	17-20 years	41 (21.4%)	52 (27.7%)	93 (24.5%)
	21-25 years	125 (65.1%)	110 (58.5%)	235 (61.8%)
	26 years and above	26 (13.5%)	26 (13.8%)	52 (13.7%)
Total		192 (100.0%)	188 (100.0%)	380 (100.0%)
Year of Study	100 level	6 (3.2%)	17 (9.1%)	23 (6.1%)
	200 level	50 (26.3%)	66 (35.5%)	116 (30.9%)
	300 level	40 (21.1%)	51 (27.4%)	91 (24.2%)
	400 level	94 (49.5%)	52 (28.0%)	146 (38.8%)
Total		190 (100.0%)	186 (100.0%)	376 (100.0%)

The result in table 2 shows that males have the highest percentage of 52%: 58% from Nigeria and 45% from South Africa. COLMAS has the highest percentage of 23%: 23% from Nigeria and 24% from South Africa. Also, Respondents who have between the years brackets 21-25 years have the highest frequency (62%): 65% from Nigeria and 59% from South Africa. Furthermore, respondents in 400 level has the highest percentage (39%): 40% from Nigeria and 28% from South Africa.

Table 3: Cybertechnology Skills among Respondents

		Institutions		Total
		Nigeria	South Africa	
Cybertechnology skills	Beginning	37 (19.4%)	35 (18.7%)	72 (19.0%)
	Intermediate	113 (59.2%)	116 (62.0%)	229 (60.6%)
	Advance	41 (21.4%)	36 (19.2%)	77 (20.3%)
Total		191 (100.0%)	187 (100.0%)	378 (100.0%)
How long have you been using technology	Less than a year	15 (7.9%)	20 (10.7%)	35 (9.3%)
	1-2 years	30 (15.7%)	33 (17.6%)	63 (16.7%)
	3-4 years	43 (22.5%)	47 (25.1%)	90 (23.8%)
	5-6 years	44 (23.0%)	32 (17.1%)	76 (20.1%)
	7 years and above	59 (30.9%)	55 (29.4%)	114 (30.2%)
Total		191 (100.0%)	187 (100.0%)	378 (100.0%)

The result in table 3 shows that individuals with intermediate cybertechnology skills have the highest percentage (61%): 59% from Nigeria and 62% from South Africa. Also, individuals who

have used technology for above 7 years have the highest percentage (30%): 31% from Nigeria and 29% from South Africa. This implies that majority of students in Nigeria and South Africa have intermediate cyber technological skills and have been using it for above 7 years.

Research Question Analysis

This section provides descriptive statistics of the research questions in this study hence, there are five sub sections in this section, each addressing one research question.

Research Question One: What is the attitude of students toward cyber ethical behavior in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

The distribution of the attitude of students towards cyber ethical issues is presented in table 4.

Table 4: Distribution of the attitude of students towards cyber ethical issues

		Institutions		Total	Chi-Square
		Nigeria	South Africa		
Cyberethical violation should be viewed as good behavior	Disagree	79 (42.7%)	77 (42.3%)	156 (42.5%)	.641 (df=2; p=.726)
	Neutral	29 (15.7%)	34 (18.7%)	63 (17.2%)	
	Agree	77 (41.6%)	71 (39.0%)	148 (40.3%)	
Total		185 (100.0%)	182 (100.0%)	367 (100.0%)	
Reporting cyberethical violation is not necessary	Disagree	94 (50.8%)	102 (56.0%)	196 (53.4%)	1.583 (df=2; p=.453)
	Neutral	28 (15.1%)	29 (15.9%)	57 (15.5%)	
	Agree	63 (34.1%)	51 (28.0%)	114 (31.1%)	
Total		185 (100.0%)	182 (100.0%)	367 (100.0%)	
Students should be allowed to engage in unethical use of cybertechnology	Disagree	98 (53.0%)	109 (59.9%)	207 (56.4%)	2.805 (df=2; p= .246)
	Neutral	29 (15.7%)	30 (16.5%)	59 (16.1%)	
	Agree	58 (31.4%)	43 (23.6%)	101 (27.5%)	
Total		185 (100.0%)	182 (100.0%)	367 (100.0%)	
Unethical cybertechnologybehaviour would be attractive	Disagree	92 (49.7%)	105 (57.7%)	197 (53.7%)	3.409 (df=2; p= .182)
	Neutral	28 (15.1%)	29 (15.9%)	57 (15.5%)	
	Agree	65 (35.1%)	48 (26.4%)	113 (30.8%)	
Total		185 (100.0%)	182 (100.0%)	367 (100.0%)	
Not be policy guidance of the use and appropriate cyber behaviour	Disagree	24 (13.5%)	30 (17.0%)	54 (15.3%)	1.157 (df=2; p= .561)
	Neutral	38 (21.3%)	40 (22.7%)	78 (22.0%)	
	Agree	116 (65.2%)	106 (60.2%)	222 (62.7%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	
There is no need to increase the awareness on appropriate knowledge of cyber behaviour	Disagree	27 (15.2%)	32 (18.2%)	59 (16.7%)	2.295 (df=2; p= .317)
	Neutral	33 (18.5%)	41 (23.3%)	74 (20.9%)	
	Agree	118 (66.3%)	103 (58.5%)	221 (62.4%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	

The result in table 4 shows that there is no significant difference in the components of attitudes of students towards cyber ethical issues between South Africa and Nigeria (p>0.05). However, 42% stated that cyberethical violation should not be viewed as good behavior: Nigeria (43%) and South Africa (42%); and 53% stated that it is necessary to report cyberethical violation: Nigeria (51%) and South Africa (56%). Also, 56% stated that students should not be allowed to engage in unethical use of cyber technology: Nigeria (53%) and South Africa (60%); 53% stated that unethical cyber technology behaviour should not be made attractive: Nigeria (50%) and South Africa (58%). In addition, only 15% stated that the there is need for a policy guidance in the use of and appropriate cyber behavior: Nigeria (14%) and South Africa (17%); and 17% stated that there is need to increase the awareness on appropriate knowledge of cyber behavior. This implies that attitude of students towards cyber ethical issues are of average among students in Nigeria and South Africa. The qualitative response from respondent is also provided below:

", we as the administrator of the internet we are putting somethings 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 make 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" (FUNAAB, Nigeria)

" 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" (FUNAAB, Nigeria)

Research Question Two: How do peers approve or disapprove cyber ethical behavior among students in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

The distribution of the subjective norms among students in cyber ethical issues is presented in table 5.

Table 5: Distribution of subjective norms among students in cyber ethical issues

		Institutions		Total	Chi-Square
		Nigeria	South Africa		
Personal factors contribute very little to concept of right cyber technology behavior	Disagree	36 (20.2%)	51 (29.0%)	87 (24.6%)	7.210 (df= 2; p= .027)
	Neutral	36 (20.2%)	45 (25.6%)	81 (22.9%)	
	Agree	106 (59.6%)	80 (45.5%)	186 (52.5%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	
Friends and peers impact a person's right and wrong cyber technology behavior	Disagree	24 (13.5%)	40 (22.7%	64 (18.1%)	6.129 (df= 2; p= .047)
	Neutral	34 (19.1%)	37 (21.0%)	71 (20.1%)	
	Agree	120 (67.4%)	99 (56.3%)	219 (61.9%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	
Event in students' life can influence their cyber technology behavior	Disagree	17 (9.6%)	24 (13.6%)	41 (11.6%)	6.547 (df= 2; p= .038)
	Neutral	31 (17.4%)	46 (26.1%)	77 (21.8%)	
	Agree	130 (73.0%)	106 (60.2%)	236 (66.7%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	
Students' beliefs influence their reactions to university's policy	Disagree	31 (17.4%)	34 (19.3%)	65 (18.4%)	1.524 (df= 2; p= .467)
	Neutral	29 (16.3%)	36 (20.5%)	65 (18.4%)	
	Agree	118 (66.3%)	106 (60.2%)	224 (63.3%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	
The morale level of the university does not influence students cyber technology behavior	Disagree	41 (23.0%)	48 (27.3%)	89 (25.1%)	4.192 (df= 2; p= .123)
	Neutral	47 (26.4%)	58 (33.0%)	105 (29.7%)	
	Agree	90 (50.6%)	70 (39.8%)	160 (45.2%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	
Students cyber technology ethical foundation is unaffected by their participation in university society.	Disagree	42 (23.6%)	46 (26.1%)	88 (24.9%)	5.632 df= 2; p= .060)
	Neutral	43 (24.2%)	59 (33.5%)	102 (28.8%)	
	Agree	93 (52.2%)	71 (40.3%)	164 (46.3%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	

The result in table 5 shows that there is significant difference in some components of subjective norms among students with respect to cyber ethical issues between South Africa and Nigeria ($p<0.05$). For example, the result in table 5 shows that there is a significant difference between students in Nigeria (60%) and South Africa (46%) with respect to the importance of personal factors in contributing to cyber technology behavior. There is also a significant difference between students from Nigeria (67%) and South Africa (56%) with respect to the impact of friends and peers on cyber technology behavior. Also, there is a significant difference with respect to the effect of event in students' life on cyber technology behavior between students from Nigeria (73%) and South Africa (60%). The result shows that there is no significant difference in students' beliefs as a major influencing factor on the reactions to university's policy with respect to cyber ethical behavior between Nigeria (66%) and South Africa (60%). There is no significant difference in the morale level of the university and its influence on students' cyber technology behavior between Nigeria (51%) and South Africa (40%). Finally, there is no significant difference in students' cyber technology ethical foundation been unaffected by their participation in university society between Nigeria (52%) and South Africa (40%). This implies that students are been controlled by their friends/peers, university environment, among others in cyber ethical behavior.

Research Question three: What are the perceptions of students on how easy or difficult cyber ethical behavior is in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

The distribution of the perception of students of cyber ethical behaviour is presented in table 6.

Table 6: Distribution of the perception of students of cyber ethical behaviour

		Institutions		Total	
		Nigeria	South Africa		Chi-Square
Cyberethicalbehaviour is affected by the skills of cybertech	Disagree	24 (12.8%)	26 (14.0%)	50 (13.4%)	3.847 (df= 2; p= .146)
	Neutral	33 (17.6%)	47 (25.3%)	80 (21.4%)	
	Agree	131 (69.7%)	113 (60.8%)	244 (65.2%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
Ability to make decision has effect on cybertech	Disagree	23 (12.2%)	27 (14.5%)	50 (13.4%)	1.573 (df= 2; p= .455)
	Neutral	42 (22.3%)	49 (26.3%)	91 (24.3%)	
	Agree	123 (65.4%)	110 (59.1%)	233 (62.3%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
Ability to resolve conflict can impact cyberethicalbehavior	Disagree	22 (11.7%)	28 (15.1%)	50 (13.4%)	3.156 (df= 2; p= .206)
	Neutral	45 (23.9%)	55 (29.6%)	100 (26.7%)	
	Agree	121 (64.4%	103 (55.4%)	224 (59.9%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
Awareness of consequence of ethical decisions influence cyberethical behavior	Disagree	19 (10.1%)	31 (16.7%)	50 (13.4%)	5.303 (df= 2; p= .071)
	Neutral	32 (17.0%)	39 (21.0%)	71 (19.0%)	
	Agree	137 (72.9%)	116 (62.4%)	253 (67.6%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
Education impacts cyberethicalbehaviour	Disagree	20 (10.6%)	26 (14.0%)	46 (12.3%)	1.742 (df= 2; p= .419)
	Neutral	37 (19.7%)	29 (15.6%)	66 (17.6%)	
	Agree	131 (69.7%)	131 (70.4%)	262 (70.1%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
I discuss with friends about cyberetech	Disagree	29 (15.4%)	47 (25.3%)	76 (20.3%)	6.918 (df= 2; p= .031)
	Neutral	56 (29.8%)	58 (31.2%)	114 (30.5%)	
	Agree	103 (54.8%)	81 (43.5%)	184 (49.2%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	

The result in table 6 shows that there is no significant difference in the components of the perception of students of cyber ethical issues between South Africa and Nigeria (p>0.05).However, 65% stated that cyberethical behaviour is affected by the skills of cyber technology: Nigeria (70%) and South Africa (61%); 62% stated that the ability to make decision has effect on cyber technology: Nigeria (65%) and South Africa (59%). Also, 60% stated that the ability to resolve conflict can impact cyber ethical behavior: Nigeria (64%) and South Africa (55%); 67% stated that the awareness of consequence of ethical decisions influence cyber ethical behavior: Nigeria (73%) and South Africa (62%). Furthermore, 70% stated that education has impetus on cyber ethical behavior: Nigeria (70%) and South Africa (70%); and 49% stated that they use to discuss about cyber technology with their friends: Nigeria (55%) and South Africa (44%).

Research Question four: Are students aware of cyber ethical behaviours in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

The distribution of the awareness of students on cyber ethical related issues is presented in table 7.

Table 7: Distribution of awareness students on issues related to cyber ethical behaviour

		Institutions		Total	
		Nigeria	South Africa		Chi-Square
Aware of the problems of cyber ethical related issues	Not Aware	24 (12.8%)	30 (16.1%)	54 (14.4%)	1.271 (df= 2; p= .530)
	Not sure	37 (19.7%)	40 (21.5%)	77 (20.6%)	
	Aware	127 (67.6%)	116 (62.4%)	243 (65.0%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
Awareness of consequence of ethical decisions	Not Aware	19 (10.1%)	31 (16.7%)	50 (13.4%)	5.303 (df= 2; p= .530)
	Not sure	32 (17.0%)	39 (21.0%)	71 (19.0%)	
	Aware	137 (72.9%)	116 (62.4%)	253 (67.6%)	
Total		188 (100.0%)	186 (100.0%)	374 (100.0%)	
Awareness on appropriate knowledge of cyber behavior	Not Aware	27 (15.2%)	32 (18.2%)	59 (16.7%)	2.295 (df= 2; p= .317)
	Not sure	33 (18.5%)	41 (23.3%)	74 (20.9%)	
	Aware	118 (66.3%)	103 (58.5%)	221 (62.4%)	
Total		178 (100.0%)	176 (100.0%)	354 (100.0%)	

The result in table 7 shows that there is no significant difference in the components of the awareness among students of cyber ethical issues and behaviour between South Africa and Nigeria (p>0.05). However, the result of the study shows that 65% stated that they are aware of the problems of cyber ethical related issues: Nigeria (68%) and South Africa (62%). Also, 67% stated that they are aware of the consequences of various ethical decision: Nigeria (72%) and South Africa (62%). Moreover, 62% stated that they are aware of the various appropriate knowledge of cyber behavior: Nigeria (66%) and South Africa (59%).

Research question five: What is the level of cyber ethical behavior prevalence among students in University of Zululand, South Africa and Federal University of Agriculture, Abeokuta, Nigeria?

The distribution of the level of cyber ethical behavior prevalence among students is presented in table 8.

Table 8: Distribution the level of cyber ethical behavior prevalence among students

		Institutions		Total	
		Nigeria	South Africa		Chi-Square
Easy for me to spread wrong info by means of cybertech	Disagree	30 (16.0%)	53 (28.6%)	83 (22.3%)	11.356 (df= 2; p= .003)
	Neutral	24 (12.8%)	30 (16.2%)	54 (14.5%)	
	Agree	134 (71.3%)	102 (55.1%)	236 (63.3%)	
Total		188 (100.0%)	185 (100.0%)	373 (100.0%)	
Using someone else bank Identity to purchase items	Disagree	85 (45.2%)	102 (55.1%)	187 (50.1%)	
	Neutral	24 (12.8%)	31 (16.8%)	55 (14.7%)	7.978(df= 2; p= .019)
	Agree	79 (42.0%)	52 (28.1%)	131 (35.1%)	
Total		188 (100.0%)	185 (100.0%)	373 (100.0%)	
Easy to access and download copyrighted material	Disagree	54 (28.7%)	62 (33.5%)	116 (31.1%)	2.246(df= 2; p= .325)
	Neutral	26 (13.8%)	31 (16.8%)	57 (15.3%)	
	Agree	108 (57.4%)	92 (49.7%)	200 (53.6%)	
Total		188 (100.0%)	185 (100.0%)	373 (100.0%)	
Make and use a copy of illegal software	Disagree	66 (35.3%)	86 (46.7%)	152 (41.0%)	5.437(df= 2; p= .066)
	Neutral	37 (19.8%)	34 (18.5%)	71 (19.1%)	
	Agree	84 (44.9%)	64 (34.8%)	148 (39.9%)	
Total		187 (100.0%)	184 (100.0%)	371 (100.0%)	
Reading someone email without their consent	Disagree	95 (50.8%)	104 (56.5%)	199 (53.6%)	1.799(df= 2; p= .407)
	Neutral	25 (13.4%)	26 (14.1%)	51 (13.7%)	
	Agree	67 (35.8%)	54 (29.3%)	121 (32.6%)	
Total		187 (100.0%)	184 (100.0%)	371 (100.0%)	
Search and use someone private details	Disagree	84 (44.9%)	103 (56.0%)	187 (50.4%)	4.566(df= 2; p= .206)
	Neutral	28 (15.0%)	22 (12.0%)	50 (13.5%)	
	Agree	75 (40.1%)	59 (32.0%)	134 (36.1%)	
Total		187 (100.0%)	184 (100.0%)	371 (100.0%)	
Willfully using another person's password	Disagree	93 (49.7%)	101 (54.9%)	194 (52.3%)	1.306(df= 2; p= .521)
	Neutral	28 (15.0%)	28 (15.2%)	56 (15.1%)	
	Agree	66 (35.3%)	55 (29.9%)	121 (32.6%)	
Total		187 (100.0%)	184 (100.0%)	371 (100.0%)	
Acceptable Use cybertech for cyberbullying	Disagree	98 (52.7%)	114 (62.3%)	212 (57.5%)	4.013(df= 2; p= .134)
	Neutral	27 (14.5%)	25 (13.7%)	52 (14.1%)	
	Agree	61 (32.8%)	44 (24.0%)	105 (28.5%)	
Total		186 (100.0%)	183 (100.0%)	369 (100.0%)	

The result in table 8 shows that there few items show significant difference (p<0.05) while others do not show significant difference (p>0.05) in the prevalence of level of cyber ethical behaviour between South Africa and Nigeria. For example, there is a significant difference in the prevalence of the easy spread of wrong information by means of cybertech between Nigeria (71%) and South Africa (63%) (p<0.05). There is also a significant difference in the use of someone else bank identity to purchase items between Nigeria (42%) and South Africa (28%) (p<0.05). There is however no significant difference in the easy access to download copyrighted material between Nigeria (57%) and South Africa (50%) (p>0.05). Also, there is no significant difference in make and using a copy of illegal software between Nigeria (45%) and South Africa (35%) (p>0.05). There is no significant difference in reading of

someone email without their consent between Nigeria (36%) and South Africa (29%) (p>0.05). Also, there is no significant difference in the search and use of someone private details between Nigeria (40%) and South Africa (32%) (p>0.05). In addition, there is no significant difference in the willfully use of another person's password between Nigeria (35%) and South Africa (29%) (p>0.05). Moreover, there is no significant difference in the acceptable use of cybertech for cyberbullying between Nigeria (33%) and South Africa (24%) (p>0.05). This implies that the prevalence of cyber ethical behavior among students is low among students but where it exists, it is higher among students in the Nigeria than those in South Africa.

The result from the qualitative study also show some responses from the respondents with respect to the level of cyber behaviours exhibited by students. From the interview, the responses of some of the respondents are provided below:

"…, for students when you give them access to the internet, they will try to access anything, to download movies, access porn sites. Although most of the porn sites are blocked, but yet you find our student trying to circumvent the security barriers to gain access to these sites" (UZ, SA)

"…, for a number of students, it is normal for them 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 student will log in into the system and do the very same thing they said they wouldn't do by accepting the rule" (UZ, SA)

"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 these is consequence on their use of cyber technology ." (FUNAAB, Nigeria)

"...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." (FUNAAB, Nigeria)

Testing of Hypotheses of the Study

Also, the following hypotheses of this study are subjected to test at 0.05 level of significance:

Ho1: There is no significant relationship between attitude toward and actual cyber ethical behavior

The regression analysis result of hypothesis one is presented in table 9. The adjusted R Square was .297 showing that the variable attitude toward cyber ethical issues constitutes a major factor influencing actual cyber ethical behavior among students by approximately 30%. This shows that there are other factors that constitute important variable but are not part of this analysis, which this model fail to inculcate into this analysis.

Table 9: Regression Analysis for Hypothesis One

Coefficients[a]					
Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	11.142	1.901		5.861	.000
Attitude of students	1.848	.151	.547	12.223	.000

a. Dependent Variable: Cyber ethical behavior

The result in table 9 shows that attitude toward cyber ethical issues is found to be significant (p<0.05), and predicts actual cyber ethical behavior among students. Thus, the null hypothesis one is rejected and hence, there is a significant relationship between attitude toward and actual cyber ethical behavior among students in South Africa and Nigeria.

Ho2: There is no significant relationship between awareness and cyber ethical behavior between undergraduates from SA and Nigeria

The regression analysis result of hypothesis two is presented in table 10. The adjusted R Square was .025 showing that the variable awareness of cyber ethical issues among students constitutes to a little extent a factor influencing actual cyber ethical behavior among students by approximately 3%. This shows that there are other major factors that constitute important variable but are not part of this analysis, which this model fail to inculcate into this analysis.

Table 10: Regression Analysis for Hypothesis two

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	25.349	2.712		9.347	.000
	Awareness	.126	.039	.167	3.230	.001

a. Dependent Variable: Cyber ethical behavior

The result in table 10 shows that awareness of cyber ethical related issues is found to be significant ($p<0.05$), and predicts actual cyber ethical behavior among students. Thus, the null hypothesis two is rejected and hence, there is a significant relationship between awareness of and cyber ethical behavior among students in South Africa and Nigeria.

Ho3: There is no significant relationship between subjective norms and actual cyber ethical behavior

The regression analysis result of hypothesis three is presented in table 11. The adjusted R Square was .095 showing that the variable subjective norms among students with respect to cyber ethical issues constitutes to a little extent a factor influencing actual cyber ethical behavior among students by approximately 9%. This shows that there are other major factors that constitute important variable but are not included in this analysis, which this model fails to inculcate into this analysis.

Table 11: Regression Analysis for Hypothesis three

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	16.659	2.811		5.927	.000
	Subjectivenorms	1.013	.165	.312	6.146	.000

a. Dependent Variable: Cyber ethical behavior

The result in table 11 shows that subjective norms among students in respect to cyber ethical related issues is found to be significant ($p<0.05$), and predicts actual cyber ethical behavior among students. Thus, the null hypothesis three is rejected and hence, there is a significant relationship between subjective norms and cyber ethical behavior among students in South Africa and Nigeria.

Ho4: There is no significant relationship between perceived behavioral control and actual cyber ethical behavior

The regression analysis result of hypothesis three is presented in table 12. The adjusted R Square was .046 showing that the variable perceived behavioural control among students with respect to cyber ethical issues constitutes to a little extent a factor influencing actual cyber ethical behavior among students by approximately 5%. This shows that there are other major factors that constitute important variable but are not included in this analysis, which this model fails to inculcate into this analysis.

Table 12: Regression Analysis for Hypothesis four

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	19.771	3.307		5.978	.000
	Perceivebehaviouralcontrol	.713	.164	.221	4.339	.000

a. Dependent Variable: Cyber ethical behavior

The result in table 12 shows perceived behavioural control among students in respect to cyber ethical related issues is found to be significant ($p<0.05$), and predicts actual cyber ethical behavior among students. Thus, the null hypothesis four is rejected and hence, there is a significant relationship between perceived behavioural control and cyber ethical behavior among students in South Africa and Nigeria.

Ho5: There is no significant difference in the rate of cyber ethical behavior between undergraduates from SA and Nigeria

The significant difference in the rate of cyber ethical behavior between undergraduates from SA and Nigeria is presented in table 13. The use of T-test was adopted to analyse the significant difference between the tow locations: Nigeria and South Africa.

Table 13: T-test was of Hypothesis five

	Institutions	N	Mean	Std. Deviation	Df	t-result	Sig. (2-tailed)	Comments
Cyber ethical behavior	Nigeria	185	35.3892	10.93607	364.563	2.588	.010	Significant
	South Africa	182	32.4066	11.13749				

The result in table 13 shows that there is a significant difference in the rate of cyber ethical behavior between undergraduates from SA and Nigeria($p<0.05$), and hence, the null hypothesis five is rejected and hence, there is a significant difference between undergraduates from SA (Mean= 32.4066) and Nigeria (Mean = 35.3892) with respect to the rate of cyber ethical behavior.

Discussions

The findings of this study showed that students have intermediate cyber technology skills: higher in South Africa than in Nigeria and they have been using it for approximately 7 years. This props the work of Cassim(2011) that the lack of ICT literacy at national and regional levels have compounded the cyber ethical problems. There is no significant difference in the attitudes of students towards cyber ethical issues between South Africa and Nigeria. Also, attitude of students towards cyber ethical issues is of average among students in Nigeria and South Africa. This is because, in most occasions, students' attitudes are monitored and also guided by relevant ICT policy. The level of monitoring and existence of ICT related policy have addressed the attitude of students towards cyber ethical issues and behavior. This could be used to support the reasons why Wurst et al. (2008); Olson et al. (2011); Ifijeh et al. (2015); among others stated that ICT could have positive impact on social capital, community and national development.

There are few significant differences in some components of subjective norms among students with respect to cyber ethical issues between South Africa and Nigeria and implies that students are been controlled by their friends/peers, university environment, among others in their cyber ethical behavior. The findings of this study showed that there is no significant difference in the perception of students of cyber ethical issues between South Africa and Nigeria. However, students have accurate perception of cyberethical issues. There is no significant difference in the awareness among students of cyber ethical issues and behaviour between South Africa and Nigeria. However, students in South Africa and Nigeria are accurately aware of the issues surrounding cyber ethical behavior.

The findings of this study showed a significant difference in the prevalence of level of selected cyber ethical behaviour between South Africa and Nigeria. For example, the prevalence of the easy spread of wrong information by means of

cybertechis higher in between FUNNAB, Nigeria thanUniversity of Zululand, South Africa. The use of someone else bank identity to purchase items is also higher inNigeria than in South Africa. But there is no significant difference between Nigeria and South Africa in the easy access to download copyrighted material; using a copy of illegal software; reading of someone email without their consent; searching and using of someone private details; willfully using of another person's password; and the using of cybertech for cyberbullying. This implies that the prevalence of cyber ethical behavior among students is low among students but where it exists, it is higher among students in the Nigeria than those in South Africa. This supports the works of Cassim (2011) to an extent that negative cyber behaviours are thriving in the African continent and the fight against it seems not to be effective. This bolsters the works of Wong (1995);Lysonski and Durvasula (2008); Karim et al. (2009); Aliyu et al.(2010);Wu and Yang(2011); and Onyancha (2015) that the existence of cyber ethical issues among students in the university system is attributed to the fact that educational activities are fully relying on the internet to be carried out. This also props up the findings of Aliyu et al. (2010) that there exist various kinds of cyber behaviours among students.

This supports the works of Olivier(2013) and Symantec (2013) that cyber ethical issues have increased since the inception of the internet and are becoming increasingly complex in existence. This bolsters the work of Omiunu (2017) that the ICT such as the internet can be used to affect users negatively such as the social capital, community and national development. Hence despite the significant benefits of the use of internet, if not monitored and cushioned with existing and relevant ICT policies, it may tend to affect the social capital, community and national development. This supports the work of Berman and Cerf (2017) that the creationof effective model for its governance creates an impetus to distinguish between an internet that enhances society and one that diminishes it.This concurs with the work of Cassim(2011) that the absence of suitable legal frameworks to deal with cyber crimes at national and regional levels has compounded the cyber ethical problems.

There is a significant relationship between attitude toward and actual cyber ethical behavior among students in South Africa and Nigeria. This supports the works of Aliyu et al. (2010) and Chandarman and Niekerk (2017) that attitude serves as major factor that influences cyber behaviours among internet users. The finding of this study also concurs with the work of Ajzen (1991; 2011) that attitude serves as major factor that influences behaviours which in this present study is referred to as cyber behavior among internet users. The significant importance of the attitude of students with respect to cyber ethical behavior could be a major reason why the works of Leonard, Cronan, &Kreie (2004); Lee &Kozar (2005); Ifinedo (2012); and Chandarman and Niekerk (2017) affirmed that the Theory of Planned Behaviouris suitable in investigating individuals' ethical behaviour.

There is a significant relationship between awareness of and cyber ethical behavior among students in South Africa and Nigeria. This supports the works of Aliyu et al. (2010) and Chandarman and Niekerk (2017) that awareness serves as major factor that influences cyber behaviours among internet users. There is a significant relationship between subjective norms and cyber ethical behavior among students in South Africa and Nigeria. The finding of this study concurs with the work of Ajzen (1991; 2011) that subjective norm serves as major factor that influences behaviours which in this present study is referred to as cyber behavior among internet users. The significant importance of subjective norms with respect to cyber ethical behavior could be one of the major reasons why the works of Leonard, Cronan, &Kreie (2004); Lee &Kozar (2005); Ifinedo (2012); and Chandarman and Niekerk (2017) affirmed that the Theory of Planned Behaviouris suitable in investigating individuals' ethical behaviour.

There is a significant relationship between perceived behavioural control and cyber ethical behavior among students in South Africa and Nigeria. This supports the works of Aliyu et al. (2010) and Chandarman and Niekerk (2017) that perception serves as major factor that influences cyber behaviours among internet users. The finding of this study also concurs with

the work of Ajzen (1991; 2011) that perceived behavioural control serves as major factor that influences behaviours which in this present study is referred to as cyber behavior among internet users. The significant importance of perceived behavioural control with respect to cyber ethical behavior could be one of the major reasons why the works of Leonard, Cronan, &Kreie (2004); Lee &Kozar (2005); Ifinedo (2012); and Chandarman and Niekerk (2017) affirmed that the Theory of Planned Behaviouris suitable in investigating individuals' ethical behaviour.

There is a significant difference between undergraduates from SA and Nigeria with respect to the rate of cyber ethical behavior. Rate of cyber ethical behavior is higher among students in FUNNAB than those in University of Zululand. This contrasts the findings of the Internet Crime Complaint Center (2012) that the number of complaints with respect to cyber issues and problems have continued to grow and higher in South Africa than in Nigeria. This significant difference of the rate of cyber behaviours in the study of the Internet Crime Complaint Center (2012) and the findings of this present study between Nigeria and South Africa could be attributed to the difference in the year gap between the two studies. Also, the difference could be attributed to the fact that there exist various ICT policies as stated by Cassim(2011) to curtail cyber behavior among users in South Africa which does not exist in Nigeria as stated by Akomolede (2008) and Cassim (2011). This supports why Cassim(2011) noted that this increase in bad cyber behaviours and the lack of proper law enforcement has compounded the problem of cyber issues and has made Nigeria to receive worldwide attention and bad reputation.

Conclusion and Recommendations

In conclusion, negative cyber behaviors are higher among students in Federal University of Agriculture, Abeokuta, Nigeria than those in University of Zululand, SA. Major factors that have led to this significant prevalence of cyber behaviours are attitude of students, towards cyber ethical issues, perceptions of students, subjective norms and their perceived behavioural control. In addition, major intermediate variables that could affect the level of cyber ethical behavior, attitudes, perception, subjective norms and the perceived behavioral control with respect to cyber ethical behavior are the lack of ICT literacy and the lack of ICT policy to tackle cyber related issues. To this hence, various recommendations were provided from the findings of this study and include:

There is need for the two institutions in Africa to provide a working ICT policy that would be used to curtail negative cyber behaviours and enhance good ethical behavior in the use of internet among students.

The management of the universities should endeavour to make it possible to provide a positive cyber ethical culture in the university system that would accommodate positive cyber behaviours among students and their fellow colleagues.

The management of the institutions should also provide awareness strategies through the universities' sites and also other information dissemination outlets of the university to enhance the consciousness of cyber ethical issues in the universities.

The students should also endeavour to see to it that the indiscriminate use of internet is curtailed and they should use it with respect to the ICT policy of the institutions.

References

AjzenIcek (2011). The theory of planned behaviour: Reactions and reflections, Psychology & Health, 26:9, 1113-1127, DOI: 10.1080/08870446.2011.613995.

Ajzen, Icek (1991). "The theory of planned behavior". Organizational Behavior and Human Decision Processes. 50 (2): 179–211. doi:10.1016/0749-5978(91)90020-T.

Akomolede T.I. (2008), 'Contemporary legal issues in electronic commerce in Nigeria', 3 PER 1–24 at 13–15.

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, Jakarta, 13-14 December. https://doi.org/10.1109/ict4m.2010.5971884

Berman F. and Cerf V.G. (2017), Social and Ethical Behavior in the Internet of Things, Communications of the ACM, 60 (2), 6-7, Doi: 10.1145/3036698.

Campbell, M. and Stylianou, A. (2009), "Personal Internet Usage at Work: The Dark Side of Technology Adoption" (2009). DIGIT Proceedings. 8. http://aisel.aisnet.org/digit2009/8

Cassim F. (2011), Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players, A paper presented at the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011.

Center for Internet Security (2018), Know the Rules of Cyber Ethics, https://www.cisecurity.org/daily-tip/know-the-rules-of-cyber-ethics/

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication (AJIC), 20, 133-155. https://doi.org/10.23962/10539/23572

Cohen R. J. and Swerdlik M. E. (2007), Psychological Testing and assessment: An Introduction to tests and Measurement, seventh edition, McGraw-Hill Higher education.

Ifijeh G., Michael-Onuoha H., Ilogho J. and Osinulu I., (2015), Emergence of hi-techexamination malpractices in Nigeria: issues and implications, International Journal of Educationand Research, 3(3), pp 113-122, retrieved from http://www.ijern.com/journal/2015/March-2015/10.pdf

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computer & Security, 31(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Internet Crime Complaint Center (2012), "Internet Crime Report", available at: www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Kaplan, R.M. and Saccuzzo, D.P., (2001). Psychological Testing: Principle, Applications and Issues (5th Edition), Belmont, CA: Wadsworth, http://changingminds.org/disciplines/hr/selection/validity.htm#typ

Karim, N.S., Zamzuri, N.H.A., Nor, Y.M.: (2009), Exploring the relationship between internet ethics in university students and the big five model of personality. Comput. Educ. 53(1), 86–93

Lee, Y., &Kozar, K. (2005). Investigating factors affecting the anti-spyware system adoption. Communications of the ACM, 48(8), 72-77. https://doi.org/10.1145/1076211.1076243

Leonard, L. N. K., Cronan, T. P., &Kreie, J. (2004). What are influences of ethical behavior intentions – planned behaviour, reasoned action, perceived importance, or individual characteristics? Information & Management, 42(1), 143-58. https://doi.org/10.1016/j.im.2003.12.008

Lysonski, S., Durvasula, S.: (2008), Digital piracy of MP3: consumer and ethical predispositions. J. Consumer Mark. 25(3), 167–178

Olivier B. (2013), Is there a need for cyber-ethics? Mail & Guardian, https://thoughtleader.co.za/bertolivier/2013/07/28/is-there-a-need-for-cyber-ethics/

Olson J., Codde J., deMaagd K., Tarkleson E., Sinclair J., Yook S. and Egidio R., (2011), AnAnalysis of e-Learning Impacts & Best Practices in Developing Countries, With Reference toSecondary School Education in Tanzania, Michigan State University, USA, Information &Communication Technology for Development , http://tism.msu.edu/ict4d

Omiunu O.G. (2017), Paradoxical Modeling of the Negative Uses of ICT and their Implications among Secondary School Students in Oyo State, Nigeria, Library Philosophy and Practice, University of Nebraska – Lincoln, https://digitalcommons.unl.edu/libphilprac/1485

Onyancha O. B. (2015) "An informetrics view of the relationship between internetethics, computer ethics and cyberethics", Library Hi Tech, Vol. 33 Issue: 3, pp.387-408, https://doi.org/10.1108/LHT-04-2015-0033

Peits,M.,andWaelbroeck, P. (2006), Why the music industrymay gain from free downloading—the role of sampling. Intl. J. Ind. Organ. 24, 907–913

Siponen, M., and Vartianen, T. (2004), Unauthorized copying of software and levels of moral development: a literature analysis and its implication for research and practice. Inform. Syst. J. 14, 387–407

Spinello, R.A. and Tavani, H. (Eds) (2004), Readings in Cyberethics, Jones and Bartlett Publishers, Sudbury, MA.

Symantec. (2013). 2013 Norton report: Cost per cybercrime victim up 50 percent. Retrieved fromhttp://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029_01

Wong, E.Y.W. (1995), "How should we teach computer ethics? A short study done in Hong Kong",Computer Education, Vol. 25 No. 4, pp. 179-191.

Wu W. and Yang H., (2011), A comparative study of college students' ethicalperception concerning internet piracy, Qual Quant (2013) 47:111–120, DOI 10.1007/s11135-011-9506-1

Wurst, C., Smarkola C., & Gaffney, M. A. (2008). Ubiquitous laptop usage in higher education:Effects on student achievement, student satisfaction, and constructivist measures in honors andtraditional classrooms. Computers & Education, 51, 1766–1783.