Aug 2nd, 9:00 AM - 12:00 AM

The African Digital Citizen's Awareness of Online Information Privacy

Sam Takavarasha Jr
Women's University in Africa, stjnr1@gmail.com

liezel cilliers
University of Fort Hare, liezelcilliers@yahoo.com

Willie Chinyamurindi
University of Fort Hare

The African Digital Citizen's Awareness of Online Information Privacy

Abstract

Internet access continues to increase among the youth in developing countries, like South Africa, due to the exponential growth of mobile penetration and the higher education system's reliance on Information and Communication Technologies. Higher education graduates are expected to be digital citizens in the workplace, which is characterised by socio-economic inclusion and academic capability. However, this increased exposure to the Internet does present information privacy challenges. This paper investigates young adults' perceptions and concomitant behaviours to protect their information privacy when using Internet sites. The paper further aims to unpack young adults' understanding of the potential problems and their preparedness for privacy breaches that may cause.

The study makes use of Azjen's (2006) Theory of Planned Behaviour (TPB) as its theoretical foundation. A mixed methods approach that consisted of a survey of 148 questionnaires and five focus groups with 31 participants was used to investigate the online information privacy awareness of young adults. The study was conducted at a previously disadvantaged university in the Eastern Cape Province in South Africa and found that most of the students are unaware of the activities that may threaten their online privacy. While some students were aware of potential online identity theft and financial loss, most of them did not use privacy settings or read the terms and conditions when signing up to protect their privacy. The study recommends that privacy awareness of young people must increase and digital skills training must be undertaken in order to protect their information privacy when online.

Keywords

Online information privacy, digital citizen, young adults, South Africa, social media, e-commerce

1. Introduction

The emergence of the African digital citizen is a phenomenon that must stimulate the intellectual curiosity of Information Systems scholars in developing countries given Africa's youthful age structure, which has a potential for driving industrialization (UNECA, 2016). The African digital citizen is emerging at a time that is characterized by leapfrogging from low digital access to ubiquitous computing in the wake of exponential 3G mobile penetration and affordable smart phones in developing countries like South Africa (Haung, 2011). Against this background, there is a need to investigate whether the emergent digital citizen has the necessary digital fluency, i.e. the right digital skills and knowledge of the online environment (NETSAFE, 2016). While digital citizenship is concerned with several issues, the incumbent study focuses

on digital commerce where products are bought and sold, social media such as Facebook and digital security, i.e. precautions to guarantee online safety (Agarwal, Shrivastava, Jaiswal, & Panjwani, 2013).

One of the main risks that threaten the privacy of the individual is that their information can be tracked by Internet service providers (ISPs), mobile phone companies, and any web-based business that holds the private data of individuals for financial purposes (Rao, Schaub, & Sadeh, 2015). The profiling of health records, finances and children's details has been criticised because sensitive data may be used for malicious or unintended purposes (FTC, 2009). Cranor (2012) justifies the need to investigate the new digital user's perception as a lack of awareness and concern may suggest that digital citizens have insufficient skills to protect their data online (Mossberger, Tolbert & Hamilton, 2012).

This paper investigates young adults' perceptions and concomitant behaviours to protect their information privacy when using Internet sites. University students were selected as an appropriate unit of analysis because they have the regular ICT access and technological skills due to their educational background that is synonymous with digital citizenship as articulated by Mossberger et al., (2012). Universities are also responsible for fostering digital citizenship but need to be aware of the extent of the problem to tailor educational programs. The following section presents a literature review, followed by a theoretical framework, methodology, research findings and discussion.

2. Literature Review

This section reviews literature on digital citizenry followed by consumers' attitude towards online safety as well as the online tracking industry, and regulators' efforts to control its negative effects in the context of users' online safety concerns.

2.1 An overview of digital citizenry: Digital citizenship has been defined as the "norms of behaviour for the use of technology" (Ribble, 2014, p. 2) and as "a sensible and reasonable approach to online interaction" (Miles, 2011, p. 1). This study adopted Farmer's (2011) definition that it is "the ability to use technology safely, responsibly, critically, productively, and civically" (p. 292). There is a growing body of literature on digital citizens that focuses specifically on young peoples' increasing online presence and the concomitant opportunities and challenges thereof (Miles, 2011; Mossberger et al., 2012; Ribble, 2014; Al-Zahrani, 2015). South African studies have shown incidences of cyber security breaches and concern for online safety (Kritzinger, 2016; Butler & Butler, 2015). Of particular interest to this study is safe, responsible, critical and productive use of technology which prepares a user for the privacy threats and personalised content opportunities of using the Internet for e-commerce purposes.

Ribble (2014) identified nine key factors that characterize digital citizenship: 1) Etiquette, which refers to electronic standards of conduct or procedure; 2) communication, which is about engaging in electronic exchange of information; 3) education, which is the process of teaching and learning about technology and its use; 4) access, that is participating in electronic society; 5) commerce, which refers to the buying and selling of goods and services over electronic platforms; 6) responsibility, which relates to exercising responsibility for one's deeds and actions on electronic platforms; 7) rights, that is the freedoms extended to everyone in a digital world; 8) safety, which is the physical well-being of a digital technology world, and finally 9) security or self-protection, which is the electronic precautions taken to in order to guarantee safety.

While all of these aspects of digital citizenships are important, this study is mostly concerned with security, commerce, responsibility, etiquette and rights. Security is critical because it affects people's confidence when conducting business over the Internet without fear of financial loss or emotional abuse. Etiquette defines the standards of online conduct and procedure. Such standards will detect the ethics that the OBA industry and other users must adhere to for the Internet to be secure for social and commercial engagement. Finally, the study acknowledges the rights of users to manage their privacy and use of their personal information.

Al-Zahrani (2015) presents digital citizenship as a promising route towards addressing the challenges posed by various forms of information misuse and vulnerability to financial loss, emotional abuse and breach of privacy among other concems. The study presents three key factors that influence digital citizenship i.e.: Internet attitude, computer self-efficacy and computer expertise (Al-Zahrani, 2015). Internet attitude is presented in other studies as 'attitude towards computers' (Sam, Orthman, & Nordin, 2005) and 'technology attitude' (Shelly et al., 2004). It determines digital citizenship because it defines young adults' propensity to use the Internet. Computer self-efficacy is a key aspect of digital citizenship, which is critical to this study. Computer self-efficacy must not be confused with computer expertise, which refers to the user's actual skill. Since computer self-efficacy is concerned with a user's perception of their capacity, it will determine the user's confidence in their ability to protect themselves from the threats and to exploit the opportunities they expect to encounter in cyberspace.

2.2 Young adults' attitude towards online privacy: The attitude of Africa's young people toward online privacy is critical because of its high proportion of young people. Sub-Saharan Africa has the highest proportion of young adults worldwide (Boumphrey, 2012). The literature suggests that 79% of young adults own a smartphone, with 70% using the device to stay connected to their peers making use of social media. Mobile phones have evolved from single-purpose communication devices into dynamic tools that support users in a wide variety of ways (Kinnula and Ijas, 2012). A large proportion of young adults,

between 18-24 years of age, have embraced social media as part of their lifestyle. However, nineteen percent of young adults have reported that they have regrets regarding the disclosures they have made on social media in the past (Madden, 2012; Hayes, van Stolk-Cooke, & Muench, 2015).

Online tracking is one of the core activities of the Online Behavioural Advertising (OBA) industry. There is contentious debate on the utility versus invasiveness of OBA on people's online activity (Mullock, Groom, & Lee, 2010; McDonald & Corner, 2010; O'Donell & Cramer, 2015). Some empirical evidence shows that privacy was of concern to most users who also regarded tracking of online behaviour as invasive (McDonald & Corner, 2010). Leon et al. (2013) found that people's willingness to disclose their personal information were affected by the kind of information, the scope of its use, and the retention period thereof. However, there is also evidence that there is a lack of concern with online safety is due to both users' lack of education on the dangers of Internet usage (Mullock, Groom, & Lee, 2010). Users rarely read the privacy policies of personalized advertisement companies (O'Donell & Cramer, 2015).

3. Theoretical Framework

This study adopted Ajzen's (2006) Theory of Planned Behavior (TPB) to investigate young people's privacy concerns and protection behaviour when using online commercial sites. (Knabe, 2012; Al Nahdi, Habib, & Albdour, 2015; Takavarasha, Chinyamurindi, & Cilliers, 2017). Ajzen's (2006) TPB has previously been used for assessing the behavioural intentions of individuals from various business and social perspectives (Knabe, 2012; Al Nahdi et al., 2015). It posits that an individual's behavioural intention influences their behaviour patterns as articulated by Ajzen, 1991 and Ajzen & Fishbein (1980).

At the centre of the model is **behavioural intention,** which is influenced by the independent variables, control beliefs that determine behavioural control, normative beliefs that establishes subjective norms, and behavioural belief that defines attitude toward beliefs (See Figure 1 below). **Attitude to act** refers to the extent to which a person's perception generates positive or negative feelings about the behaviour of interest, protecting online privacy in this case. **Subjective norm** refers to one's belief in whether significant others, such as parents or peers, believe that he or she is capable of the behaviour. **Perceived behavioural control** refers to the student's perception of the degree of difficulty to perform the behaviour of interest (protect their privacy online) (Ajzen, 1991). This behavior is expected to increase with the students' perception that they have more resources and confidence to perform the behaviour (Ajzen, 1985; Lee & Kozar, 2005). This is operationalized in the study as computer self-efficacy.

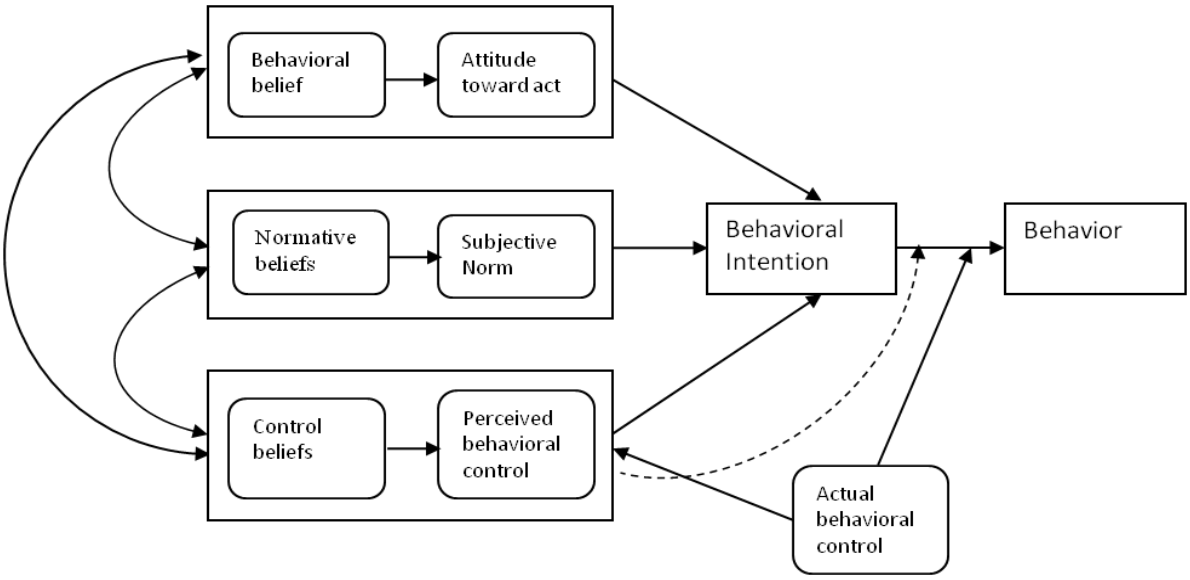


Figure 1: Theory of Planned Behavior (Ajzen, 2006)

The nine factors of digital citizenship are operationalized under the three independent variables of TPB i.e. normative beliefs, behavioural beliefs and control beliefs as follows: *normative beliefs* that establishes subjective norms, encompasses Internet attitude, etiquette, responsibility, and rights. Secondly, *behavioural beliefs* that defines attitude toward beliefs includes, safety, and security or self-protection. Thirdly, *control beliefs* includes, computer self-efficacy, and computer expertise which covers commerce, access, education, and access.

4. Methodology

This study made use of a sequential mixed methods approach that consisted of a survey of 148 questionnaires followed by five focus groups that included 31 participants (Creswell, 2009). The research was conducted at an institution of higher learning in the Eastern Cape of South Africa. The institution under investigation is a previously disadvantaged university which enrolls most of it students from impoverished rural areas in the Eastern Cape. Internet access in the province has been reported to be at 37%. At least 11.3% of this access is at educational institutions and Internet cafes, while in 2014 the majority of the population (80%) accessed the Internet through mobile devices (MyBroadband, 2015). These access patterns are defined by a context of unaffordable internet access where many young people access the Internet at school and mobile devices as articulated by Takavarasha Jr, Cilliers and Chinyamurindi (2018). Such a scenario may provide less opportunity for young people to focus on their personal security as they concentrate on maximizing the value of limited access.

The questionnaire was distributed to 148 students at a university in the Eastern Cape Province of South Africa. The questionnaire was designed as closed questions in the form of a Likert Scale with four options that included Disagree = 1; Disagree Strongly = 2; Agree =3, and Agree Strongly = 4. The questionnaire comprised of two sections: Demographics of the participants, perceived privacy on the Internet organized along the three broad sections (behavioural beliefs, normative beliefs and control beliefs) operationalised from Azjen's (2006) TPB. The collected data were cleaned and imported into SPSSV24 where descriptive and inferential statistics were conducted using frequencies and cross-tabulations respectively Ethical approval was granted by the University's Ethical Research Committee.

After the analysis of the quantitative phase, the researchers designed a follow-up interview guide to investigate the quantitative findings further. The interview was designed to get a deeper understanding of the results in the questionnaire and explore the reasons behind some of the unexpected behaviours of the cohort of young adults that participated in the survey.

Data analysis: In the quantitative data analysis phase, the researchers took the following steps to ensure data validity, reliability and objectivity. Firstly, the researchers attempted to design simple and easy questions to make sure that the respondents would get the same message without misunderstanding them. After this, a pilot study was conducted to validate the questionnaire for user friendliness. A few problems were identified through user feedback, and these were documented and used for refining the final version of the questionnaire.

The researchers adopted selective coding (Glaser, 1992) for analysing the qualitative phase. After the first two focus groups, preliminary coding of the data was conducted. The coding process was repeated after each focus group to assess the emergence of new codes and refine the research instrument before proceeding to the next one. The process seemed to have reached saturation after the researchers conducted five focus groups and the final analysis was conducted.

5. Research Findings

This section presents research findings from the quantitative and qualitative phases. The first section presents the findings of the quantitative phase, which is the survey results. This is followed by the qualitative phase that consists of the focus group results.

5.1 Phase One Quantitative Research Findings

The demographic characteristics of the respondents who participated in the survey showed an increase in privacy awareness with gender and year of study. The gender of the students was evenly distributed while the majority of the students that participated in the in study were in the 2nd and 3rd year of study.

Table 1: Gender distribution and year of study of participants

Item	*Category*	*Frequency*	*Percentage (%)*
Gender			
	Male	*65*	*43.9*
	Female	*83*	*56.1*
	Total	*148*	*100*
Current year of study			
	1st year	*3*	*2,1*
	2nd year	*64*	*43.2*
	3rd year	*61*	*41.2*
	4th year	*20*	*13.5*
	Total	*148*	*100*

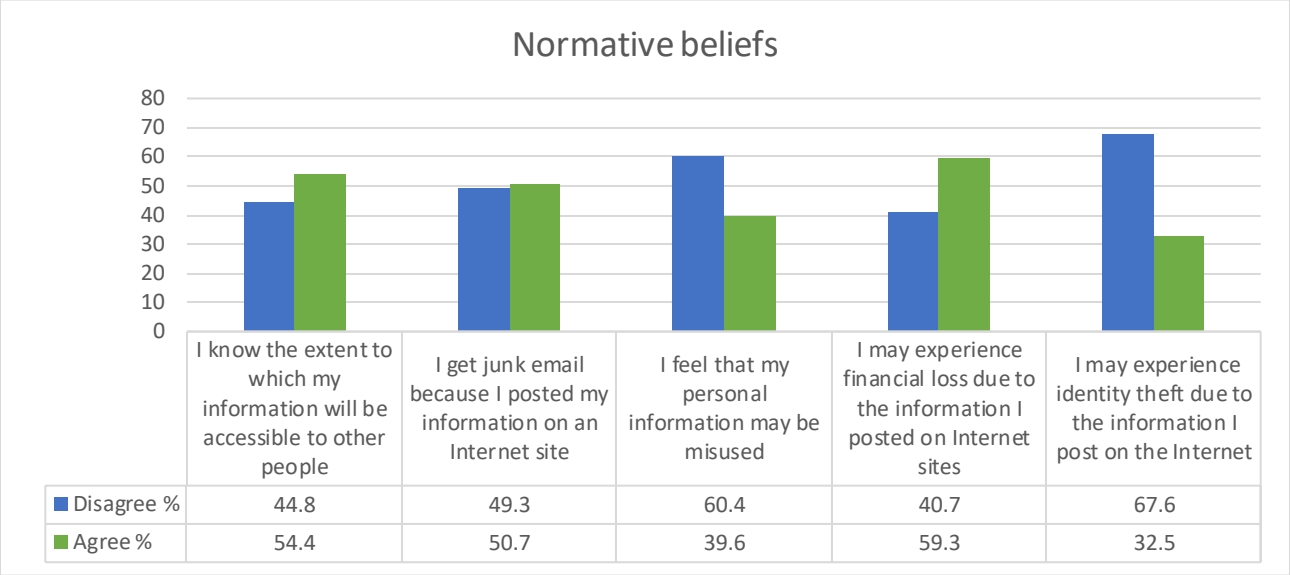
The Pearson's Chi-Square cross tabulation was used to test the various categories against each other. The following were the significant results that were found during this exercise.

- More females were in agreement with the statement 'I control my privacy settings so that what I do on Facebook doesn't show up on my newsfeed' than male students ($\chi = 7.82$; $p < 0.05$).
- A cross-tabulation of 'year of study' and 'privacy self-efficacy' showed that second, third and fourth-year students disagreed with the statement 'I feel confident that I have the skills to protect my privacy on Internet sites' than first years' ($\chi = 20.68$; $p < 0.001$).

The questionnaire addressed normative beliefs through questions that focus on the users' privacy knowledge, and it probed behavioural beliefs through questions that investigated perceived vulnerability of privacy risk and responsibility of users online activity. This was because the researchers expected users' behavioural beliefs to be shaped by their knowledge of the use of their private information as well as their perception of the vulnerability of their private information on the Internet. Lastly, it addressed control belief through sets of questions that address self-efficacy and computer expertise for privacy protection behaviour. This stance was taken because the researchers expected control beliefs to be shaped by one's self-efficacy and that it was predicated on privacy protection behaviour. The following figures (Figure 2 to 4) shows the results for the various categories of the survey.

While most students did agree that they understand the extent to which their information will be accessible to third parties on the Internet, most felt that their personal information would not be misused. Interestingly,

more students perceived that they will not be the victims of identity theft, but rather suffer financial loss due to their personal information that is posted on Internet sites. Very often these two consequences of privacy breaches occur together, but students did not perceive this to be true. It could also be that the students did not perceive identify theft to be a big risk for them due to lack of awareness of this type of fraud.



	I know the extent to which my information will be accessible to other people	I get junk email because I posted my information on an Internet site	I feel that my personal information may be misused	I may experience financial loss due to the information I posted on Internet sites	I may experience identity theft due to the information I post on the Internet
Disagree %	44.8	49.3	60.4	40.7	67.6
Agree %	54.4	50.7	39.6	59.3	32.5

Figure 1: Normative beliefs of students

Figure 2 presents the normative beliefs of the students regarding their personal information on the Internet. The difference between the two groups of students was much smaller for this category, which can indicate that students were less confident when dealing with normative beliefs. Almost the same percentage of students reported that they have the skills to protect their personal information on the Internet, while 58,8% indicated that they were not confident dealing with companies that collect and use their personal information.

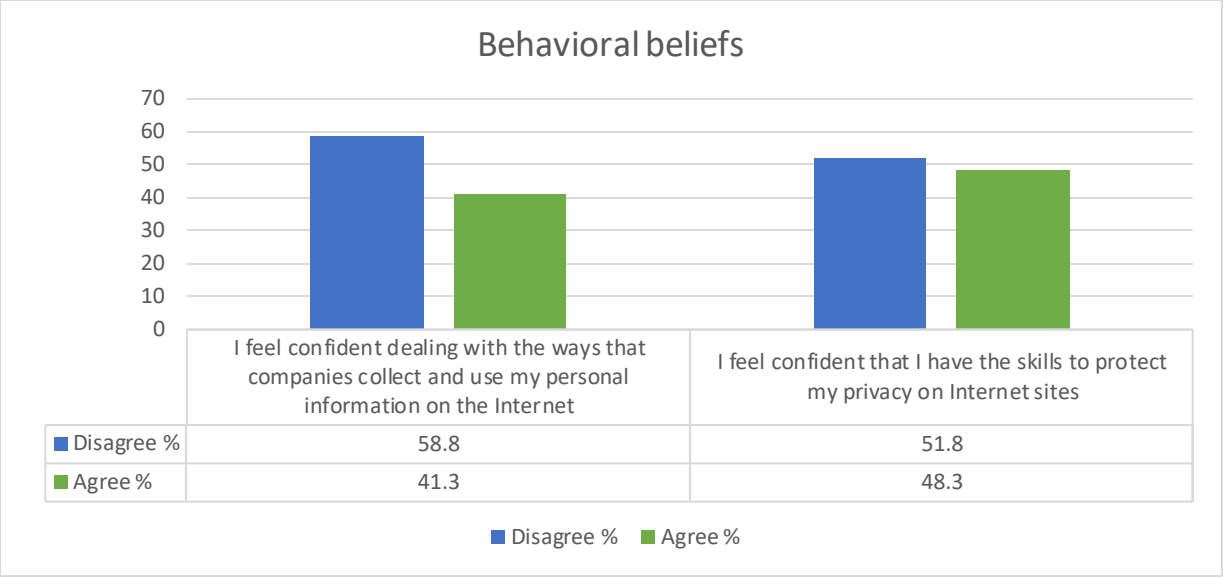


Figure 2: Behavioral beliefs of students

The last category, control beliefs, investigated the actions (i.e. expertise and self-efficacy) that students take to protect their behavior on the Internet. More than two-thirds of the students used a false name or ID when registering on websites, but the same percentage of students provided all the personal information the website requested. This could mean that companies can still trace students when they collect and integrate the personal information that the student offers on their website. Interestingly, more than half of the students (57.1%) indicated that they did read the privacy statement of the website before providing personal information.

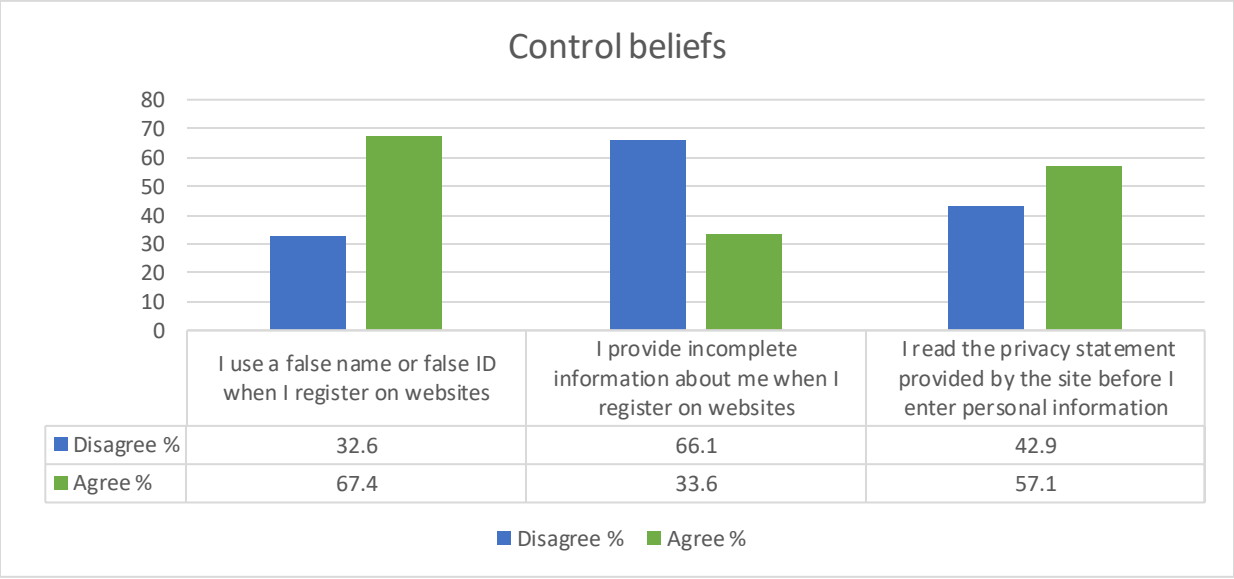


Figure 3: Control beliefs of the students

5.2 Qualitative Data Findings

In this section, the qualitative data that was collected during the focus groups are presented in a table format. Table 2 below presents the theme; the question asked, key extracts from the informants, as well as the location where the focus group was conducted.

Table 1: Focus group results of students' perception of OBA

#	Theme	Quote	Location
Do you know what they do with the personal information we post when subscribing to APPs etc.?			
1	**Privacy Knowledge**: Awareness of use of Personal Information	"No, maybe to check how many people in an area are using that particular app."	(FG 1 EL Campus)
		"I think they may use it to see, to analyse behavioural patterns of certain people and if they want to do advertising they know that this particular person according to the information they posted, they seem interested in this kind of thing then we can tailor-make that advertisement for those people that subscribe to certain things, that is what I think."	(FG 2 EL Campus)
		"Yes, somewhere somehow I think I do, for example, an app for clothing, when you shop online through your email they will check the frequency of your shopping and the things you order, and then the next time you will see emails suggesting some other things similar to what you have shopped before. I think somewhere they store your information on some software to send you other things you might be interested that are similar to what you've shown frequent information on."	(FG 4 A Campus)
		Confidence in the ways that companies collect and use my personal information	
		"In most cases, I do agree that they don't get transparent because sometimes you not even aware of the information that they want but you give it away, not even aware of the company they want it for."	(FG1 EL Campus)
		"…it is unfair because it means companies are not protective of their users because you just cannot trap users like that, they need to protect them so they know what they getting into."	(FG4A Campus)
		"Yes, I trust them because they provide on the internet options to check the legitimacy of the company before you can even join it and since they have to specify where they are located, and it is easy because you can also check how it is rated and that determines a lot even when you read the comments from all over."	(FG2 EL Campus)
		"I cannot say I always disagree with it because sometimes I get to have other interesting things I did not know about even though sometimes the emails from other companies may be boring, I can just say it's 50/50 good and bad."	(FG2 EL Campus)
		"It is not all bad that they share your information, and you receive emails from others, but sometimes I become scared when it comes to the scams."	(FG5 A Campus)
Have you ever felt uncomfortable with the information that a website wanted you to give; tell us why?			
2	Perceived	"Yes, I get suspicious when I am asked for an ID number. I don't have a problem with my age or date of birth but not my ID."	(FG1 EL Campus)

		"My age, when they start to talk about my age, my marital status those things I do not like to talk about."	(FG2 EL Compass)
		"Yes, there was one time when the website asked for my location, and I usually decline because I am not looking for a store near me or anything so I don't understand what does my location have to do with what I am doing online, so I do not give that up. I can't really say I am scared of something but to me it is unnecessary for them to ask for my location."	(FG3 EL Compass)
		"…like for my date of birth and they can access all my documents even on my computer, my bank account and everything even the PIN, so I feel like some very good criminal might invade all my privacy and steal all my belongings. So even though I would like to access their website, I do not trust them. What are they going to use it for, because there are lots of IT criminals out there who can hack that information."	(FG3 EL Compass)
		Do you worry that that information could be abused?	
		"Oh yes, I could find myself married if I was not married already to someone I don't even know, to the extent of making a marriage certificate for identity theft and citizenship frauds."	(FG1 EL Compass)
		"Some people could even sell your identity and your personal information to commit serious crime, I remember the case that happened in maybe 4/5years back in Bloemfontein via Facebook where a lady gave her information and this gentleman took the information and then he tried to get ways to chat with her and meet and the lady ended up raped and killed."	(FG2 EL Compass)
3	Privacy self- efficacy	"For now I would say yes because it all goes back to awareness and knowledge, once one becomes aware and know something then he will have skills to defend himself again these things."	(FG1 EL Compass)
		"I wouldn't say I have necessary skills but I think the only thing that we can do on the internet is not give everything about yourself for example ID number or bank account and when you have an email have strong password."	(FG2 EL Compass)
		"We cannot [protect ourselves]."	(FG3 EL Compass)
		"No, I do not think I have the skills because I feel like the online robbers are always ahead and advanced than us, so the moment we realise their trick they will be on another level, so I think we will never be skilled to win. I think like without taking risks is not life, so we want access to the Internet anyway."	(FG4 Alice Compass)
		"Yes, but you know if you set them for people not to see your information for example in Whatsapp, you also won't be able to see their information and me being curious I want to see others information, so I do not set them."	(FG5 Alice Compass)

Awareness of use of personal information: The results of the focus groups presented in Table 2 show that most students could link the collection of their personal information on commercial websites to analysing online behaviour that could be used for targeted advertising or forecasting of customer demand. Half of the students understood that this could lead to them receiving junk mail, but most found this useful as they were exposed to new items and news. The findings also show that those that had low confidence

(58.8 %) with the way the OBA industry collects their data were concerned about lack of transparency. Furthermore, the results show that those that had some confidence in the marketing efforts of companies considered the value of free content and the opt-out options available to users as fair practice.

Perceived vulnerability or privacy risk: The findings show that the participants were concerned about their personal information, such as ID number, age, marital status and location. If there were no apparent reason as to why the information was needed from the user, e.g. to recommend store locations, students did not feel comfortable providing their personal information to the company. Identity fraud, as well as citizenship fraud (bogus marriage), were two of the main vulnerabilities that students voiced in this category.

Privacy self- efficacy: Half of the participants claimed not to have the skills to protect their information online (52%) suggested it was because they believed that online 'fraudsters' were able to stay ahead of them and that there is a general lack of awareness and education about online privacy. The students that professed to have skills to protect their information (48%) were more aware of the possible risks. Some students believed they would not limit the amount of information provided online because it would stop them from accessing other people's posts on social media.

6. Discussion

This paper investigated young adults' perceptions and concomitant behaviours to protect their information privacy when using Internet sites. The ability of the African digital citizen to cope with the practices of the OBA industry must be judged according to their ability to protect personal privacy. In this study, we have focused on perceived vulnerability, awareness of use of personal information and computer self-efficacy (Al-Zahrani, 2015), and security or self-protection which is the electronic precautions taken to guarantee safety (Ribble, 2014).

The results showed that older students did not think they had the necessary skills to protect their information online. The awareness of senior students as to the consequences of privacy breaches online are likely to increase as they are exposed to information security risks. This is supported by the result that only half of the university students were aware of how to protect their personal information online and did read the privacy policy of the website before providing their personal information. However, students did not take precautionary measures to determine how much of their personal information to volunteer or withhold. While almost half of them did not know what their data was being used for, they did recognise that targeted

marketing could be one of the potential consequences as can be seen in these quotes. A male participant in the EL campus focus groups confirmed the connection between junk mail and personal data posting as follows: "*Yes, in a short space of time you could have 21 emails and that is ridiculous and annoying….*" A female participant added, "*It means they allow other people to get access to your private information, for example, you give one company your information and all of a sudden you are receiving email from other different companies that you didn't give your details, so we are not safe on the internet once we give out our information.*"

There was, however, some concern about identity fraud. While 60% disagreed that their information could be abused, 59% agreed that they may experience financial loss due to information they posted on the Internet. The students interviewed did not think that financial loss could be associated with identify fraud, possibly indicating that they are not using banking services online. These answers are also in contrast to the findings in the questionnaire where financial consequences, and not identity theft, was the main concern of the students.

Participants' concern with security is in line with Kritzinger (2016) who found that there was a concern about the cybersecurity of young South African students, but it does not equip the emergent African digital citizen for the user-friendliness information collection and profiling activities of online retailers. When it was suggested to participants that they would have consented to information sharing and personal profiling when they signed up for a mobile app or opened an Internet account, they expressed surprise. Contrary to our survey findings, which showed that 57% read the terms and conditions when signing up, most of our focus groups did not. Only 43% of our survey respondents disagreed with statement: I read the privacy statement provided by the site before I enter personal information. However, when we followed that up using focus groups, we concluded that the participants were not reading the small print. For instance, a female participant at EL campus stated that she never read the small print. Another participant from the same focus group added, "*I think they should revise that because you cannot be expected to read two pages of agreement in the computer, you will not be able to attend to all the details. They need to be brief and specific, so people do not get bored in reading that.*" This confirms O'Donell and Cramer's (2015) findings that users rarely read online terms and conditions. In this regard, it puts the African digital citizen in the same sphere as their Western counterparts. This erosion of trust capital may hurt companies as consumers and regulators continue to object to the collation, storage and use of their data as articulated by Hunt (2016). A female participant concurred by way of example: "*I remember I went to a gym, and they gave me their contract in the computer screen, so I just signed without reading, and when I got home I realized that if I*

don't pay my debt will pile up and it will be a blacklist threat, and I did not know." This example confirmed the challenge of reading small print on a computer during the signing up process.
When we asked whose fault it was, there was disagreement between the participants. Some felt that the failure to read terms and conditions was their fault as users while others felt the content providers were to blame for making it unreadable.

In our endeavour to assess young people's digital fluency as articulated by NETSAFE (2016), this study also probed their self-efficacy. The findings show that about half of the students claimed to have privacy self-efficacy. Only 52% agreed with the statement: I feel confident that I have the skills to protect my privacy on Internet sites. Focus group findings revealed a different story. A respondent in the A campus focus group categorically emphasised, "*We cannot [protect ourselves]***"**. The same sentiments were echoed by other participants. A typical example was given by one participant at the EL campus: "*No, I do not think I have the skills because I feel like the online robbers are always ahead and advanced than us, so the moment we realise their trick they will be on another level. So I think we will never be skilled to win."* This statement revealed that they did not believe in their capacity to protect themselves as well as their concern with Internet fraudsters. Such differences from South African studies like Butler and Butler (2015) that showed some overestimation of perceived personal ability was plausible because it guarded participants against a false sense of security as articulated by Weinstein (1980). Also emanating from a combination of low self-efficacy and perennial desire to use the Internet was a discernable sense of resignation to fate. This shows that the African digital citizen will use the Internet in spite of their concomitant discontentment with potential privacy breeches. In this regard, this exploratory work is consistent with existing literature (Brandimarte, Acquisti, & Loewenstein, 2013; Smith, Dinev & Xu, 2011; Smith, Milberg, & Burke, 1996). We conclude that the emergent African digital citizens are sacrificing privacy for immediate benefit, just like their Western counterparts although their paths are different.

7. Limitations and future research

We acknowledge a limitation emanating from a research design did not ensure that users are speaking from their experience of the same digital platforms. While our concern was meant to capture behavioural beliefs, normative beliefs and control belief of the African digital citizen on any digital commerce platforms which is exposed to the OBA industry, the survey's measure of privacy awareness may have been influenced by contemporaneous factor emanating from different digital platforms that have different ways of portraying privacy statements.

8. Conclusion

This study shows that online companies have the opportunity to exploit the emerging digital citizen in Africa. The African digital citizen is not security conscious enough to understand and mitigate the security risks that privacy breaches may cause, but will continue the use the Internet regardless. Regulators may need to protect these youths from the Internet companies that profile unsuspecting people. The fact that educated youths are ill-equipped suggests that the other young people could be more vulnerable. There is need for young people to raise awareness and educate themselves about potential consequences of privacy breaches and how to protect themselves from these risks. This study, therefore, concludes that the emergent African digital citizen is not equipped to cope with safeguard their online privacy because of their limited awareness of the use of their personal information by companies.

One of the limitations of using university students as a proxy for all young adults in South Africa's Eastern Cape Province. The majority of young people who were born in the digital age may have different online behaviours and experiences from universities that have constant access to free Internet. As a result, the overall situation may be worse than university students who often have higher levels of digital literacy. Future research should include a wider audience of young adults to generalise the results.

9. Declaration of interest

The authors have no competing interest to declare.

10. References

Agarwal, L., Shrivastava, N., Jaiswal, S., & Panjwani, S. (2013). Do not embarrass: Re-examining user concerns for online tracking and advertising. In Proceedings of the symposium on usable privacy and Security (SOUPS). ACM, 2013.

Ajzen, I. (1985). From intentions to action: a theory of planned behaviour. In J. Huhl, & J. Beckman (Eds.), *Will; performance; control (psychology); motivation (psychology)* pp. 11–39. Berlin and New York: Springer -Verlag.

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behavior and Human Decision Processes*, *50*(2), 179 - 211.

Ajzen, I. (2006). *Constructing a TPB Questionnaire: Conceptual and Methodological Considerations*. Retrieved from the World Wide Web: http://www.people.umass.edu/aizen/pdf/tpb.measurement.pdf.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

Al Nahdi, T. S., Habib. S.A.,& Albdour, A.A. (2015).Factors influencing the intention to purchase real estate in Saudi Arabia: Moderating effect of demographic citizenship. *International Journal of Business and Management*, *10*(4) 35-48.

Al-Zahrani, A. (2015) Toward Digital Citizenship: Examining Factors Affecting Participation and Involvement in the InternetSociety among Higher Education. *International Education Studies*, *8*(12), 203-217.

Beales, H. (2010). *The value of behavioural targeting, Network Advertising Initiative, Jan. 2010*. Retrieved from: www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

Bhattacharyya, M. (2016) A Study on People's Concerns on Social Media Analysis for Online Audience Identification and its Impact on New Media Advertising. *Amity Journal of Media & Communication Studies*, *1*(6), 124-130.

Boumphrey S (2012) Special report: the world's youngest populations. Euromonitor International Market Research, News & Resources. Available at: http://blog.euromonitor.com/2012/02/special-report-the-worlds-youngest-populations.html (accessed 25 March 2017).

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science, 4(3), 340–347. https://doi.org/10.1177/1948550612455931

Butler, R. &Butler, M., 2015). The password practices applied by South African online consumers: Perception versus reality. South African Journal of Information Management 17(1), Art. #638, 11 pages. http://dx.doi.org/10.4102/sajim.v17i1.638

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook. Information Systems Research, 27(4), 848–879. https://doi.org/10.1287/isre.2016.0672

Cranor, L.F. (2012). Can users control online behavioural advertising effectively? Security & Privacy Economics. *IEEE Computer and Reliability Societies*. Available at http://lorrie.cranor.org/pubs/msp2012020093.pdf

Creswell, J. W. (2009). Editorial: Mapping the Field of Mixed Methods Research**,** *Journal of Mixed Methods Research*, (3) 95.

EASA (2011). EASA Best practice recommendation for a European industry-wide self-regulatory standard and compliance mechanism for consumer controls in Online Behavioural Advertising. Retrieved from: http://www.edaa.eu/wp-content/uploads/2012/10/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf

Farmer, L. (2011). Teaching digital citizenship. Paper presented at the Global TIME 2011. Retrieved from http://www.editlib.org/p/37093

FTC (2009) *FTC Staff Report: February 2009 self-regulatory principles for online behavioural Advertising*. Available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

KinnulaMand Ijas T (2012) On the brink of adulthood: a qualitative study of adolescent engagement with the Internet. In: Proceedingsof the 7th Nordic conference on human-computer interaction: making sense through sesign, 14 October 2012, Copenhagen, Denmark, pp. 418–428. Copenhagen: ACM.

Knabe, A. (2012). Applying Ajzen's Theory of Planned Behavior to a Study of Online Course Adoption in Public Relations Education.Dissertations (2009 -). Paper 186.http://epublications.marquette.edu/dissertation

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, *28*(1), 1–17.

Glaser B.G. (1992) *Basics of Grounded Theory Analysis*. MillValley: Sociology Press. Retrieved from: http://www.sciencedirect.com/science/article/pii/S0040162510002489

Haung, C-Y., (2011). Rethinking leapfrogging in the end-user telecom market. *Technological Forecasting & Social Change* 78 (2011) 703–712.

Hayes, M., van Stolk-Cooke, K., & Muench, F. (2015). Understanding Facebook use and the psychological effects of use across generations. Computers in Human Behavior, 49, 507e511.

Lee, Y., & Kozar, K. (2005). Investigating factors affecting the anti-spyware system adoption. Communications of the ACM, 48(8), 72–77.

Leon, P. G., Ur, B, Wangz, Sleeper, M., Rebecca Balebako, R., Shay, R., Bauer, L., Christodorescuy, M., Cranor, L. F., (2013) What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers. Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26,2013, Newcastle, UK.

Madden, M. (2012). Privacy management on social media sites. Pew Internet Report, 1-20.

Mathews-Hunt, K. (2016).Cookieconsumer: tracking online behavioural advertising in Australia.*Computer Law & Security Review ,32* (2016) 55–90.

McDonald, A. M., & Cranor, L. F. (2010) Americans' Attitudes about Internet Behavioral Advertising practices. In Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES) October 4 2010.

McDonald, A.M., & Cranor, L. F. (2010). *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*. Retrieved from http://aleecia.com/authors-drafts/tprc-Behav-AV.pdf

Miles, D. (2011). Youth protection: Digital citizenship-Principles and new resources. Paper presented at the Cybersecurity Summit (WCS), 2011 Second Worldwide.

Mossberger, K., Tolbert, C., & Mamilton, A. (2012). Measuring Digital Citizenship: Mobile Access and Broadband. *International Journal of Communication, 6* (2012), 2492–2528.

My Broadband (2015) Retrieved from https://mybroadband.co.za/news/telecoms/127450-internet-access-in-south-africa-best-and-worst-provinces.html

NETSAFE, (2016). From literacy to fluency to citizenship: Digital Citizenship in Education. Retrieved from: https://www.netsafe.org.nz/wp-content/uploads/2016/11/NETSAFE-WHITEPAPER-From-literacy-to-fluency-to-citizenship.pdf

O'Donnell, K., & Cramer, H. (2015).People's perceptions of personalised ads. International World Wide Web Conference Committee (IW3C2). May 18–22, 2015, Florence, Italy. ACM 978-1-4503-3473-0/15/05. Available at http://dx.doi.org/10.1145/2740908.2742003

Mullock, J., Groom, S. and Lee, P. (2010)International online behavioural advertising survey 2010. Retrieved From: http://www.osborneclarke.com/media/filer_public/f3/5d/f35d8f61-b0cd-485c-afe8-d44b4c13cc4d/international-online-behavioural-advertising.pdf

Online behavioural advertising Tracking and Targeting legislative primer, (2009). Retrieved from: https://www.eff.org/files/onlineprivacylegprimersept09.pdf

Rao, A., Schaub, F., & Sadeh, N. (2015). What do they know about me? Contents and Concerns of Online Behavioral Profiles. Retrieved from file:///C:/Users/201716575/Documents/Forthare%20ACIST/Paper%20OBA/Contents%20and%20Concerns%20of%20OBprofiles_Rao%20et%20al(2015).pdf

Ribble, M. (2014). *Digital Citizenship: Using Technology Appropriately*. Retrieved from http://www.digitalcitizenship.net/uploads/1stLL.pdf

Shelley, M., Thrane, L., Shulman, S., Lang, E., Beisser, S., Larson, T., & Mutiti, J. (2004). Digital citizenship: Parameters of the digital divide. Social Science Computer Review, 22(2), 256-269. http://dx.doi.org/10.1177/0894439303262580

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35(4), 989. https://doi.org/10.2307/41409970

Smith, S. M., Milberg, S. J., & Burke, S. J.(1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly, 20(21), 167–196.

Takavarasha Jr, S., Chinyamurindi, W., & Cilliers, L. (2017).Investigating the privacy concerns and protection behaviour of young people on Face Book in South Africa's Eastern Cape Province. ACIST. Presented at: http://www.acist2017.uct.ac.za/aboutacist.php

Takavarasha Jr, S., Cilliers, L., and Chinyamurindi, W. (2018). Assessing ICT access disparities between the institutional and home front: A case of university students in South Africa's Eastern Cape. *This Changes Everything – ICT and Climate Change: What Can We Do?* In Kreps, D., Ess, C., Leenen, L., and Kimppa, K., (eds.) *This Changes Everything: ICT and Climate Change: What Can We Do? 13th IFIP TC9 International Conference on Human Choice and Computers, HCC13 2018, Poznan, Poland, September 19-21, 2018, Proceedings. Cham, Switzerland: Springer International.*

UNECA, (2016). The Demographic Profile of African Countries. Retrieved From: https://www.uneca.org/sites/default/files/PublicationFiles/demographic_profile_rev_april_25.pdf

Youn, S. (2009). Were of online privacy concern and its influence on privacy protection, among young adolescents. *The Journal of Consumer Affairs*, 43(3)200