Synopsis on Cyberethics Behaviour: A Literature Review

Nurudeen. A. Aderibigbe[1]

Nimbe Adedipe Library
College of Agricultural Management and Rural Development
Federal University of Agriculture, Abeokuta
Ogun State, Nigeria
rabshittu@yahoo.com
aderibigbena@funaab.edu.ng
https://orcid.org/0000-0002-7072-1773

Abstract

This paper provides an overview of the empirical literature on cyberethics issues within an academic environment, specifically young adults' behaviours in using cyber technology. While digital media is a part of the institutional and societal drive for informational inclusion and knowledge development, the ethical practices and behaviours among the users of cyber technology have raised questions on users' awareness and understanding of the implications of ethical violations in cyberspace. Using technology might provide significant theoretical paradigms in understanding how digital media adoption and diffusion, driven by information technology, can vary globally. The study reviews the literature on the emergence of cyber technology ethics, individual characteristics, awareness level, challenges to undergraduates' cyberethics behaviour, and the central role policy plays in strengthening or promoting ethical conduct in cyberspace. This paper provides current information for awareness of CE, teaching and research on information ethics and related domains.

Keywords: cyberethics, information ethics teaching, information ethics research, literature review, Theory of Planned Behaviour (TPB)

Introduction

The research interest in cyberethics is motivated by the interaction of students with cybertechnology in academic institutions. Undergraduate students' exposure to the fast pace of technology impacts their behaviour in relationship to using cyber technology. Thus, as modern information users, undergraduate students cannot afford to ignore proper cyberethical behaviour to navigate their way into the complex cybertechnological superhighway. In the light of this, this author considers it necessary to review the literature on cyberethics for informing proper cyberethical behavior, teaching and research.

Universities provide an enabling academic environment for students to use cyber technology for educational purposes. Consequently, unlimited access to cyberspace has raised concerns over cyberethics behaviours. For example, the increase in intellectual property violations, such as software piracy, counterfeiting in films, music, videos, books and pictures, has become worrisome (Rujoiu & Rujoiu, 2014). These cyberethics behaviours have become a standard feature among students in the university environment and may have implications for their professional life in the larger civil and corporate society. Although ethical rules govern the use of such technology to prevent ethical violations in many institutions, research indicates that

1. The author works as a principal librarian at Federal University of Agriculture, Abeokuta, in Nigeria. He completed his PhD on cyberethical behaviour of students at the University of Zululand, South Africa in 2018.

students lack understanding of ethical issues, awareness and cyber technology use. Students' unawareness ultimately results in decisions without foreknowledge about cyberethic responsibilities and use (Moor 1995).

Human behaviour is classified into two separate but interrelated worlds: real-world behaviour and cyber behaviour. While natural institutions have been with humans from the genesis of human history, cyberspace is only a few decades old, a sequel to the invention of the Internet. According to Yan (2012), cyber behaviour is simply a hybrid of cyberspace and human behaviour, referred to as human behaviour in cyberspace. Similarly, Goritz *et al*. (2012) described cyber behaviour as any physical, social or mental activity human beings engage in while interacting with the Internet within cyberspace.

The term "cyber behaviour" refers to users' behavioural patterns when using different cyber technologies for various purposes. Hence, it is understood to be the usage pattern of new media technologies, focusing on cyberspace. It includes studying what people use the Internet for, how they use it, how often they use it and its various applications (Brandtzæg 2010). Based on the preceding, human activities that involve physical, social or mental engagement in connecting to and interacting in cyberspace could broadly be referred to as "cyber behaviour".

Many studies draw on moral theoretical concepts on the behaviour of cyber technology among young adults within the university environment. Some authors (Vallor 2010; Calvani *et al*. 2012; Plaisance 2013) have called for a consideration of the moral dimensions of cyber technology; yet others (Capurro 2008) advance universal ethical principles for the use of cyber technology. Like other technological inventions and innovations throughout human history, some of the literature affirmed that cyber technology has positive and negative impacts on society and tends to raise moral and ethical questions (Stahl *et al*., 2013; Von Schomberg, 2012).

Not much has been published on the impact of information communications technology (ICT) and ethical use on African societies (Cappuro 2008). There are few scholarly articles on cyberethics in Africa, and research on current unethical behaviour trends is relatively new in this part of the world. Therefore, most African studies on cyberethics take their perspectives from the western philosophical tradition.

This paper consists of an introduction, the research method is explained, the theory of planned behavior is reviewed, an examination and the awareness of issues, challenges of cyberethical behaviour among students, highlighted policy issues, reflection on the reviewed studies and finally conclusions.

How this paper was compiled

In order to capture sufficient literature on cyberethics and related behaviour, literature searches were done in August 2015 using a ten-year window, searched from 2006 to 2016 on cyberethics and related terms in different fields such as computer science, social science, engineering, arts and the humanities, medicine, business management and accounting, on some open-access databases. Searches on Scopus returned 137 results. As is widely known, SCOPUS is the largest abstract and citation database of peer-reviewed literature, indexing 20,000 peer-reviewed journals and 5.5 million conference papers.

Web of Science returned 160 results. This database contains over 12,000 high impact journals and over 150,000 conference proceesings. The analysis of these publications revealed that none of them emanated from Africa. Evidence from the existing related literature shows limitations in scope and content

It was decided that the best literature review to adopt for this paper was the scoping literature review. This implies the scope or coverage of body of literature on cyberethical behaviour. The main advantage of this type of literature review is useful for examining emerging evidence when it is still unclear and it allows for the exploration of general question. Given the reported low-level research output in this research area, this study is designed to discover the

cyberethics behaviour of students and thus support ongoing efforts to curb the high rate of cyberethics violations among students.

Theory of Planned Behaviour (TPB)

The Theory of Planned Behaviour (TPB) informs the lense through which the literature reviewed in this article on cyberethics behaviour is conducted. Research has shown that social, psychological and mental factors influence an individual's cyberethics decision when using cyber technology. Socio-cognitive approaches to understanding the reasoning behind cyberethics behaviour frequently use the Theory of Planned Behaviour. According to the theory, the stronger the subjective norm, the stronger the intention to perform a targeted behaviour (Ajzen, 2011). This premise implies that individuals experience social pressure from their referents to engage in or desist from a targeted behaviour. The Theory of Planned Behaviour assumes that behavioural intention is the most vital determinant of actual behaviour. In contrast, the direct determinants of individual behavioural intentions are attitudes, subjective norms and Perceived Behavioural Control (PBC) (Ajzen 1991).

Deontology and teleology are prominent theories of ethics that have caught the attention of cyberethicists (Basse 2012). Deontological theory of ethics is an approach to ethical decision-making dating back to theorists such as Socrates and, more recently, Kant. Deontology is about the concept of universal truths and principles that need to be adhered to regardless of the situation (MacKinnon & Fiala 2014). Kant's categorical imperative states that an individual confronted with an issue should react consistently, conform to their ethical principles and feel comfortable with the choice made (Plaisance 2007). According to Wood (2007), people make ethical decisions because of anticipated results. Therefore, deontology views the means as more important than the end, unlike teleology, where the end justifies the means.

The societal perspective of the theories mentioned above helps form and employ various tools to control cyberethics behaviour. From a legal perspective, command and control instruments like laws, codes of conduct and acceptable policy play critical roles. From the view of deontologists, breaking the law will contradict their idea of ethics. Therefore, they abide by and comply with legislation regardless of its value (Spangenberg 2016). Contrarily, a teleologist weighs both the consequences and benefits of violating the law. Therefore, authorities must establish stringent penalties to influence teleologists' cyberethics behavioural choices.

Influence of Attitude on Undergraduate Students' Cyberethics Behaviour Intention

Siegfried (2004) reported that university students perceived their attitudes towards various cyberethics behaviours, such as software and music downloading, as acceptable. Furthermore, the students did not believe that using a university system for their benefit was a bad habit as long as it did not affect others negatively.

Aliyu *et al*. (2010) noted that perception and attitude towards cyberethics behaviour significantly influence cyber technology use. They showed that students' attitudes towards cyberethics behaviour depend on background factors, such as general attitude, personality traits, moral values and the sense of right and wrong. Other studies have identified perceived personal gain, personal beliefs and attributes (i.e. religious values) (Leonard & Cronan 2005; Kreie & Cronan 2000). Attitude towards cyberethics intention has also been blamed on the economic and hedonic benefits and negative moral judgement (Cesareo & Pastore 2014). Chiang and Lee (2011) note that female students in a Chinese university have a high regard for effective use of cyber technology, particularly in respecting regulation, privacy and intellectual property rights. Therefore, we can say that many undergraduate students have hostile attitudes to cyber technology usage because there is a lack of legal and moral restrictions. Consequently, many companies have experienced significant losses because of the negative attitudes to cyber technology. Vitell and Muncy (2005) have stated that $1.5 billion was lost in the United States due to the piracy of cyber technology software.

Kelly *et al*. (2009) discovered a positive relationship between age and respondents' attitudes to ease of interaction of information systems. According to Lehnerk *et al*. (2015), factors that influence unethical behaviour and the use of cyber technology among universities include economic, social and cultural factors. ICT researchers observe that universities' poor attitudes and unethical use of ICT pose a problem in the ICT and educational sectors (Chatterjee *et al*., 2015; Karim *et al*., 2009).

On the other hand, Al-Rafee and Cronan (2006) argue that university students' attitudes toward digital piracy are a function of their beliefs related to their behaviour, including happiness, excitement, age and perceived importance of the issue. Banerjee *et al*. (1998) listed various determinants influencing information ethics attitudes, including moral beliefs, organisational climate and self-esteem. Kuo and Hsu (2001) linked information ethics attitude to self-efficacy. Thong and Yap (1998) attributed it to ethical judgment processes, while gender, age, marital position, level of education and cyber technology knowledge and experiences are some of the factors that influence both negative and positive attitudes in cyberethics behaviour (Loch & Conger 1996; McCabe *et al*. 2006).

Influence of Subjective Norms on Behavioural Intention of Cyber Behaviour of Undergraduate Students

Various researchers have examined cyberethics behaviour using subjective norms (Al-Rafee & Cronan 2006; Cronan & Al-Rafee 2008; Conger *et al*. 2013). Subjective norms are reflected in users' perceptions of their parents and friends' assessment of their behaviours. Ajzen (1985) defined it as the "perception of the social pressures put on him to perform or not perform the behaviour in question". Subjective norms are personal, behavioural and social norms, including the influence of parents and friends who provide norms and value judgments that can influence behaviour (Grube *et al*.1986).

The study of Leonard *et al*. (2004) focusing on cyberethics issues concerning ethical behaviour intention using subjective norms among American university students revealed that behavioural choice was influenced by attitude, personal normative beliefs, ego, strength, sex and moral judgment. In addition, Al-Rafee and Cronan (2006), Peace *et al*. (2003), Bebetsosi and Antoniou (2009) discovered that attitudes and beliefs about personal behaviour influence cyberethics behaviour, especially concerning using cyber technology.

In their various studies, Stone *et al*. (2010), Beck and Ajzen (1991), and Harding *et al*. (2007) noted that a subjective norm is a factor that influences the intention of university students to engage in multiple unethical behaviours. Others have acknowledged that subjective norms are significantly related to university students' academic misconduct (Stone *et al.* 2010). Furthermore, subjective norms have been significant predictors of intent to engage in unethical cyber behaviour by undergraduate students. They also discovered that subjective norms were an essential factor favouring academic dishonesty, which significantly influenced the intention to cheat in tests and examinations (Cesareo and Pastore 2014).

Influence of Perceived Behavioural Control on Behavioural Intention towards Cyber Behaviour

Perceived behavioural control is another component of the Theory of Planned Behaviour. It is determined by two other factors: control belief and perceived power, or the motivation to act in a particular manner while drawing inspiration from a perception of the likely success of the executed task. A study found the unethical use of cyber technology to be very high among university students when they perceived that their mates were engaged in various negative ways of using cyber technology (McCabe & Treviño, 1997). Knowing that their mates have previously been involved in unethical use of cyber technology and are getting away with it may increase their desire to join in the behaviour.

Peace *et al*. (2003) conducted a study among university students. Their findings reveal that individual attitudes, subjective norms and perceived behavioural control were significant precursors to their intention to download pirated software illegally. It has also been reported that there is a meaningful relationship between lower academic levels and unethical use of cyber technology in universities. Researchers discovered that unethical use of cyber technology was high among university students who perceived themselves as more knowledgeable about cyber technology (Sahni *et al*. 2012). A study by Nkhugulu and Deda (2013) also affirmed a significant relationship between unethical cyber behaviour and perceived behavioural control on intentions to engage in academic dishonesty due to a lack of sanctions on the sampled students.

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

Influence of Demographic Characteristics on Cyberethics Behaviour among Students

Demographic factors are sometimes adopted as units of measurement to examine their influence on the study phenomenon. It is common among behavioural scientists to refer to them as "personal characteristics" (Tella & Mutula 2008). Studies have listed some demographic variables to include age, gender and religion (Lau *et al*. 2013).

Studies on ethical decision-making in cyberspace are generally determined and searched for from two directions. They can either examine demographic and personality styles of deontological cyber technology users or observe the process of ethical decision-making to identify beliefs and attitudes which lead to cyber technology misuse (Haines & Leonard 2007). Others have observed that research on demographic variables as the determinants of cyber technology ethics of undergraduate students may enrich the body of knowledge concerning the teaching and learning of moral and ethical education (Lau & Yuen 2014). Despite the practical importance, previous studies have failed to consider or paid less attention to this phenomenon in the context of cyberethics education and the eventual behaviour of undergraduate students in institutions in developing economies.

Williamson *et al*. (2010) examined age, gender, college major, number of hours per weekend and the self-rating of their respondents' expertise on cyber technology to determine their ethical or unethical use of devices in the university's cyberspace. In a related study, Shemroske (2011) identified the various demographic variables that may influence the ethical use of cyber technology. These include age, gender, computer experience, software sharing and work experience. In addition, in current literature there is a consensus on the attitudinal description of undergraduate students. Researchers understand that demography and attitudinal factors influence students' cyberethics behaviour (Upshaw & Babin 2010; Chiang & Lee 2011). For instance, a demographic norm depicts how male young adults and students with faster Internet connections are more likely to engage in cyberethics behaviour (Goel *et al*. 2012). Kini *et al*. (2000) noted that unethical behaviour in using the computer are not affected by students' experiences with computers but by social demographic variables such as age. Similarly, studies have established that female students are more aware of various unethical behaviours in using cyber technology than their male counterparts (Domeova & Jindrova 2013; Hu & Lei 2015).

Sargolzaei and Nikbakht (2017) reported that in some cases, gender has a significant impact on the ethics of information technology, which can be due to local traditions, beliefs and cultural factors, especially in Islamic countries. From a traditional and cultural point of view, women are expected to have different values from men; therefore, as Sidani *et al*. (2009) report, women are expected to follow cultural and family values and obey strict constraints.

Awareness of Cyberethics Behaviour among Undergraduate Students

Studies have shown that 50-70% of overall unethical use of cyber technology in institutions directly or indirectly ranges from naivety to intentional ethical violations (Siponen & Vance, 2010). Therefore, improving cyberethics awareness is necessary for improved ethical conduct in using cyber technology within academic institutions.

It is essential to clarify what is meant by awareness in the context of cyberethics behaviour. For Dinev and Hu (2007:390) awareness means "the extent to which a target population is conscious of innovation and formulates a general perception of what it entails. Awareness is an antecedent for the attitude formation stage of cyber ethics intention and behaviour." In the framework and context of this study, this would mean that awareness is an antecedent of attitudes and behavioural intentions. Cyberethics behavioural awareness was developed from the perspective of Butterfield *et al*. (2000:982), who viewed it as "an individual's recognition that his/her potential decision or action could affect the interest, welfare, expectations of the self or others in a fashion that may conflict with one or more ethical standards". Here, awareness is seen as the ability to be alert to scenarios that pose a potential ethical dilemma in cyberspace and cyber technology use. Similarly, awareness as a concept is seen as a primary driver of behaviour in students' cyberethics intentions (Yogesh *et al*. 2012).

Diverse studies have shown awareness to be an essential determinant of cyberethics behaviour. Galvez and Guzman (2009:4) observe that awareness shapes behaviour. Hence, they concluded that "the higher the cyberethics awareness, the higher the cyberethics behaviour practice". Dinev and Hu (2007) found that individuals' awareness of the potential consequences and negative implications of cyber technologies determines the intention to use protective information technologies.

D'Arcy *et al*. (2009) used the deterrence theory to prove that users are highly aware of an institution's countermeasures, such as security education training awareness (SETA) programmes and computer surveillance cyberethics policies to reduce bad cyber technology intentions. North *et al*. (2007) used 465 volunteers in their study to investigate cyber technology security and awareness at black universities. The study reported a lack of understanding of cyber technology security and ethics violations. The study further suggested a need for cyberethics education and awareness training for cyber technology users.

The steady growth and reliance on cyber technology and innovations within academic institutions make the oversight of technology far more complex, political and disruptive than in the past (Falconi 2014). Developing nations have set up awareness and education initiatives to cater for the increased reliance on cyber technology and the accompanying behaviour in cyberspace. They established these initiatives to combat unethical cyber behaviours arising from ignorance (Thomson *et al*. 2006). Kortjan and von Solms (2012) noted that cyberethics awareness and education are prerequisites for ethical implementation in cyberspace. They, however, observed that academic institutions in South Africa offer moral cyber behaviour education and awareness. Igwe and Ibegwam (2014) also noted that many students in Nigerian universities are aware of various cyber ethics violations like plagiarism, copyright violations, computer hacking, misinformation, online gambling and various Internet addictions.

Ngoqo and Flowerday (2014) considered awareness and knowledge as two crucial factors of cyber technology behaviour intentions of students in higher institutions in South Africa. Their result showed a moderate positive correlation between awareness and behavioural intent, which

implies that there is a need for every student in an academic environment to be aware of cyberethics behaviour as a guide to ethical cyber technology use. It can also be said that there is a need for ethical use of information technology to prevent violation of use. Students will use the resources legally when they are aware of the negative cyberethics behaviours. Lysonski and Durvasula (2008) have also noted that a lack of awareness of the social costs of downloading and its consequences in terms of the impact on copyright ownership may increase users' inclination to participate in unethical cyber behaviour. In addition, Tadele (2013) also affirmed this position in his study that students do not believe that cyberethics behaviour could result in monetary loss to some people. The University of North Carolina (2014) reported that many students in the university face various ethical problems, including plagiarism and software piracy.

Adetimirin (2017) conducted a study in two public universities in Nigeria on awareness of cyberethics. The findings revealed that the understanding of cyberethics in Nigerian universities varied, with the level of awareness higher in one university than the other. Other researchers have found a strong correlation between unethical cyber behaviour of students while in the academic environment and later in their future professional lives (Anitsal *et al*. 2009; Martin *et al*. 2009). Summing up this assertion, Kidwell and Kent (2008) observe that the cyberethics behaviours that students learn during their academic pursuit may inform their professional expectations of acceptable digital behaviour in their professional lives. Otherwise, it would not be easy to form an ethical attitude towards using cyber technology.

Challenges of Cyberethicsl behaviour

According to a policy brief by the Economic Commission for Africa (2014), the increasing cyber technological exposure in Africa, especially in the education sector, is characterised by cybercrime, lack of policy, a limited level of awareness of cyber technology-related security issues and cyber technology laws. Bear (2014) commented on challenges in the efforts made by students to act ethically in cyberspace on university campuses and the challenges of institutions teaching the implications of cyber technology. He argued that ethics is often the last priority explored in institutions.

Other factors include the restricted perceptions of cyber technology literacy, the limitations of measuring objectives related to computer implications and ethics, lack of trained staff and teaching materials about cyberethics. Walczak *et al*. (2010) also highlight the following challenges: lack of adequate training and incentives to incorporate cyberethics into the curriculum, inconsistent policies on academic dishonesty on campus, incomprehensive curriculum, inadequate cyberethics education, lack of qualified academics to teach cyberethics and restricted perception of cyber technology.

Despite the undeniable benefits of cyber technology, users and organisations face new challenges stemming from unethical information practices, including invasion of personal privacy and theft of intellectual property (Stylianou *et al*. 2013).Greening *et al*. (2006) also highlights some barriers to students' ethical behaviour in the university cyberspace as it concerns integrating honest content into specialised units. Others have, however, noted that separating the moral issues will result in a lack of connections and will poorly reflect the injection of ethical problems and computing into the field. This notion was also articulated in the study by De Melo and De Sousa (2017), whose study expressed concern about the educational system's open challenges due to lack of coordinated courses in cyberethics education for undergraduate engineering students.

In their study, Lowry *et al*. (2015) draw attention to the challenges of internet policy development. They suggest that acceptable use policies are generally drawn up after an incident has occurred and are usually reactive. Using this model, policy developers initiate standards for dealing with specific cyber behaviours that have previously occurred while trying to forestall future problems. Thus, the articulation of acceptable use policies often conveys a disciplinary

tone understood by students and other users as rules to follow instead of a guiding framework for decision-making (Herath & Wijayanayake 2009).

African researchers have also published their findings on the challenges faced by students in their efforts to behave ethically in cyberspace. For example, Dadzie (2011:68) observed some internal and external obstacles to information ethics within the university environment in Ghana. The study notes a lack of teaching modules on cyberethics and a lack of experts and professionals to teach the course. Since most faculties in the institutions were already overburdened with course loads, it has been difficult for the academic board of the Ghanaian universities to introduce and approve new courses. Other noticeable challenges in a study by Aderibigbe and Ocholla (2020) are: lack of adequate training for teaching cyberethics, lack of cyber morality and ethical conduct in the use of cybertechnology, among others.The study also observed external challenges like the absence of a National Information Policy (NIP) on cyberethics or information ethics. As noted by the author, the situation may be connected to the slow nature of the judicial system to curb the harmful practices regarding cyberethics behaviour. An earlier study by Ocholla (2009) also noted similar challenges.

Other challenges faced by undergraduate students in their efforts to act ethically in cyberspace include restricted perceptions of computer literacy and cyber technology, poor understanding of cyber technology implications and ethics, and the lack of teaching content and materials (Haughton *et al*., 2013).

Influence of Cyberethics Policy in Promoting Ethical Conduct in Cyberspace

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 cyberethics behaviour. Institutions are adopting surveillance systems and continuous monitoring around the globe to spy on their students and other users of their networks (Zetter 2007). Policy adoption is another method used by institutions to deter misuse (Lyu 2012).

The most common form of cyber behaviour regulation within academic institutions is the Acceptable Use Policy (AUP) (Lyu 2012), which is seen as a significant step towards promoting cyberethics. The AUP, or cyberethics policy, is usually a document that every user of cyber technology within an academic institution must sign before accessing the university's network resources. It aims to prevent illegal and unethical activities within the institution's cyberspace. The overall goal of the institution's cyber technology service is to enhance teaching, learning and innovations; hence, the AUP helps to flag any activity deviating from this goal. The development of AUP serves as a reactionary attempt to cope with unethical cyber technology behaviour, both inside and outside the university environment. This approach has created a debate around the role that institutions must play in policing inappropriate activity and the effectiveness of such policies (Gottschalk 2010).

Supporters of the AUP emphasise the need for a straightforward course of action for dealing with Information and Communications Technology issues. According to DiScala and Weeks (2013), established Internet policies help remove uncertainty regarding the security of computer equipment, access and sharing of materials and the availability of services. In a hierarchical analysis of acceptable use policies, Laughton (2008) noted that policies often serve to interpret the role of technology in the educational curriculum. As a result, faculty, students and the public gain the assurance necessary to use cyber technology responsibly. In addition, Dill (2003) opines that establishing guidelines for responsible use provides the reason and support for administrative action when dealing with specific issues within the university.

Critics suggest that using AUP as the sole method for dealing with Information and Communications Technology issues is insufficient to establish a culture of responsibility for ICT

use. Scholars have highlighted the challenges that arose in developing and applying the policy and suggest that the result is the establishment of ambiguous guidelines inapplicable to practical circumstances (Boynton 2004; Kafai *et al*. 2007).

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

In recent times, many researchers have found that students demonstrate misconceptions about Internet policies within their institutions in several cases, which invariably results 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) observes 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 created confusion about what a violation of copyright is. What is apparent in these examples is that "while trying to integrate cyber technology into teaching and learning and instruction process, institutions' managements must deal with highly debated, continually changing, and often incomprehensible policies regulating students' cyber technology behaviour and Internet use" (Davies 2002:60).

Taherdoost *et al*. (2011) conducted an academic survey to investigate knowledge of the educational framework on the future career and behavioural experience of undergraduate students in dealing with ethical dilemmas and cyber technology ethics. The study suggests that professional bodies and institutions should update policies, codes and rules guiding ethical behaviour in cyberspace. Livingstone *et al*. (2011) have found that users also showed a lack of awareness regarding the guidelines in their institutions' policies and tended to use personal judgments when deciding what constitutes inappropriate use. Renee Taylor *et al*. (2006) also found that faculty and students did not share the same perspectives on cyber technology use, which led to differing interpretations of written policies.

Reflection of the reviewed literature

In this paper, factors that influence cyberethical behaviour through the lense of the theory of planned behaviour were highlighted in the introduction and also reflected in the literature. Cyberethical attitude, for instance, is dependent on many factors, both internal (personal values, belief system) and external (societal environment, legal environmnet and so on, arguably a cornerstone of influence on cyberethical behaviour is frequently addressed. Furthermore, as noted above, this focus probably has an impact on the types of cyberethical behaviour addressed and the context of the moral issues involved. As a consequence, there is an uneven characterisation of the attitude's influence in the literature; for instance, the attitude influencers have probably changed over time and might depend on the situation being assessed; thus, attitude could change continually as new influences are introduced, or society changes.

A general dimension that was found in several of the cluster categories represented in the subjective norms angle of the adopted theory is that students agree that their decisions towards cyberethical behaviour are strongly influenced by not only their parents but other significant others, i.e their friends and course peers. This is hardly surprising, since much of the students' behaviour at this stage in life in the university are informed by perceived social pressure of some sort to perform or not to perform a given behaviour (Fishbein and Ajzen 1975), and other people can influence assessment of their behaviours. A possible explanation for these common

phenomena may be the lack of adequent policy guidelines that could enforce compliance with acceptable ethical norms.

Given the focus of this study, this author noted important studies on cyberethics behaviour. For example, Thomas and Ahyick (2010) focused on helping information systems students improve their ethical decision-making. The study found that while students who had taken courses and orientations were more aware of the issues in cyberethics misuse and thought them essential, still there was no significant change in their behaviour; neither was there a difference in their perception of what influenced their ethical decision-making despite taking a complete course module in information ethics.

Chatterjee *et al*. (2015) and Johnson (2007) used a scenario-based academic investigation to uncover the nuances of several factors influencing young adults' unethical cyber behaviour and cyber technology use. The study's results showed nonlinear and distinctive relationships between the study constructs. However, the results suffer from limitations and are especially lacking in appropriate qualitative data that could have revealed additional nuances in tensions and dialectic relationships in the studied variables. A cross-cultural study conducted by Martin and Woodward (2011) compared the cyberethics of American and European technology students. They discovered significant differences in the rating of the ethicality of the studied scenarios, as American students rated most strategies as more unethical than the European participants. However, samples in the study were not scientifically represented, as details of the precise socio-demographic characteristics of respondents in the context of some of the studies were generally lacking. Most of the studies reviewed were conducted with only a single methodological approach, i.e. the quantitative research method. Also, existing theories used to explore current phenomena such as students' cyberethics behaviour seemed inadequate or incomplete. Therefore, the present study has fill this gap by extending the findings of these previous works, using qualitative and quantitative methodological approaches to unravel the phenomenon of cyberethics behaviour of undergraduate students in the studied institutions.

Conclusions

One of the siginificant findings to emerge from this study is that the Theory of Planned Behaviour (TPB) sums up all the variables that express cyber behaviours and the awareness of cyberethics. The theory covers subjective norms, behavioural control and attitudes and portrays how university students operate under the aegis of the university system when utilising cyberspace. Although the theory has its strengths and weaknesses and has been criticised for its weaknesses, its direct and extant relationship with other ethical theories and the practical deliberation that accompanies unethical behaviour among students in cyberspace is critical.

The literature also revealed that university policies on the Internet are deficient among students and that many universities in developing countries do not even have laws regulating the use of cyberspace. This deficiency portrays a high level of ignorance among students and faculty regarding cyberspace even though they are in the citadels of learning, thus impacting the extent of their intellectual development and adherence to global academic advancement.

The results of this literature review support the idea that a need for training staff and students about the preponderance of unethical behaviour in cyberspace and the necessity for increased education, research and theory building on cybertechnology and data ethics. This implies that aggressive awareness campaigns are necessary to ensure that students and faculty are aware of acceptable and unacceptable behaviour online in order to safeguard the integrity of the university.

The review is largely informed by non-African studies that makes contextualisation cumbersome. However students' cyberethical behavior because of increasingly easy access to cybertechnologies used elsewhere in the world, as well more similarities than differences of students behaviour in higher education institutions, makes the reviewed study largely unversally

applicable. For example, although most higher institutions of learning are now conducting online registration and, in some cases, online teaching, their ethical cyber behaviour is not readily known

The literature shows that unethical cyber behaviour is a reality that has bedevilled every known society covered by cyberspace. This means that the battle against unethical cyber behaviour is global and requires a great deal of seriousness from all stakeholders to eradicate it. Further research on cyberethics and cybertechnology environments, issues, challenges and opportunities in different academic environments (eg schools) should be encouraged.

Further research is recommended to determine ways to help students apply ethical principles in cyberspace and their own lives. Voiskounsky's (2009) study on web plagiarism as a cyberethics problem revealed that Russian students had few moral barriers to committing web plagiarism. The study is, however, lacking in theoretical rigour. Similarly, Tahat *et al*. (2014) used theoretical constructs to evaluate the cyber ethics misuse by Middle-Eastern countries. Their study results showed that respondents had a low regard for intellectual property violations. A closer study is that by Chiang and Lee (2011) on ethical attitude and behaviour regarding computer use. The study was a survey of political science students in Taiwan. The study showed that attitude, subjective norm, and perceived behavioural control of the respondents all significantly impacted on personal observations of information ethics and recommended that future research was required on cyberethics in Taiwan and elsewhere.

Acknowledgement

I wish to thank the reviewers of the paper and my PhD research supervisors, Prof. Dennis Ocholla and Prof. Johannes Britz, for reading and commenting on the draft review and encouraging me to publish the paper.

References

Aderibigbe, N.A. and 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.

Adetimirin, A., 2017. Awareness and knowledge of cyber ethics by library and information science doctoral students in two Nigerian universities. *International Journal of Technology Policy and Law*, 3(1):43-55.

Ajzen, I. and Fishbein, M. 1975. A Bayesian analysis of attribution processes. *Psychological bulletin*, *82*(2):261-277

Ajzen, I. 1985. From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer, Berlin, Heidelberg.

Ajzen, I. 1991. The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2):179-211.

Ajzen, I. 2011. The theory of planned behaviour: Reactions and reflections. *Psychology & health*, *26*(9):1113-1127.

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. Retrieved June 30 2016, from *https:// doi.org/10.1109/ ict4m.2010.5971884*

Al-Rafee, S. and Cronan, T.P. 2006. Digital piracy: Factors that influence attitude toward behavior. *Journal of Business Ethics*, 63(3):237-259.

Baase, S. 2012. *A gift of fire. Social, Legal and Ethical Issues in Computing.* Upper Saddle River: Prentice-Hall.

Banerjee, D., Cronan, T.P. and Jones, T.W. 1998. Modeling IT ethics: A study in situational ethics. *Mis Quarterly*:31-60.

Bear, L. 2014. 3 For labour: A jeet's accident and the ethics of technological fixes in time. *Journal of the Royal Anthropological Institute*, *20*:71-88.

Bebetsosi, E. and Antoniou, P. 2009. Gender differences on attitudes, computer use and physical activity among Greek university students, *The Turkish Online Journal of Educational Technology,* 8(2):63-67

Beck, L. and Ajzen, I., 1991. Predicting dishonest actions using the theory of planned behavior. *Journal of research in personality*, *25*(3):285-301.

Boynton, R.S. 2004. The Tyranny of Copyright? *The New York Times*, *25*.

Brandtzæg, P.B. 2010. Towards a unified Media-User Typology (MUT): A meta-analysis and review of the research literature on media-user typologies. *Computers in Human Behavior*, *26*(5):940-956.

Butterfield, K.D., Trevin, L.K. and Weaver, G.R. 2000. Moral awareness in business organizations: Influences of issue-related and social context factors. *Human relations*, *53*(7):981-1018.

Calvani, A., Fini, A., Ranieri, M. and Picci, P. 2012. Are young generations in secondary school digitally competent? A study on Italian teenagers. *Computers & Education*, *58*(2):797-807.

Capurro, R. 2008. Intercultural information ethics: foundations and applications. *Journal of Information, Communication and Ethics in Society*.

Cesareo, L. and Pastore, A. 2014. Consumers' attitude and behavior towards online music piracy and subscription-based services. *Journal of Consumer Marketing*. (Domeova & Jindrova, 2013;

Chatterjee, S., Sarker, S., & Valacich, J. S., 2015. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4):49–87. Retrieved June 30 2016, From *https://doi.org/10.1080/07421222.2014.1001257.*

Chiang, L. and Lee, B., 2011. Ethical attitude and behaviors regarding computer use. *Ethics & Behavior*, *21*(6):481-497.

Conger, S., Pratt, J.H. and Loch, K.D. 2013. Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5):401-417.

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

Dadzie, P.S., 2011. Rethinking information ethics education in Ghana: Is it adequate? *The International Information & Library Review*, *43*(2):63-69.

D'Arcy, J., Hovav, A. and Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research*, *20*(1):79-98.

Davies, M. 2002. Ethics and Methodology in Legal Theory-A (personal) Research Anti-Manifesto. *Law Text Culture*, *6*:7.

Devi, S.R. and Yogesh, P. 2012. Detection of application layer DDoS attacks using information theory based metrics. *CS & IT-CSCP*, *10*:213-223.

Dill, D.D. 2003. An institutional perspective on higher education policy: the case of academic quality assurance. In *Higher Education: Handbook of theory and research* :669-699). Springer, Dordrecht.

Dinev, T. and Hu, Q. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7):23.

DiScala, J. and Weeks, A.C. 2013. Access Denied: School Librarians' Responses to School District Policies on the Use of Social Media Tools. *School Library Research*, *16*.

Elmore, R., Anitsal, M.M. and Anitsal, I. 2011. Active versus passive academic dishonesty: Comparative perceptions of accounting versus non-accounting majors. *Journal of Legal, Ethical and Regulatory Issues*, *14*(2):89-104.

Falconi, T.M. 2014. Global stakeholder relationships governance: An infrastructure. In *Global Stakeholder Relationships Governance: An Infrastructure* (:1-55). Palgrave Pivot, London.

Foltz, C.B., Schwager, P.H. and Anderson, J.E. 2008. Why users (fail to) read computer usage policies. *Industrial Management & Data Systems*.

Galvez, S.M. and Guzman, I.R. 2009. Identifying factors that influence corporate information security behavior. *AMCIS 2009 Proceedings* :765.

Goel, S., Watts, D.J. and Goldstein, D.G. 2012, June. The structure of online diffusion networks. In *Proceedings of the 13th ACM conference on electronic commerce* :623-638).

Göritz, A.S., Singh, R.K. and Voggeser, B.J. 2012. Human Behavior on the WWW. In *Encyclopedia of Cyber Behavior* :117-131. IGI Global.

Gottschalk, P., 2010. Policing cyber-crime. *Igarss 2014*. Retrieved January 25 2016, From *https://doi.org/10.1007/s13398-014-0173-7.2.*

Greening, T., Kay, J. & Kummerfield, B., 2006. Integrating Ethical Content into Computing Curricula. Retrieved February 20, 2016, from *www.acs.org.au/documents/public/crpit/CRPITV30Greening.pdf (*Grube *et al*., 1986).

Haines, R., and Leonard, L. N., 2007. Individual characteristics and ethical decision-making in an IT context. *Industrial Management & Data Systems*, *107*(1):5-20.

Harding, T.S., Mayhew, M.J., Finelli, C.J. and Carpenter, D.D. 2007. The theory of planned behavior as a model of academic dishonesty in engineering and humanities undergraduates. *Ethics & Behavior*, *17*(3):255-279.

Haughton, N.A., Yeh, K.C., Nworie, J. and Romero, L., 2013. Digital disturbances, disorders, and pathologies: A discussion of some unintended consequences of technology in higher education. *Educational Technology*:3-16.

Herath, H. M. P. S., & Wijayanayake, W. M. J. I., 2009). Computer misuse in the workplace. *Journal of Business Continuity and Emergency Planning*, 3(3):259–270. Retrieved June 30 2016, *From http://henrystewart.metapress.com/index/Q02418647747G2T4.pdf*

Hu, G. and Lei, J. 2015. Chinese university students' perception of plagiarism. *Ethics and Behaviour*. 25:3, 233-255. Retrieved June 30 2016, from *http://10.1080/1080842-2014.923313*

Igwe, K.N. and Ibegwam, A. 2014. Imperative of cyber ethics education to cyber-crimes prevention and cyber security in Nigeria. *International Journal of ICT and Management*, *2*(2):102-113.

Johnson, D. G. (2007). Computer ethics. In *A Companion to Applied Ethics* :608–619. London: Blackwell Publishing Ltd. Retrieved June 30 2016, From *https://doi.org/10.1002/9780470996621.ch45.*

Kafai, Y.B., Peppler, K.A. and Chiu, G.M. 2007. High tech programmers in low-income communities: Creating a computer culture in a community technology center. In *Communities and technologies 2007* :545-563. Springer, London.

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 model of personality. *Computers and Education*, *53*(1), 86–93. Retrieved June 30 2016, From *https://doi.org/10.1016/j.compedu.2009.01.001.*

Kelly, M., Lyng, C., McGrath, M., & Cannon, G. (2009). A multi-method study to determine the effectiveness of, and student attitudes to, online instructional videos for teaching clinical nursing skills. *Nurse Education Today*, *29*(3):292-300.

Kidwell, L. A., & Kent, J. (2008). Integrity at a distance: A study of academic misconduct among university students on and off campus. *Accounting Education: An International Journal*, *17*(S1):S3-S16.

Kini, R. B., Rominger, A., & Vijayaraman, B. S. (2000). An empirical study of software piracy and moral intensity among university students. *Journal of Computer Information Systems*, *40*(3):62-72.

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.

Kreie, J. and Cronan, T.P., 2000. Making ethical decisions. *Communications of the ACM*, *43*(12):66-71.

Kuo, F.Y. and Hsu, M.H., 2001. Development and validation of ethical computer self-efficacy measure: The case of softlifting. *Journal of Business Ethics*, *32*(4):299-315.

Lau, G.K., Yuen, A.H. and Park, J., 2013. Toward an analytical model of ethical decision making in plagiarism. *Ethics & Behavior*, *23*(5):360-377.

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

Laughton, P.A., 2008. Hierarchical analysis of acceptable use policies. *South African Journal of Information Management*, *10*(4):2-6.

Lehnert, K., Park, Y.H. and Singh, N., 2015. Research note and review of the empirical ethical decision-making literature: Boundary conditions and extensions. *Journal of Business Ethics*, *129*(1):195-219.

Lennie, S. 2013. Ethical Complexities in the Virtual World: Teacher Perspectives of ICT Based Issues and Conflicts (Doctoral dissertation). Retrieved June 30 2016, From *https://tspace.library.utoronto.ca/bitstream/1807/35879/7/Lennie_Shawn_SD_201 306_PhD_thesis.pdf*

Leonard, L.N. and Cronan, T.P. 2005. Attitude toward ethical behavior in computer use: a shifting model. *Industrial Management & Data Systems.* 105(9):1150-1171 Retrieved June 30 2016, From *https://doi.org/10.1108/02635570510633239*

Leonard, L.N., Cronan, T.P. and Kreie, J. 2004. What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics?. *Information & Management*, *42*(1):143-158.

Lewis, J.M., Ross, S. and Holden, T. 2012. The how and why of academic collaboration: Disciplinary differences and policy implications. *Higher education*, *64*(5):693-708.

Livingstone, S., Haddon, L., Görzig, A. and 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.

Loch, K.D. and Conger, S., 1996. Evaluating ethical decision making and computer use. *Communications of the ACM*, *39*(7):74-83.

Lowry, P.B., Posey, C., Bennett, R.B.J. and Roberts, T.L., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3):193-273.

Lysonski, S. and Durvasula, S., 2008. Digital piracy of MP3s: consumer and ethical predispositions. *Journal of Consumer Marketing*.

Lyu, H.S. 2012. Internet policy in Korea: A preliminary framework for assigning moral and legal responsibility to agents in internet activities. Government Information Quarterly, 29(3):394-402.

MacKinnon, B. and Fiala, A., 2014. *Ethics: Theory and contemporary issues*. Nelson Education.

Martin, D.E., Rao, A. and Sloan, L.R., 2009. Plagiarism, integrity, and workplace deviance: A criterion study. *Ethics & Behavior*, *19*(1):36-50.

Martin, N.L. and 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.

McCabe, D.L. and Trevino, L.K., 1997. Individual and contextual influences on academic dishonesty: A multicampus investigation. *Research in higher education*, *38*(3):379-396.

McCabe, D.L., Butterfield, K.D. and Trevino, L.K., 2006. Academic dishonesty in graduate business programs: Prevalence, causes, and proposed action. *Academy of Management Learning & Education*, *5*(3):294-305.

Melo, C.D.O. and de Sousa, T.C., 2017, May. Reflections on cyberethics education for millennial software engineers. In *2017 IEEE/ACM 1st International Workshop on Software Engineering Curricula for Millennials (SECM)* (pp. 40-46). IEEE.

Moor, J.H., 1995. Is ethics computable? *Metaphilosophy*, *26*(1/2):1-21.

Nkhungulu, C. F. & Deda, F. 2013. An Investigation of Academic Dishonesty in a South African Institution, 2(2):1294–1300.

North, M. M., George, R. & North, S. M., 2007. A brief study of information security and ethics awareness as an imperative component of management information systems. In *Proceedings of the 45th annual southeast regional conference* (pp. 515-516). ACM.

Ocholla, D. (2009). Information ethics education in Africa. Where do we stand? *The International Information & Library Review*, *41*(2):79–88. Retrieved June 30 2016, From *https://doi.org/10.1016/j.iilr.2009.04.001.*

Peace, A. G., Galletta, D. F. & Thong, J. Y., 2003. Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, 20(1):153-177

Phyo, A. H., Furnell, S.M. & Phippen, A.D., 2007. Prerequisites for Monitoring Insider IT Misuse, In Bleimann, U.G., Dowland, P.S. & Furnell, S.M. (Eds.): Proceedings of the Third Collaborative Research Symposium Security, ELearning, Internet and Networking (SEIN 2007):41–52.

Plaisance, P. L., 2007. Transparency: An assessment of the Kantian roots of a key element in media ethics practice. *Journal of Mass Media Ethics*, *22*(2-3):187-207.

Plaisance, P.L., 2013. Media ethics. *International Encyclopedia of Ethics*,:1-11.

Rujoiu, O. and Rujoiu, V., 2014, November. Academic dishonesty and workplace dishonesty: an overview. In *Proc. Int. Manage. Conf* (Vol. 8,:928-938).

Sahni, S. P., Jain, G., Author, C., Gupta, I., Sciences, B., Capano, G., Truong, Y. (2012). A Comparative study on cyber ethics, religious awareness and satisfaction in using Facebook for social networking. *Computers and Education*, *6*(2):5-16 Retrieved June 30 2016, From *https://doi.org/10.1111/1468-5930.00107.*

Sargolzaei, E., & Nikbakht, M. (2017). The ethical and social issues of information technology: A case study. *International Journal of Advanced Computer Science and Applications*, *8*(10):138-146.

Shemroske, K. 2011. *The ethical use of IT: A study of two models for explaining online file sharing behavior*. University of Houston.

Sidani, Y., Zbib, I., Rawwas, M. and Moussawer, T., 2009. Gender, age, and ethical sensitivity: the case of Lebanese workers. *Gender in Management: An International Journal*.

Siegfried, R.M., 2004. Student attitudes on software piracy and related issues of computer ethics. *Ethics and Information technology*, *6*(4):215-222.

Simonson, M., Zvacek, S.M. and Smaldino, S., 2019. Teaching and Learning at a Distance: Foundations of Distance Education 7th Edition.

Siponen, M. and Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly.*:487-502.

Spangenberg, L., 2016. *An exploration of the ethics of scam advertising and advertising awards shows in South Africa* [Doctoral dissertation, University of Pretoria].

Stahl, B.C., Eden, G. and Jirotka, M., 2013. Responsible research and innovation in information and communication technology: Identifying and engaging with the ethical implications of ICTs. *Responsible innovation*, :199-218.

Stone, T.H., Jawahar, I.M. and Kisamore, J.L., 2010. Predicting academic misconduct intentions and behavior using the theory of planned behavior and personality. *Basic and Applied Social Psychology*, *32*(1):35-45.

Stylianou, A.C., Robbins, S.S. and Jackson, P. 2003. Perceptions and attitudes about e-commerce development in China: An exploratory study. *Journal of Global Information Management (JGIM)*, *11*(2):31-47.

Tadele, B. (2013). Motivations behind software piracy: From the viewpoint of computer ethics theories. [Masters' dissertation]. Retrieved June 30 2016, from *http://jultika.oulu.fi/files/nbnfioulu-201405241494.pdf*

Tahat, L., Elian, M.I., Sawalha, N.N. and Al-Shaikh, F.N., 2014. The ethical attitudes of information technology professionals: a comparative study between the USA and the Middle East. *Ethics and information Technology*, *16*(3):241-249.

Taherdoost, H., Sahibuddin, S., Namayandeh, M. & Jalaliyoon, N. (2011). Propose an educational plan for computer ethics and information security. *Procedia - Social and Behavioral Sciences,* 28 :815-819. Retrieved June 30 2016, from *https://doi.org/10.1016/j.sbspro.2011.11.149*

Taylor, D., Bury, M., Campling, N., Carter, S., Garfied, S., Newbould, J. and Rennie, T., 2006. A Review of the use of the Health Belief Model (HBM), the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB) and the Trans-Theoretical Model (TTM) to study and predict health related behaviour change. *London, UK: National Institute for Health and Clinical Excellence*, pp.1-215.

Tella, A., & Mutula, S. M. (2008). Gender differences in computer literacy among undergraduate students at the University of Botswana: Implications for library use. *Malaysian Journal of Library & Information Science*, *13*(1), 59-76.

Thomas, T., and Ahyick, M., 2010. Can we help Information Systems students improve their ethical decision making? *Interdisciplinary Journal of Information, Knowledge & Management.* 2010, Vol. 5, :209-224. Retrieved June 30 2016, from *http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=58079830&S=R&D=iih&EbscoContent=dGJyMMvl7ESeqLE4v%2BbwOLCmr1Cep7VSsq64SLCWxWXS&ContentCustomer=dGJyMOzprkmvqLJPuePfgeyx43zx*

Thomson, K. L., Von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. *Computer Fraud & Security*, *2006*(10):7-11.

Thong, J.Y. and Yap, C.S., 1998. Testing an ethical decision-making theory: The case of softlifting. *Journal of Management Information Systems*, *15*(1):213-237.Upshaw & Babin, 2010;

Union, A. 2015, February. United Nations Economic Commission for Africa. 2014.“. In *Illicit Financial Flows. Report of the High Level Panel on Illicit Financial Flows from Africa”. Commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development*.

University of North Carolina General Administration. (2014). *Student services: Responding to issues and challenges: The fifth compendium of papers*. University of North Carolina General Administration.

Vallor, S. 2010. Social networking technology and the virtues. *Ethics and Information technology*, *12*(2), pp.157-170.

Vitell, S.J. and Muncy, J., 2005. The Muncy–Vitell consumer ethics scale: A modification and application. *Journal of Business Ethics*, *62*(3):267-275.

Voiskounsky, A. (2009). Web plagiarism: Empirical study. *Psychology in Russia: State of the art,* (1996), 565–584. Retrieved June 30 2016, from *https://doi.org/http://dx.doi.org/10.11621/pir.2009.0028*

Von Schomberg, R., 2012. Prospects for technology assessment in a framework of responsible research and innovation. In *Technikfolgen abschätzen lehren*. :39-61). VS Verlag für Sozialwissenschaften.

Walczak, K., & Finelli, C., Holsapple, M., Sutkus, J., Harding, T., and Carpenter, D. 2010. Institutional Obstacles To Integrating Ethics Into The Curriculum And Strategies For Overcoming Them. Paper presented at 2010 Annual Conference & Exposition, Louisville, Kentucky. *10.18260/1-2--16571*

Williamson, S., Clow, K. E., Walker, B. C., and Ellis, T. S., 2011. Ethical issues in the age of the Internet: A study of students’ perceptions using the multidimensional ethics scale. *Journal of Internet Commerce*, *10*(2):128-143.

Yan, Z. ed., 2012. *Encyclopedia of cyber behavior* (Vol. 1). IGI Global.

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