Assessment of Cyber Ethics Behaviour among Undergraduate Students at the Nigerian Federal University of Agriculture and the University of Zululand in South Africa

Nurudeen. A. Aderibigbe[1]
aderibigbena@funaab.edu.ng
https://orcid.org/0000-0002-7072-1773
Kehinde. A. Owolabi[1]
yomiowolabi2000@yahoo.com
Nancy. C. Okorie[1]
okorienc@funaab.edu.ng
Olawale, Gabriel Sola[2]
gabrielolawale@bowen.edu.ng

[1]Federal University of Agriculture, Abeokuta Ogun State; [2] Bowen University, Information Research and Instruction Services Unit, Iwo Nimbe Adedipe Library

ABSTRACT
There has been an alarming increase in cyber-technology misuse and abuse among young adults in recent years. This study examines types of cyberethics behaviours exhibited by undergraduate students Federal University of Agriculture (FUA), Nigeria, and the University of Zululand (UZ), South Africa. Both quantitative and qualitative design and a survey method were used. The sample for the study was purposively selected comprising 14 Information Technology (IT) professionals for the interview and 380 undergraduate students from the two universities. The findings of the study revealed that undergraduate students from the two universities exhibited a higher prevalence of cyberpiracy, cybersex, and cyber smearing. It has been established that these vices are more prevalent in undergraduate students from a Nigerian universities. Based on the findings of the study, the study recommended more awareness of the negative effect of cyberethics behaviours and the review of cyber ethics policies in both Nigeria and South Africa.

Keywords: Cyberethics behaviour, Cyberethics policy, Cyberspace, Undergraduate students

1. INTRODUCTION

The rapid advancement and extensive use of the Internet have made more social actors enter cyberspace, leading to cybercrime and other unethical behaviours. As a result, cyber ethics has become a topic of discussion in Information Science. Since the inception of the Internet, hackers have laboured to exploit it for selfish interests such as sophomoric mischief, theft, and espionage, among others (Olivier, 2013). Symantec (2013) noted that cyber-attacks are increasing and becoming more complex in existence. Nevertheless, various cybersecurity methods and solutions have been introduced with time, but these have shown no signs of stopping the nefarious activities of hackers on the Internet. To this end, social behaviour and appropriate use of the Internet have become more crucial with the increasingly interconnected cyber-physical-biological environment that links devices, systems, data, and people (Berman & Cerf, 2017).

A considerable volume of literature has been published in the field of cyber ethics on various unethical cyber-crime practices. For instance, (Peslak, 2008) revealed that pirated software and intellectual copyright violations are common phenomena in universities. Siponen and Varitianen (2007); Cilliers (2017) reported that young adults considered the production of copies of protected items on the Internet to be socially and morally acceptable. Similarly, in Abeokuta, Nigeria, Folorunso et al.

(2010) reported that university students attempted to use social networking sites before adopting their uses. Thus, the sites' users often examine them and probably know the gratifications they could derive from the media before accepting to use any of them.

Criminal activities in cyberspace are now on a global scale. Halder et al. (2011) described cybercrimes as offences that are committed against individuals or groups of individuals, with a motive to intentionally harm the victims, using modern telecommunication networks such as the Internet (chat rooms, emails, notice boards, and groups) and mobile phones. According to Pahuja (2011), cybercrimes could mean the vandalisation of a site by hackers, viewing confidential information, or stealing trade secrets or intellectual property using the Internet. It can also include the denial of services and virus attacks, preventing regular traffic from reaching a site.

1.1 Objectives of the Study

The main objective of the study was to assess the cyber ethics behaviour among undergraduate students at the Nigerian Federal University of Agriculture and the University of Zululand in South Africa. The study specifically sought to:

(i) identify the kinds of cyberethics misuse behaviours exhibited by undergraduate students in the two universities;
(ii) determine the usefulness of cyber ethics policy in promoting cyberethics behaviours in the two universities.

2. LITERATURE REVIEW

Many people have embraced cybercrime as a means of livelihood at the expense of physical and mental well-being. (Tade and Aliyu 2011) affirmed that many have become rich through cybercrimes while some have been apprehended. Still, cybercrimes are continually evolving beyond what is currently known in cyberspace, therefore making a crackdown seemingly herculean. Some common unethical practices in cyberspace by students include cyberpiracy (software piracy, music, and movie downloads), cybersex (online pornography, privacy violation, fake news dissemination, and cybercrime), amongst others (Aggarwal, 2015; Pahuja, 2011; Aderibigbe & Ocholla, 2020; Aderibigbe, Ocholla & Britz, 2021; Aderibigbe & Ocholla, 2018). These unethical cyber behaviours in the form of harassment via emails, cyber-stalking, cyberbullying, dissemination of obscene materials, defamation, hacking, cracking, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, forgery, and phishing, potentially cause harm to individuals. Likewise, there are cybercrimes and cyber misconducts that harm the property of an individual or organisation. These involve intellectual property crimes, cybersquatting, cyber vandalism, system hacking, transmitting viruses and malicious software to damage information, cyber trespass, Internet time theft, and fraud, amongst others.

Academic institutions recognise the importance of curtailing students' internal cyber technology misuse or unethical cyber behaviour, defined as students' unacceptable use of cyber technology in terms of application, organisation and ethical conduct in cyberspace (Phyo et al., 2007). Institutions use several strategies to reduce unethical cyber behaviour. They are also adopting surveillance systems and continuous monitoring around the globe to spy on their students and other users of their networks (Zetter, 2007). Adopting policies is another method used by institutions to deter misuse (Case & Young, 2002).

In recent times, many researchers have found out that students demonstrate misconceptions about internet policies within their institutions in several cases, which invariably result in inappropriate use (Lennie, 2013; Simonson et al., 2014). A recurring example of this misunderstanding is students' conflicting perceptions regarding violating intellectual property rights. Furthermore, Lewis et al. (2012) observed that despite policy guidelines regulating the copying and distribution of shared software programmes, students are still in a dilemma about what constitutes copyright infringement. In addition, the conflicting legal and ethical principles surrounding the broader issue of intellectual property rights create confusion about what a violation of copyright is.

What is apparent in these examples, as well as many others, is that "while trying to integrate cyber technology into teaching, learning and instruction processes, institutions' managements must deal with highly debated, continually changing, and often difficult-to-understand policies regulating students' cybertechnology behaviour and Internet use" (Davies, 2002).

3. METHODOLOGY

The study was both quantitative and qualitative in design and a survey method was employed. The sample population was drawn from undergraduate students and staff of the Information Technology Section/Information at the University of Zululand & Communication Technology Resource Centre at Federal University of Agriculture. The respondents were drawn from all faculties and colleges in the two universities. The sampling frame mirrored the target population's profile and was designed to enumerate the undergraduate students for the 2017 academic year.

Four hundred and fifty (450) undergraduate students participated in the survey. However, only three hundred and eighty (380) respondents completed and returned the questionnaire, giving a total response rate of 84.4%. To validate the information obtained from the undergraduate students on assessment of cyber ethical behaviour of undergraduates in the studied universities, the researcher got more information from members of staff of the Information Technology (IT) and Information and Communications Technology Resource Centre ICTREC sections. From the expected 16 members of staff of both ITS and ICTREC, 14 were interviewed, giving a response rate of 88%.

Data collected using questionnaires were coded, and the analyses were carried out using the Statistical Packages for Social Sciences (SPSS) (version 25.0). Data from the interview schedule were analysed using thematic analysis.

4. RESULTS AND DISCUSSION

To provide answers to the research question of the study, respondents were asked to indicate their level of agreement with a list of 30 cyber ethics behaviours. The result is presented in table 1.

Table1. Types of Cyberethics Behaviours among Students in the Two Universities

S/N	Cyberethics Behaviour – Average Mean = 2.5	Federal University Agriculture			University of Zululand		
		Freq.	*Mean ($\underline{x}$)*	*SD*	*Freq.*	*Mean($\underline{x}$)*	*SD*
1	Cyber-piracy: music and film downloading	192	3.66	1.47	182	3.69	1.33
2	Cybersex: online pornography	192	3.53	1.44	182	3.28	1.56
3	Privacy violation	192	3.22	1.48	182	3.09	1.52
4	Blackmailing and disseminating junk mail	192	3.31	1.59	182	3.07	1.57
5	Disseminating fake news	192	3.39	1.56	182	3.35	1.59
6	Cybercrime	192	3.33	1.53	182	3.16	1.65
7	Cyberstalking	192	3.14	1.50	182	3.18	1.54
8	Cyber fraud (e.g. fraudulent online banking)	192	3.41	1.49	182	3.06	1.51
9	Cyberbully	192	3.13	1.36	182	3.15	1.54
10	Hacking; carding; phreaking; cracking	192	3.41	1.35	182	3.12	1.48
11	Cyber vandalism	192	3.10	1.37	182	3.02	1.48
12	Accessing inappropriate; illegal online materials	192	3.35	1.33	182	3.07	1.48
13	Identity theft	192	3.32	3.94	182	3.09	1.50
14	Denial of service attack	192	3.33	1.27	182	2.76	1.50
15	Data mining (e.g. indirect gathering of personal information)	192	3.14	1.34	182	2.84	1.44
16	Cybersquatting	192	2.99	1.33	182	2.80	1.44
17	Spoofing and phishing	192	3.23	1.38	182	2.84	1.50
18	Violating intellectual property	192	3.20	1.38	182	2.94	1.51
19	Violating software license agreement	192	3.39	1.42	182	2.95	1.50
20	Using another user's password	192	3.39	1.40	182	3.35	1.45
21	Unleashing worms and viruses	192	3.29	1.39	182	3.16	1.46
22	Cybersquatting	192	3.21	1.32	182	2.99	1.51
23	Cyber libel (e.g. false statements that harm others' reputation)	192	3.21	1.37	182	2.89	1.49
24	Cyberterrorism	192	3.31	1.39	182	2.95	1.52
25	Social media profile cloning	192	3.47	1.42	182	3.24	1.49
26	Cyberespionage	192	3.39	1.42	182	3.49	1.44
27	Copyright violation	192	3.42	1.37	182	3.37	1.47
28	Plagiarism	192	3.38	1.48	182	3.17	1.52
29	Cyber smearing; humiliation in a social network	192	3.66	1.47	182	3.69	1.33
30	Sharing malicious programmes with the intent of shutting down the network	192	3.53	1.44	182	3.28	1.56

The results presented in table 1 reveal Cyber piracy has the highest mean score of $\underline{x}$= 3.66, SD = 1.47 and m = 3.6, SD = 1.3 among Nigerian and South African students. This indicates that cyberpiracy is at an alarming rate in the two universities. This is not surprising as several studies (Charlesworth & Sewry, 2008; Dinev et al., 2009) have shown that cyberpiracy tends to be higher in collectivist societies like Nigeria and South Africa. Following this, is cyber-sex behaviour ($\underline{x}$= 3.5, SD =1.4) for Federal University of Agriculture and ($\underline{x}$ = 3.2, SD = 1.5) for University of Zululand.

The third-ranked cyber behaviour is cyber-smearing. Federal University of Agriculture scored $\underline{x}$ = 3.6, SD = 1.4 while for University of Zululand obtained $\underline{x}$=

3.7, SD = 1.3. This result should be expected due to the anonymous nature of social media and the growing reliance on same for socio-political engagement by students.

Other cyber ethics behaviours which include spoofing and phishing obtained $\underline{x}$= 3.4, SD = 1.4 for FUA and $\underline{x}$= 3.2, SD = 1.4 for UZ. Another prominent behaviour is copyright violation ($\underline{x}$ = 3.4; SD = 1.3) for FUA and ($\underline{x}$ = 3.3; SD = 1.4) for UZ. Aside from the 30 cyber ethical behaviours, respondents were asked to identify other cyber ethical behaviours they are aware of. However, no other one was identified by respondents from either Nigeria or South Africa.

An interview was sought with ICT managers in the two selected universities in Nigeria and South Africa to establish whether or not policies regarding cyber technology use among students. From the responses in table 2, there is a policy guiding cyber technology use for the students at FUA while for UZ there is no such a policy.

Table 2: Availability of Policy Guiding Cyber Technology used by the Students

Participant	**Response**
UZ 1	*"Not that I know of. I think we are still trying to put that in place."*
UZ 2	"It *is on the university website. There is user access policy in terms of what is permitted or allowed on the university devices and what is not."*
UZ 3	*"I heard that health and safety do have a policy, and to send people for training, the staff will, in turn, educate others."*
UZ 4	"*We do have a policy, but my answer to that I won't say yes or no because we do not have a director, but we do have policies guiding the activities of the section."*
FUA1	*"Yes, I think the university has,*
FUA 2	*"Yes, we have ICT policy, where there in you have regulations on the ethical use of the devices that are connected to the university network the attitudes and behaviours that are allowed are also spelt out."*
FUA 3	*"I know the university at some time approved internet policy, but what I am not sure about is the clauses on the ethical use of cyber technology within the policy."*

The in-depth interviews revealed weaknesses in the current measures to check cyber ethics misuse behaviour and evidence of some cyber infractions from the students in both institutions. Student users tend to have a less favourable attitude towards cyberethics misuse behaviour. The findings of this study on the types of cybertechnology misuse behaviours exhibited by undergraduate students at the two universities corroborate with the works of (Karim, et al. 2009, Molluzzo & Lawler 2012; Martin & Woodward 2011; Tavani 2013, & Khalil & Seleim2012) that there have been wide ranges of cyberethics misuse behaviours associated with users in colleges and universities. Lau and Yuen 2014 argue that young adults, who are generally referred to as digital natives, have greater access to cyber technology and are more excellent consumers of information than the generations before them but that they are lacking in discerning and making the right decision when confronted with an ethical dilemma. There is a correlation between these views and other results obtained from developed economies (WeulenKranenbarg et al., 2017). The results obtained showed an extensive, non-educational utilisation of internet-derived information, a lack of knowledge or ignorance of ethical aspects, and a poor implication of their actions. Typically, the boundaries of acceptable and unacceptable cyber behaviour are defined by government authorities, who develop laws around specific illegal cyberspace behaviours, and businesses that represent inappropriate actions in their terms of service agreements. This may explain why

they carry on these vices without legal concern. On the other hand, the pervasiveness of cyberethics misuse behaviour among undergraduate students may imply that students and young adults, in general, are less grounded in ethical norms and are rarely controlled by rules and ideals (Wolfe et al., 2008). A study by (Iyadat et al. 2012) suggested that users avoid legal consequences of unethical cyber-related behaviours.

The researchers' interaction with staff members of the Federal University of Agriculture, Abeokuta, Nigeria, further revealed that the policy is available on the university's website, but copies are never made available to students during the university's orientation exercise. This lack of awareness and understanding of the existence of the policy on ethical use may indicate that the policy is ineffective or lacks implementation. This view is supported by the findings from the study of Olafsson, et al. (2013) who believed that a lack of awareness of guidelines in an institution's ethical policy might lead to students using personal judgments when deciding what constitutes appropriate behaviour in the cyberspace of their institutions. This finding negates those reported by (Grant and Grant 2016), where hard copies of clear policy guidelines and a well-designed applied cybertechnology ethics course have been seen to produce measurable positive changes in the ethical stances of students. Others have shown that the establishment and publicity of ICT ethics policy in the university is a way to improve the concepts of justice, fairness and moral rightness among cybertechnology users on the university's campus (Jung, 2009).

To counter misbehaviour, universities have resorted to limiting access to non-educational sites. This is done under the guise of virus control, spam control, users' safety, and the protection of university bandwidth. One South African university informant claimed that downloading music, software, or pictures eat up the connection's bandwidth, causing a severe downturn and network traffic. This is evidenced by the findings from the two universities. For instance, there is limited access to the Internet from 8 a.m. to 4 p.m. at the Federal University of Agriculture, Abeokuta, Nigeria. In contrast, at the University of Zululand, students have unlimited access to the network but with restrictions on educational sites. This regulation is due to specific guidelines given in the form of offences and fines regarding downloading of non-educational materials. For example, at the University of Zululand, YouTube videos that serve no academic purposes are prohibited. Other violations like viewing pornography, burning and downloading music, and playing games on a personal computer attract some stipulated fines and, on some occasions, the loss of access. Unfortunately, most students now access the university's network on their various hand-held devices, which give no visible conditions before they can gain access.

The situation is different at FUA, where a clear ICT policy draft (2016) stipulates conduct on the acceptable use of cybertechnology. Among others, the policy states that "Internet access through the university network is not a right but a privilege". The ICTREC section is responsible for the implementation of appropriate filtering facilities for web-based and non-web-based internet traffic that may not have direct educational value, such as pornography and gaming sites. Another policy states that "user's access on the university network is monitored and logged". However, these clear stipulations do not deter cyberethics misuse behaviour and violations by undergraduate students, as affirmed by the results from the interview with ICTREC respondents. Furthermore, downloading copyrighted items, pornography and the like can cause legal liabilities and risk other threats to the university's network. Therefore, it can be deduced that universities that have adopted

acceptable use policies may likely enjoy more productive educational usage than their counterparts that have not.

The results from the University of Zululand support the work of Cronan et al. (2006), who found in their study of five hundred and sixteen (516) students those undergraduates who have unrestricted access to computer technologies committed significantly more cybertechnology misuse behaviour. Thus, the assertion that consistent access to cybertechnology without stipulated prohibited conduct and practices in the university policy will influence students to misuse intention is supported by this study. In their research, a similar pattern of results was obtained by Foltz et al. (2005) who concluded that the mere presence of a computer usage policy does not make a difference in a university environment.

The findings of this study also call for institutions to review existing cyber ethics policies to reflect clauses in cybertechnology ethics and behaviour expected from users of their networks. This observation aligns with findings from staff members in the ICT sections in the two universities, who believe that the institutions' current policies are due for review. This finding concurs with the works of Yamano 2014, Laughton (2008); Chang and Lee (2011) that internet and ICT policy and code of ethics should be made very important in academic institutions to guide students in the utilisation of cyber technologies. This bolsters the work of Foltz et al. (2008) that many university students do not use cybertechnology policies, which are supposed to guide them from unethical cybertechnology usage. This also supports the work of Livingstone et al. (2011) and Sendag et al. (2012) who found in their studies that lack of institutional policies and awareness of institutional guidelines were direct reasons for the involvement of their respondents in e-dishonesty.

5. CONCLUSION AND RECOMENDATIONS

Cybertechnology's unique and remarkable nature, which has served students as a revolutionary medium of expression and access to globalised information, comes with new challenges. The increasingly unlimited access to the Internet on university campuses has made cyberpiracy and other forms of cyber behaviour among students prevalent. Studies have underscored the difficulty in identifying and policing cyberethics infringements, most especially where the policies and laws are flexible. Thus, the study established the most prevalent forms of cyberethics misuse behaviour among undergraduate students in the studied universities are cyber piracy software piracy (music and film downloading), cyberstalking, cyberbullying, cyberespionage, and cyber smearing. In addition, the study revealed that there is limited awareness of the publicity of cyber ethics policy in the two selected universities.

Given the above findings, the study recommends that the two universities:

(i) educate their users on the implication of cyberpiracy and other aberrant cyber behaviours;
(ii) adopt a more severe strategy against illegal and inappropriate digital content on their networks;
(iii) strengthen the publicity of their users' policy to increase the awareness of the existence of guidelines in the use of cyber technology in the two selected universities.

REFERENCES

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), 1-8.

Aderibigbe, N., Ocholla, D., &Britz, J. (2021). Differences in the ethical cyber behavioural intention of Nigerian and South African students: A multi-group analysis based on the theory of planned behaviour. *Libri*, *71*(4), 389-406.

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* (pp. 21-24).

Aggarwal, C. C. (2015). Outlier analysis. In Data mining, 237-263. Springer, Cham.

Case, C. J.,& Young, K. S. (2002). Employee internet management: Current business practices and outcomes. *CyberPsychology and Behaviour*, *5*(4), 355-361.

Cilliers, L. (2017). Evaluation of information ethical issues among undergraduate students: An exploratory study. *South African Journal of Information Management*, *19*(1), 1-6.

Cronan, T. P.,& Al-Rafee, S. (2008). Factors that influence the intention to pirate software and media. *Journal of Business Ethics*, *78*(4), 527-545.

Folorunso, O., Vincent, R. O., Adekoya, A. F.,&Ogunde, A. O. (2010). Diffusion of innovation in social networking sites among university students. *International journal of computer science and security*, *4*(3), 361-372.

Foltz, C., Schwager, P.,& Anderson, J. (2008). Porqué los usuarios (no) leenlasdirectivas de
uso del equipo. *Gestión industrial y sistemas de datos*, *108*(6), 701-712.

Halder, D., Jaishankar, K., Periyar, E.,&Sivakumar, R. (2011). Cyber victimisation in India: An empirical analysis. At *First International Conference of the South Asian Society of*
Criminology and Victimology (SASCV), 15-17 January 2011, Jaipur, Rajasthan, India: SASCV 2011 Conference Proceedings, 77.

Iyadat, W., Iyadat, Y., Ashour, R., &Khasawneh, S. (2012). University students and ethics of computer technology usage: Human resource development. *E-learning and Digital Media*, *9*(1), 43-49.

Khalil, O. E., &Seleim, A. A. (2012). Attitudes towards information ethics: a view from Egypt. *Journal of Information, Communication, and Ethics in Society*.

Karim, N. S. A., Zamzuri, N. H. A.,& Nor, Y. M. (2009). Exploring the relationship between Internet ethics in university students and the big five models of personality. *Computers and Education*, *53*(1), 86-93.

Kortjan, N. & von Solms, R. (2012). Cyber security education in developing countries: A South African perspective. In *International conference on e-infrastructure and e-services for developing countries*, 289-297. Springer, Berlin, Heidelberg.

Lau, W. W.,& Yuen, A. H. (2014). Internet ethics of adolescents: Understanding demographic differences. *Computers and Education*, *72*, 378-385.

Lennie, S. (2013). *Ethical complexities in the virtual world: Teacher perspectives of ICT-based issues and conflicts* [Doctoral dissertation]. https://tspace.library.utoronto.ca/bitstream/1807/35879/7/Lennie_Shawn_SD_201306_PhD_thesis.pdf

Livingstone, S., Haddon, L., Görzig, A.,&Ólafsson, K. (2011). Risks and safety on the Internet: The perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16-year-olds and their parents in 25 countries.

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.

Mishna, F., Cook, C., Gadalla, T., Daciuk, J., & Solomon, S. (2010). Cyberbullying behaviours among middle and high school students. *American Journal of Orthopsychiatry*, *80*(3), 362-374.

Molluzzo, J. C.,&Lawler, J. (2012). A study of the perceptions of college students on cyberbullying. *Information Systems Education Journal*, *10*(4), 84.

North, M. M., Richardson, R.,& North, S. M. (2017). Information security and ethics awareness: A concise comparative investigation. *Calitatea*, *18*(160), 141.

Pahuja, S. (2011). *Decolonising international law: Development, economic growth and the*
politics of universality. Vol. 86. Cambridge University Press.

Peslak, A. R. (2008). Current information technology issues and moral intensity influences. *Journal of Computer Information Systems*, *48*(4), 77-86.

Phyo, A.H., Furnell, S.M.,&Phippen, A.D. (2007). Pre-requisites for monitoring insider IT
misuse. In Bleimann, U.G., Dowland, P.S.,& Furnell, S. M. (Eds.), *Proceedings of the Third Collaborative Research Symposium Security, E-Learning, Internet and Networking, 41–52.*

Olafson, L., Schraw, G., Nadelson, L., Nadelson, S., & Kehrwald, N. (2013). Exploring the judgment–action gap: College students and academic dishonesty. *Ethics & Behavior*, 23(2), 148-162.

Sendag, S., Duran, M., & Fraser, M. R. (2012). Surveying the extent of involvement in online
academic dishonesty (e-dishonesty) related practices among university students and the
rationale students provide: One university's experience. *Computers in Human Behaviour*, 28(3), 849-860.

Simonson, M., Smaldino, S., &Zvacek, S. M. (Eds.). (2014). *Teaching and learning at a*
distance: Foundations of distance education. IAP.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee
information systems security policy violations. *MIS Quarterly*, 487-502.

Tade, O., & Aliyu, I. (2011). Social organisation of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2).

Tavani H. T. (2013). Cyberethics. In Runehov A.L.C. Oviedo L. (Eds). *Encyclopedia of sciences and religions*. Springer, Dordrecht.

WeulenKranenbarg, M., Holt, T. J.,& van Gelder, J. L. (2017). Offending and victimisation in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap.*Deviant Behaviour*, 1-16.

Yamano, P. (2006). Cyberethics in the elementary classroom: Teaching responsible use of technology. In *Society for Information Technology & Teacher Education International Conference,* 3667-3670. Association for the Advancement of Computing in Education (AACE).

Zetter, K. (2007,November).Is your boss spying on you? It's legal, it's happening and it can get you fired.*Reader's Digest*, 97-103.