

Insight into ethical cyber behaviour of undergraduate students at selected African universities



Authors:

Nurudeen A. Aderibigbe¹ 
Dennis N. Ocholla¹ 

Affiliation:

¹Department of Library and Information Science, Faculty of Arts, University of Zululand, KwaDlangezwa, Empangeni, South Africa

Corresponding author:

Nurudeen Aderibigbe,
rabshittu@yahoo.com

Dates:

Received: 20 July 2019
Accepted: 16 July 2020
Published: 08 Oct. 2020

How to cite this article:

Aderibigbe, N.A. & Ocholla, D.N., 2020, 'Insight into ethical cyber behaviour of undergraduate students at selected African universities', *South African Journal of Information Management* 22(1), a1131. <https://doi.org/10.4102/sajim.v22i1.1131>

Copyright:

© 2020. The Authors.
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Background: Worldwide, immoral cyberspace users have continued to use the Internet to commit crimes; this has caused unease and has called for quick response to the problem especially within the educational sector. The practical value of this study is in its benefit to other researchers who may be attempting to understand South African or Nigerian cyber technology user's behaviour; it may also help relevant educational authorities to get relevant understanding of behaviour in the realm of cyberspace.

Objectives: This study examined undergraduate students in relation to cyber technology at the University of Zululand (UNIZULU), South Africa, and the Federal University of Agriculture in Abeokuta (FUNAAB), Nigeria.

Method: A survey design, questionnaire as the tool for data collection was adapted and samples for the study were drawn from undergraduate students in two conveniently selected universities in South Africa and Nigeria. Overall, 450 undergraduate students were invited to participate in the survey; 380 respondents completed and returned the questionnaire, resulting in a response rate of 84.4%.

Results: Most of the respondents from the sampled universities reported that they were aware of what constitutes unethical cyber behaviour. Furthermore, the participants revealed that they hardly received orientation at the universities on cyber behaviour. The challenges that the students faces were reported.

Conclusion: This study recommends that universities should sustain orientation and/or training programmes on cyber-ethics and cyber security awareness at the start of each academic year. The results of this study may spark further discussions and research on cyber technology access and use in contemporary society.

Keywords: cyber-ethics; ethical behaviour; South Africa; Nigeria; undergraduate students; 4th industrial revolution; Internet of things.

Introduction

Increasingly, universities strive to provide an enabling academic environment in which students can use cyber technology for educational purposes. Students in Nigeria and South Africa use information and cyber technologies on a daily basis to perform a broad range of academic tasks. There are ethical guidelines that govern the use of such technologies, and these, to some extent, guard against ethical violations. However, research indicates that students, generally, lack the understanding and awareness of the ethical use of cyber technology, leading to decisions taken without foreknowledge about ethical responsibilities and consequences (Aderibigbe 2020). Some of these unwholesome behaviours include intellectual property violations, copyright infringement, digital piracy and plagiarism. This new breed of intellectual property issues that are provoked by the steady commercialisation of the Internet and the proliferation of websites and information reflects unfair dealing and trespass on the ownership rights of intellectual property in the information utilisation chain. The levels of software piracy and counterfeiting in films, music, videos, books and images, amongst many other vices, have become increasingly troubling in recent years (Cummings 2017; Liu 2018; Okojie & Umoru 2017). These unethical cyber practices have become a common feature amongst students in the university environment and may have implications on their professional status in the larger corporate society.

There are relatively few research publications on cyber-ethics in an African context, and the current interest in unethical behaviour in research is relatively new in developing countries. Although there is a strong development of information ethics in Africa¹ through African Network

1.The first African Information Ethics Conference were held in Tshwane, South Africa, 05-07 February 2007.

Read online:



Scan this QR code with your smart phone or mobile device to read online.

on Information Ethics (ANIE) and African Centre of Excellence for Information Ethics (ACEIE) based at the University of Pretoria in South Africa, not much has been published on the impact of information communication and technology (ICT) on African societies and the ethical use of these technologies (Ponelis & Holmner 2015). Furthermore, most studies on cyber-ethics as a concept in the literature and ICT, from an ethical point of view, draw their perspectives from the western philosophical tradition. A decade long (2006–2016) search on the open access database, Scopus, on cyber-ethics and related terms 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 revealed that none of these research works emanated from Africa, particularly South Africa and Nigeria.

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. This applies to academic staff as well. In one incident, highly placed academic staff members were relieved of their jobs over plagiarism and falsification of data (Omotayo 2013). 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 light of this that we felt the need to investigate unethical cyber behaviour in a bid to contribute to the existing body of knowledge in the field of cyber-ethics. Our study is informed by knowledge, experience and personal observations during the interaction with other academic staff on the issue of ethical violations. The study was motivated by the desire to contribute to solving the problem of unethical cyber behaviour by finding ways to motivate students towards strict adherence to ethical guidelines.

In view of the limited research output in this research area within Nigeria and South Africa, this study was designed to determine the cyber behaviour of students in the two countries, to further support the ongoing efforts to curb the unethical use of cyber technologies in academia. The primary aim of this study was to determine the awareness and challenges of cyber-ethics behaviour among students from two selected universities in Nigeria and South Africa.

Purpose of the study

The objectives of this study were to:

- determine undergraduate students' awareness of cyber-ethics requirements at the University of Zululand, South Africa, and at the Federal University of Agriculture in Abeokuta, Nigeria
- identify the types of unethical cyber behaviour that are prevalent in the studied universities
- verify the influence of the Theory of Planned Behaviour (TPB) on ethical cyber behaviour

- identify the challenges faced by undergraduate students in their efforts to act ethically in cyberspace at the two universities.

Literature review

The phrase cyber technology ethics was chosen because it reflects the current trend in research attention to ICT. The review of cyber technology ethics or cyber-ethics was based on the more established fields of computer and information ethics. Computer and information ethics, which 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, cyber-ethics, is a dynamic field of study that identifies:

Ethical issues in the use of cyber technology, 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 cyber-ethics, 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 amongst communities of Information Science (IS) scholars (Onyancha 2015). Cyber-ethics, 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).

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

It has been found that the property of cyber technology 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 (Mason 1986; Moor 1985). In this consideration, unethical cyber behaviours, such as computer hacking and digital or Internet piracy, are the concerns of this study. Recent studies conducted in multiple countries revealed that computer hacking and digital piracy have become more prevalent amongst undergraduate students (Burruss, Holt & Bossler 2019; Udris 2017).

Various studies conducted in the university context have examined factors influencing cyber-ethical behaviour

(Alleyne, Soleyn & Harris 2015; Marcum, Higgins & Nicholson 2017; Martin & Woodward 2011; Thomas & Ahyick 2010). Generally, the results from these studies revealed that students did not regard unethical use of cyber technology as any form of violation. Lau, Yuen and Park (2013) pointed out that unethical behaviours are typical and prevalent, yet understudied and/or underexplored among IS researchers in developing countries. As such, further attention is needed to address the literature gap.

Theoretical approaches to cyber-ethical studies have relied on social psychology models of behaviour change that seek to identify determinants and pathways of the influence of cyber-ethics behaviour, such as ethical and unethical use of cyber technology (Aderibigbe & Ocholla 2018). To extend the frontier of knowledge in the study of cyber-ethical behaviour, this study adapted the TPB of Ajzen (1991, 2011) to provide a more elaborate and practical factors that could contribute to cyber-ethical issues in Africa. We have discussed TPB in detail in a recent publication (Aderibigbe, Ocholla & Britz in press).

The TPB (Ajzen 1985, 1991) is an extension of the Theory of Reasoned Action (TRA) (Ajzen & Fishbein 1980). The TRA assumes that attitude and subjective norms are the determinants of the individual intentions to carry out a given behaviour. In other words, the intentions to perform behaviour correlate 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 TRA brought about the TPB (Ajzen 1991). The TPB assumes that behavioural intention is the strongest determinant of actual behaviour, whilst the direct determinants of individual behavioural intentions are their attitudes, subjective norms and PBC (Ajzen 1991). The TPB (Ajzen 1991) and its predecessor the TRA (Ajzen & 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 cyber technology (Attuquayefio & Addo 2014; Goles et al. 2008; Taylor & Todd 1995); digital piracy (Liao, Lin & Lin 2010; Yoon 2010); unethical behaviour (Chatterjee, Suprateek & Joseph 2015); perception of cyber technology ethics (Chiang & Lee 2011); academic dishonesty (Harding et al. 2007) and cyber data privacy (Morgan 2015).

In practice, researchers have generally considered the TPB as a choice for explaining behaviours where ethical considerations are an issue (Aderibigbe & Ocholla 2018). In addition, the theory is widely applied to multitude of fields such as medicine, geography and public relations. In conclusion, the TPB leans to diversify and theory application, because it has been widely applied to cyber-ethical research and shows a strong predictor for behavioural intention and behaviour (Aderibigbe 2020; Aderibigbe et al. in press).

Methodology

The study adopted the pragmatic – both quantitative and qualitative – research methods, particularly survey research. Using cluster sampling, sample for the study was drawn from undergraduate students in two selected universities in South Africa and Nigeria, where each of the selected institution was a cluster, that is, University of Zululand (UNIZULU) and Federal University of Agriculture in Abeokuta (FUNAAB). The respondents were drawn from all the faculties in UNIZULU and all the colleges in FUNAAB. Data collected using the quantitative instrument were coded, and the analyses were carried out using the statistical packages for social sciences (SPSS), version 25.0. Overall, 450 undergraduate students were invited to participate in the survey; 380 respondents completed and returned the questionnaire, resulting in a response rate of 84.4%.

Given that the total number of undergraduate students at the UNIZULU 2016/2017 (UNIZULU Fact & Figure 2017) was 15 542, and the total number of undergraduate students at the Federal University of Agriculture, Abeokuta, 2017, was 15 847, the total population of the two universities was calculated as $15\ 542 + 15\ 847 = 31\ 389$. Furthermore, to ensure that each respondent had an equal chance of being surveyed (Neuman 2011), the study adopted probability proportionate to size (PPS) in the selection of sample from each cluster (Nueman 2011) (see Table 1).

The overall total numbers of the study population at both universities were 31 389. The study aimed at a minimum sample size of 380, at a confidence level of 95% and a confidence interval of 5% based on the sample size calculation. However, we invited up to 450 to make provisions for setting aside incomplete and unreliable responses.

TABLE 1: Sampling frame for selection of respondents.

Faculties/universities	Student population	Sample size	%
Faculty of Arts	3666	45	-
Faculty of Commerce, Administration and Law	3904	47	-
Faculty of Education	4718	57	-
Faculty of Science and Agriculture	3199	39	-
Total in UniZulu	15 542	188	49
College of Management Sciences	2512	30	-
College of Environmental Resources Management	1157	18	-
College of Animal Science and Livestock Production	1210	14	-
College of Agricultural Management and Rural Development	2423	29	-
College of Plant Science and Crop Production	1643	20	-
College of Biological Sciences	1525	18	-
College of Food Science and Human Ecology	1625	19	-
College of Veterinary Medicine	552	6	-
College of Engineering	900	11	-
College of Physical Science	2300	27	-
Total in Funaab	15 847	192	51
Overall population	31 389	380	100

Ethical consideration

The study received ethical clearance from the University of Zululand's Research Ethics Committee: UZREC 17110-030 PGD 2016/116

Findings

This section focuses on the four research questions as follows.

What is the level of awareness of unethical cyber behaviour amongst students at the University of Zululand, South Africa and at the Federal University of Agriculture in Abeokuta, Nigeria?

The questionnaire responses revealed that the undergraduate students were mostly aware of unethical behaviour with regard to cyber technology at the selected universities in South Africa and Nigeria. This was corroborated by the interview results, which established that students from both universities under investigation were mostly aware of unethical cyber behaviour. With respect to orientation and training, it was revealed that most students had received training in their first year at both universities on the use of cyber technology for educational purposes only and not on ethical use of cyber technology. It is noteworthy that the respondents only received training on the application of computers, laptops and other hand-held devices for learning purposes. Whilst this helps students to understand the benefits of the devices, the implication is that the negative applications of those

devices to the network, which could address issues of cyber-ethics, were not included in the orientation programmes. The institutions' orientation programmes were observed to be too focused on technological skills and the educational applications of those skills, rather than the consideration of the implications of the risks that could arise from unethical cyber behaviour. In other words, the programmes do not address the risk to the integrity of the cyber infrastructure and the image of the universities.

What are the types of unethical cyber behaviour exhibited by undergraduate students in the two universities?

The impressive and remarkable nature of cyber technology, which serves students as a revolutionary medium of expression and provides access to globalised information, comes with new challenges. The increasingly limitless access to the Internet on university campuses has made cyber piracy and other forms of unethical cyber behaviour amongst students prevalent. Multinational studies have underscored the difficulties in identifying and policing cyber infringements, especially where the policies and laws are flexible (International Centre for the Prevention of Crime ICPC 2018:121; International Telecommunication Union ITU 2012:75).

Table 2 reveals the most prevalent form of unethical cyber behaviour amongst undergraduate students at the two

TABLE 2: Types of cyber-ethics behaviour amongst students in the two universities.

S/N	Cyber-ethical behaviour – Average mean = 2.7	Nigeria			South Africa		
		Freq.	Mean (\bar{x})	SD	Freq.	Mean (\bar{x})	SD
1	Cyber-piracy (software piracy: music and film downloading)	192	3.66	1.468	188	3.69	1.329
2	Cybersex and pornography	192	3.53	1.438	188	3.28	1.562
3	Privacy violation	192	3.22	1.477	188	3.09	1.519
4	Blackmailing and disseminating junk mail	192	3.31	1.588	188	3.07	1.565
5	Disseminating fake news	192	3.39	1.560	188	3.35	1.590
6	Cybercrime	192	3.33	1.525	188	3.16	1.647
7	Cyber stalking	192	3.14	1.501	188	3.18	1.541
8	Cyber fraud, i.e., fraudulent online banking	192	3.41	1.493	188	3.06	1.506
9	Cyberbully	192	3.13	1.355	188	3.15	1.537
10	Hacking/carding/phreaking/cracking	192	3.41	1.348	188	3.12	1.481
11	Cyber vandalism	192	3.10	1.372	188	3.02	1.477
12	Accessing inappropriate or illegal online material	192	3.35	1.333	188	3.07	1.479
13	Denial of service attack	192	3.33	1.267	188	2.76	1.503
14	Data mining (indirect gathering of personal information)	192	3.14	1.342	188	2.84	1.439
15	Cybersquatting	192	2.99	1.328	188	2.80	1.437
16	Spoofing and phishing	192	3.23	1.375	188	2.84	1.500
17	Violating intellectual property	192	3.20	1.379	188	2.94	1.507
18	Violating software license agreement	192	3.39	1.417	188	2.95	1.500
19	Using another users' password	192	3.39	1.394	188	3.35	1.446
20	Cyber libel (false statements that harm another reputation)	192	3.21	1.370	188	2.89	1.493
21	Cyber terrorism	192	3.31	1.387	188	2.95	1.523
22	Social media profile cloning	192	3.47	1.421	188	3.24	1.491
23	Cyber espionage	192	3.39	1.415	188	3.49	1.442
24	Copyright violation	192	3.42	1.371	188	3.37	1.466
25	Plagiarism	192	3.38	1.478	188	3.17	1.524
26	Cybersmearing (embarrassment or humiliation in social network)	192	3.66	1.468	188	3.69	1.329
27	Worm and viruses (malicious programs shared with the intent of shutting down the network)	192	3.53	1.438	188	3.28	1.562

Freq., frequency; SD, standard deviation.

universities to be cyber piracy, which produced the highest mean score of $m = 3.6$, $SD = 1.5$ and $m = 3.6$, $SD = 1.3$ amongst students in Nigeria and South Africa, respectively. This indicates that cyber piracy is the common practice at the two universities. Following this is cyber smearing with $m = 3.6$, $SD = 1.4$ for Nigeria and $m = 3.7$, $SD = 1.3$ for South Africa and cybersex behaviour, with $m = 3.5$, $SD = 1.4$ for Nigeria, and $m = 3.2$, $SD = 1.5$ for South Africa. These findings are corroborated in several studies that have underscored the prevalence of cyber piracy and other forms of cyber violations amongst undergraduate students (Chavarria et al. 2016; Cilliers 2017). The use of cyber technology, especially computers, smart devices and the Internet, has become part of the daily routine at most university campuses. The frequency of this usage has led to the escalating nature of ethical issues among students.

What is the impact of the theory of planned behaviour on the ethical cyber intention of undergraduate students in the two universities?

As also discussed elsewhere (Aderibigbe et al. in press), overall, the significant levels of the results established that the three variables (attitude, subjective norms and PBC) were individually statistically significant in influencing students' ethical cyber behaviour. The regression results established an adjusted R^2 value of 0.517 for Nigeria and 0.543 for South Africa. Both were significant at the 0.05 level ($0.000 < 0.05$). These results indicate that the three independent variables (attitude, subjective norms and PBC of ethical cyber behaviour) jointly (as indicated by the R^2) explained or predicted 51.7% of the variations in the influence of the TPB on undergraduate ethical cyber behaviour in Nigeria, and 54.3% of the variations in the influence of the TPB on undergraduate ethical cyber 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 ethical intention, showed that PBC contributed the most to the prediction of ethical cyber intention and eventual behaviour of undergraduate students in Nigeria (beta value = 0.747) and in South Africa (beta value = 0.601). These results imply that all three constructs of the TPB exert significant influence on predicting ethical cyber intention and behaviour.

Subjective norms are an important attribute when determining ethical intention with respect to cyber technology. Hence, it is logical to assume that reference groups, such as parents, friends or faculty members, who students perceive to be important in their daily routines, have influential roles to play in their formation of ethical and unethical cyber behaviour. In other words, subjective norms may represent the 'social pressure' necessary to encourage either positive or negative intention in the cyber behaviour of students. Accordingly, this research suggests targeting these important reference groups when planning a campaign strategy or creating a persuasive message against unethical cyber behaviour. Role models, such as parents in

the home and staff members in the ICT sector or university faculties, could act as a good starting point for effectively instilling negative attitudes towards the misuse of cyber technology by students.

What are the challenges faced by undergraduate students in their efforts to act ethically in cyberspace at the two universities?

Many challenges were identified as represented on Table 3.

The findings in Table 3 revealed that undergraduate students in Nigeria face more challenges in their efforts to act ethically correct in cyberspace than those in South Africa. The challenges include:

- social negative influence
- ease of performing illegal activities
- lack of adequate security measure to ensure compliance with cyber-ethics policy
- lack of enough orientation and education on implications of ethical violations
- over-packed teaching and learning curriculum
- contradiction between copyright and freedom of information
- lack of cyber morality and ethical conduct in the use of cyber technology
- management bureaucratic processes
- breaches in confidentiality and network security
- lack of time and commitments
- lack of publicised policies about misuse of cyber technology
- lack of ethical consideration and consequence of violations
- lack adequate training for teaching cyber-ethics
- institutional growth is taxing existing cyber infrastructure
- financial constraints
- risk of anonymity of users.

Only in the lack of policy guidance on appropriate cyber behaviour do students in South Africa have higher level of prevalence. This implies that Nigerian undergraduate students are more prone to various cyber-ethical challenges that affect their behaviour. A 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, and lack of space in the curriculum, among others.

The findings of this study also cast a new light on the previous findings by National Cyber-ethics, Cybersafety, Cybersecurity Baseline (2009), in which it was also revealed that financial constraints, time commitments, bureaucratic processes and over-packed curriculum were the challenges frustrating ethically correct behaviour of university students. Similarly, Walczak et al. (2010) in their study showed that the faculty lack adequate training and understanding to teach cyber-ethics. They equally noted

TABLE 3: Challenges to students' ethical cyber behaviour in Nigeria and South Africa.

Challenges	Country	Strongly disagree		Disagree		Neutral		Agree		Strongly agree	
		<i>n</i>	%	<i>n</i>	%	<i>n</i>	%	<i>n</i>	%	<i>n</i>	%
Social negative influence	Nigeria	5	2.60	9	4.70	24	12.50	68	35.40	86	44.80
	South Africa	7	7.37	14	7.40	44	23.40	70	37.20	53	28.40
Ease of performing illegal activities	Nigeria	4	2.10	25	13.00	35	18.30	62	33.30	66	34.40
	South Africa	6	3.20	36	19.10	52	27.70	54	28.70	40	21.30
Lack of adequate security measures to ensure compliance to cyber-ethics policy	Nigeria	6	3.10	18	9.40	34	17.70	68	35.40	66	34.40
	South Africa	9	4.80	30	16.00	25	23.90	63	33.50	41	21.80
Lack of enough training and education on implications of ethical violations	Nigeria	4	2.10	17	8.90	32	16.70	77	40.10	62	32.30
	South Africa	9	4.80	19	10.10	32	17.00	78	41.50	40	46.60
Lack of policy guidance of the use and appropriate cyber behaviour	Nigeria	6	3.10	18	9.10	38	19.80	70	36.50	60	31.30
	South Africa	10	5.30	20	10.60	40	21.30	69	36.70	49	26.10
Over packed teaching and learning curriculum	Nigeria	10	5.20	17	8.90	33	17.20	71	37.00	61	31.80
	South Africa	10	5.30	22	11.70	41	21.80	64	34.00	51	27.10
Contradiction between copyright and freedom of information	Nigeria	7	3.60	18	9.40	37	19.30	68	35.40	62	32.30
	South Africa	15	8.00	19	10.10	56	29.80	61	32.40	37	19.70
Lack of cyber values and ethical conduct in the use of cyber technology	Nigeria	9	4.70	17	8.90	37	19.30	73	38.00	56	29.20
	South Africa	9	4.80	21	11.20	44	23.40	70	37.20	42	23.40
Negative violations of the integrity of the institution's cyber infrastructure	Nigeria	7	3.60	23	12.00	27	19.30	67	34.90	58	30.20
	South Africa	10	5.30	21	11.20	61	32.40	59	31.40	37	19.70
Exposure of the institution network to virus and malware	Nigeria	7	3.60	30	15.60	49	25.50	55	28.60	51	26.60
	South Africa	9	4.80	25	13.30	62	33.00	58	30.90	34	18.10
Misuse of institution license software and hardware	Nigeria	7	3.60	24	12.50	51	26.60	59	30.70	51	26.60
	South Africa	14	7.40	33	17.60	49	26.10	53	28.20	39	20.80
Management bureaucratic processes	Nigeria	11	5.70	18	9.40	35	18.20	72	37.50	56	29.20
	South Africa	17	9.00	25	13.30	44	23.40	63	33.50	39	20.80
Breaches in confidentiality and network security	Nigeria	6	3.10	26	13.50	31	16.10	73	38.00	56	29.20
	South Africa	11	5.90	28	14.90	52	27.70	60	31.90	37	19.70
Lack of time and commitments	Nigeria	9	4.70	20	10.40	39	20.30	67	34.90	57	29.70
	South Africa	18	9.60	29	15.40	47	25.00	60	31.90	34	18.10
Lack of publicised policies about the unethical use of cyber technology	Nigeria	7	3.60	19	9.90	41	21.40	62	32.30	63	32.80
	South Africa	14	7.45	23	12.20	46	24.50	67	35.60	38	20.20
Lack of ethical consideration and consequence of violations	Nigeria	9	4.70	22	11.50	33	17.20	64	33.30	64	33.30
	South Africa	18	9.60	18	9.60	50	26.60	59	31.40	43	22.90
Data theft and loss of sensitive institution's information	Nigeria	10	5.20	20	10.40	37	19.30	67	34.90	58	30.20
	South Africa	19	10.10	16	8.50	48	25.50	65	34.60	40	21.30
Compromised account or passwords	Nigeria	13	6.80	14	7.30	33	17.20	67	34.90	65	33.90
	South Africa	20	10.60	19	10.10	38	20.20	57	30.30	54	28.70
Financial constraints	Nigeria	14	7.30	12	6.20	41	21.40	68	35.40	57	29.70
	South Africa	18	9.60	22	11.70	42	22.30	55	29.30	51	27.10
Risk to anonymity of users	Nigeria	14	7.30	16	8.30	35	18.20	68	35.40	59	30.70
	South Africa	19	10.10	22	11.70	49	26.10	57	30.30	41	21.80
Theft of copyrighted materials	Nigeria	15	7.80	13	6.80	38	19.80	62	32.30	64	33.30
	South Africa	21	11.20	21	11.20	48	25.50	56	29.80	42	22.40

the inconsistency in policy instruments, within the academic, that could deal with cyber-ethical misbehaviour.

This bolsters the works of Monahan (2012) 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, Lesley and Geoffrey (2010); Calvani et al. (2012); Baykara, Demir and Yaman (2015) and Plaisance (2013) noted the need for the consideration of moral dimensions in cyber technology usage, especially among students. This supports the work by the University of North Carolina (2014) that students are faced with various cyber-ethical problems occasioned by personal and situational factors that influence against acting ethically correct in the cyberspace of universities.

Conclusion

Based on the results, the most relevant conclusions are the following: students appeared to be unaware of ethical cyber-ethics requirements and training at the selected universities. Amongst the several types of unethical cyber behaviour, cyber piracy, cybersex/pornography and privacy violation 'lead the pack'. The constructs of the TPB were found to have a significant influence on the ethical cyber behaviour of undergraduate students in this study, as the three variables (attitude, subjective norms, and PBC and intention) were individually statistically significant in influencing students' cyber behaviour. The study has highlighted many challenges (Table 2) that require attention. The findings in this report are subject to at least two limitations. Firstly, there was insufficient explanation as to why some moral philosophies did not impact the ethical judgement and behavioural intention of the students in

cyber technology use and behaviour. The use of English, as a second or third language of all the respondents in this study, could also have led to the misinterpretation of some parts of the questionnaire.

The study recommends the following: extensive and regular awareness education; the development of policies dealing specifically with cyber-ethics and the responsible use of cyber technology; devising appropriate methodology to educate the students; the use of education rather than punishment; and other strategies that can be used to train users on how to behave ethically in cyberspace. Cyber-ethics awareness would be more effective if it could account for the factor of self-efficacy of the students as cyber technology users and provide some reward to those who adhere to ethical conduct on the university network. This study should inform cyber-ethics research, policy, teaching and learning, largely within the academic environments.

Acknowledgements

A shorter version of this article was presented at the Fifth International Professional Forum 'Book, Culture, Education, Innovation', Crimea 2019, Russia. The authors wish to acknowledge the University of Zululand (UNIZULU) in South Africa, and Federal University of Agriculture in Abeokuta, Nigeria, for supporting the PhD study in different ways, particularly the UNIZULU for funding the research and travel for this conference presentation.

Competing interests

The authors have declared that no competing interests exist.

Authors' contributions

All authors contributed equally to this work.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Aderibigbe, N.A., 2020, 'Cyber ethical behaviour of university students: An overview of university of Zululand, South Africa and Federal university of agriculture, Abeokuta, Ogun state, Nigeria', *Journal of Applied Information Science and Technology* 13(1), 86–106.

- Aderibigbe, N.A. & Ocholla, D.N., 2018, 'Cyber-ethics and behavioural theories: A literature review', in *International Conference on Information and Knowledge Management 2nd: 2018*, The Technical University of Kenya, Nairobi, Kenya, August 21–24, 2018, pp. 268–277.
- Aderibigbe, N.A., Ocholla, D.N. & Britz, J., (in press), 'Differences in ethical cyber behavioural intention of Nigerian and South African students: A multi-group analysis based on the theory of planned behaviour', *Libri-International Journal of Libraries and Information Studies*.
- Ajzen, I., 1985, 'From intentions to actions: A theory of planned behaviour', in J. Kuhl, J. Beckmann (eds.), *Action control*, Springer, Berlin, pp. 11–39.
- Ajzen, I., 1991, 'The theory of planned behaviour', *Organizational Behaviour and Human Decision Processes* 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Ajzen, I., 2011, 'The theory of planned behaviour: Reactions and reflections', *Psychology and Health* 26(9), 1113–1127. <https://doi.org/10.1080/08870446.2011.613995>
- Ajzen, I. & Fishbein, M., 1980, *Understanding attitudes and predicting social behaviour* Prentice-Hall, Englewood Cliffs, N.J.
- Alleyne, P., Sherlexis, S. & Terry, H., 2015, 'Predicting accounting students' intentions to engage in software and music piracy', *Journal of Academic Ethics* 13(4), 291–309. <https://doi.org/10.1007/s10805-015-9241-7>
- Attuquayefio, S.N. & Addo, H., 2014, 'Using the UTAUT model to analyse students' ICT adoption', *International Journal of Education and Development using ICT* 10(3), 75–86.
- Baykara, Z.G., Demir, S.G. & Yaman, S., 2015, 'The effect of ethics training on students recognizing ethical violations and developing moral sensitivity', *Nursing Ethics* 22(6), 661–675. <https://doi.org/10.1177/0969733014542673>
- Brey, P.A.E., 2007, 'Computer ethics in (higher) education', in G. Dodig-Crnkovic, S. Stuart (eds.), *Computation, information cognition: The Nexus and the Liminal*, pp. 341–363, Cambridge Scholars Press, Cambridge.
- Burruss, G.W., Holt, T.J. & Bossler, A., 2019, 'Revisiting the suppression relationship between social learning and self-control on software piracy', *Social Science Computer Review* 37(2), 178–195. <https://doi.org/10.1177/0894439317753820>
- Bynum, T.W., 2008, 'Milestones in the history of information and computer ethics', in *The handbook of information and computer ethics*, vol. 25.
- Bynum, T.W., 2008, 'Milestones in the history of information and computer ethics', in K.E. Himma & H.T. Tavani (eds.), *The handbook of information and computer ethics*, pp. 25–48, John Wiley & Sons Inc, New Jersey, NY.
- 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. <https://doi.org/10.1016/j.compedu.2011.10.004>
- Chatterjee, S., Suprateek, S. & Joseph, S.V., 2015, 'The behavioural roots of information systems security: Exploring key factors related to unethical IT use', *Journal of Management Information Systems* 31(4), 49–87. <https://doi.org/10.1080/0742122.2014.1001257>
- Chavarría, J.A., Andoh-Baidoo, F.K., Midha, V. & Hughes, J., 2016, 'Software piracy research: A cross-disciplinary systematic review', *Communications of the Association for Information Systems* 38(1), 31. <https://doi.org/10.17705/1CAIS.03831>
- Chiang, L. & Lee, B., 2011, 'Ethical attitude and behaviours regarding computer use', *Ethics & Behaviour* 21(6), 481–497. <https://doi.org/10.1080/10508422.2011.622181>
- Cilliers, L., 2017, 'Evaluation of information ethical issues among undergraduate students: An exploratory study', *South African Journal of Information Management* 19(1), a767. <https://doi.org/10.4102/sajim.v19i1.767>
- Cummings, A.S., 2017, *Democracy of sound: Music piracy and the remaking of American copyright in the twentieth century*, Oxford University Press, New York, NY.
- 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. <https://doi.org/10.1007/s10551-007-9361-0>
- Harding, T.S., Matthew, J.M., Finelli, C.J. & Carpenter, D.D., 2007, 'The theory of planned behaviour as a model of academic dishonesty in engineering and humanities undergraduates', *Ethics & Behaviour* 17(3), 255–279. <https://doi.org/10.1080/10508420701519239>
- International Centre for the Prevention of Crime, 2018, *6th international report on crime prevention and community safety: Preventing Cybercrime 2018*, International Centre for the Prevention of Crime, Montreal, Canada, (ICPC), p. 1.
- International Telecommunication Union, 2012, *Understanding cybercrime: Phenomena, challenges and legal response September 2012*, International Telecommunication Union (ITU), Geneva, p. 1.
- Johnson, D.G., 1985, *Computer ethics*, Prentice Hall, Englewood Cliffs, NJ.
- Lau, G.K.K., Yuen, A.H.K. & Park, J., 2013, 'Toward an analytical model of ethical decision making in plagiarism', *Ethics & Behaviour* 23(5), 360–377. <https://doi.org/10.1080/10508422.2013.787360>
- Liao, C., Hong-Nan, L. & Yu-Ping, L., 2010, 'Predicting the use of pirated software: A contingency model integrating perceived risk with the theory of planned behaviour', *Journal of Business Ethics* 91(2), 237–252. <https://doi.org/10.1007/s10551-009-0081-5>
- Liu, H., 2018, 'In the shadow of criminalisation: Intellectual property criminal law, enforcement institutions and practices in China and the United States', *Information & Communications Technology Law* 27(2), 185–220. <https://doi.org/10.1080/13600834.2018.1458451>

- Marcum, C.D., Higgins, G.E. & Nicholson, J., 2017, 'I'm watching you: Cyber stalking behaviors of university students in romantic relationships', *American Journal of Criminal Justice* 42(2), 373–388. <https://doi.org/10.1007/s12103-016-9358-2>
- 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.
- Mason, R.O., 1986, 'Four ethical issues of the information age', *MIS Quarterly* 10(1), 5–12. <https://doi.org/10.2307/248873>
- 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. <https://doi.org/10.1111/j.1467-9973.1985.tb00173.x>
- Morgan, J.A., 2015, 'Exploring senior citizen perceptions of their cyber data privacy and security', in Doctoral dissertation, Capella University, viewed from <https://search.proquest.com/openview/63a8733c41122f856c1d20c5b1680c46/1?pq-origsite=gscholar&cbl=18750&diss=y>
- National Cyber Security Alliance, 2009, *National cyber-ethics, cybersafety, Cybersecurity Baseline Study*, viewed from <http://staysafeonline.mediaroom.com/index.php?s=67&item=44>.
- Neuman, W.L., 2011, 'Field research and focus group research', in *Social Research Methods: Qualitative and Quantitative Approaches*, pp. 420–463, Pearson, Boston, MA.
- Ocholla, D.N., 2009, 'Information ethics education in Africa. Where do we stand?', *The International Information & Library Review* 41(2), 79–88.
- Okojie, A.E. & Umoru, G.L., 2017, 'Counterfeiting and piracy: Challenges to effective protection of intellectual property rights in Nigeria', *South African Intellectual Property Law Journal* 5(1), 115–142.
- Omotayo, A., 2013, 'Intellectual property rights protection and how to avoid the trap of plagiarism', [Pamphlet], Federal University of Agriculture, Abeokuta.
- Onyancha, O., 2015, 'An informetrics view of the relationship between internet ethics, computer ethics and cyber-ethics', *Library Hi Tech* 33(3), 387–408. <https://doi.org/10.1108/LHT-04-2015-0033>
- Plaisance, P.L., 2013, *Media ethics: Key principles for responsible practice*, Sage, Thousand Oaks, CA.
- Ponelis, S.R. & Holmner, M.A., 2015, 'ICT in Africa: Building a better life for all', *Information Technology for Development* 21(2), 163–177. <https://doi.org/10.1080/02681102.2015.1010307>
- Quigley, M. (ed.), 2005, *Information security and ethics: Social and organizational issues*, Idea Group Inc (IGI), Hershey, PA.
- Tavani, H.T., 2013, 'Cyber-ethics', in A.L.C. Runehov & L. Oviedo (eds.), *Encyclopaedia of sciences and religions*, pp. 565–570, Springer, Dordrecht.
- Taylor, S. & Todd, P.A., 1995, 'Understanding information technology usage: A test of competing models', *Information Systems Research* 6(2), 144–176. <https://doi.org/10.1287/isre.6.2.144>
- Thomas, T. & Ahyick, M., 2010, 'Can we help information systems students improve their ethical decision making?', *Interdisciplinary Journal of Information, Knowledge & Management* 5, 209–224. <https://doi.org/10.28945/1160>
- Udris, R., 2017, 'Psychological and social factors as predictors of online and offline deviant behavior among Japanese adolescents', *Deviant behavior* 38(7), 792–809. <https://doi.org/10.1080/01639625.2016.1197689>
- University of North Carolina, 2014, *Student services: Responding to issues and challenges: The fifth compendium of papers*, University of North Carolina, General Administration, Chapel Hill, NC.
- Vallor, S., 2010, 'Social networking technology and the virtues', *Ethics and Information Technology* 12(2), 157–170. <https://doi.org/10.1007/s10676-009-9202-1>
- Walczak, K., Finelli, C., Holsapple, M., Harding, T., Carpenter, D., Errington, T.M. et al., 2010, 'Institutional obstacles to integrating ethics into the curriculum and strategies for overcoming them', in *ASEE Annual Conference and Exposition* 16(3), 15.749, 1–14.
- Yoon, C., 2010, 'Ethical decision-making in the Internet context: Development and test of an initial model based on moral philosophy', *Computers in Human Behaviour* 27(6), 2401–2409. <https://doi.org/10.1016/j.chb.2011.08.007>
- Zhang, A.T., Lesley, P.L. & Geoffrey, D., 2010, 'Key influences of cyberbullying for university students', viewed 22 September 2016, from <http://www.pacis-net.org/file/2010/S01-01.pdf>.