

PROCEEDINGS OF THE AFRICAN CYBER CITIZENSHIP CONFERENCE 2016 (ACCC2016)

31 October-1 November 2016
Port Elizabeth
South Africa

Editor:

J.F. Van Niekerk

Publisher:

Nelson Mandela Metropolitan University
PO Box 77000
Port Elizabeth
6031

Proceedings published at
<http://accconference.nmmu.ac.za>

ISBN: 978-1-920508-74-6

TO WHOM IT MAY CONCERN

The full papers for the African Cyber Citizenship Conference 2016 were refereed by a double-blind reviewing process according to South Africa's Department of Higher Education and Training (DHET) refereeing standards. Before accepting a paper, authors were to include the corrections as stated by the peer reviewers. Of the 31 full papers received, 16 were accepted for the Proceedings (acceptance rate: 52%).

Papers were reviewed according to the following criteria:

- Relevancy of the paper to the Cyber-based theme
- Originality and Innovativeness of the research
- Quality of Academic writing and Argument
- Appropriateness and Quality of Literature sources used

The program committee reflected the inter-disciplinary nature of the conference and consisted of international experts in the fields of Information Technology, Law, Psychology, Management, and Education.

Prof. Johan van Niekerk
The Program Chair: ACCC2016

School of ICT
Nelson Mandela Metropolitan University
South Africa
Port Elizabeth

Cell: +27 76 251 7684
Tel: +27 41 504 3048
Email: johan.vanniekerk@nmmu.ac.za

Program Committee ACCC 2016

Name	Email	Affiliation
Adrie Stander	adrie.stander@uct.ac.za	University of Cape Town
Anne Karen Seip	annikken@online.no	Finanstilsynet
Aurona Gerber	aurona.gerber@gmail.com	CAIR, University of Pretoria
Carlos Rieder	carlos.rieder@isec.ch	isec ag
Elmarie Kritzing	kritze@unisa.ac.za	UNISA
Frans Marx	Frans.Marx@nmmu.ac.za	Nelson Mandela Metropolitan University
Gertjan van Stam	g@vanstam.net	SIRDC
Greg Howcroft	greg.howcroft@nmmu.ac.za	Nelson Mandela Metropolitan University
Jacques Ophoff	Jacques.Ophoff@uct.ac.za	University of Cape Town
Jean-Paul Van Belle	Jean-Paul.VanBelle@uct.ac.za	University of Cape Town
Johan van Niekerk	johanvn@nmmu.ac.za	Nelson Mandela Metropolitan University
Karen Renaud	karen.renaud@glasgow.ac.uk	University of Glasgow
Kerry-Lynn Thomson	Kerry-Lynn.Thomson@nmmu.ac.za	Nelson Mandela Metropolitan University
Lech Janczewski	lech@auckland.ac.nz	The University of Auckland
Liesel Cilliers	liezelcilliers@yahoo.com	University of Fort Hare
Lynn Futcher	lynn.futcher@nmmu.ac.za	Nelson Mandela Metropolitan University
Mariana Gerber	mariana@nmmu.ac.za	Nelson Mandela Metropolitan University
Marijke Coetzee	marijkec@uj.ac.za	University of Johannesburg
Marlien Herselman	mherselman@csir.co.za	Meraka Institute, CSIR
Matt Bishop	mabishop@ucdavis.edu	University of California at Davis
Roxanne Piderit	rpiderit@ufh.ac.za	University of Fort Hare
Stephen Flowerday	sflowerday@ufh.ac.za	University of Fort Hare

Table of Contents – Peer reviewed papers

Dating in the Dark: A Phenomenological Study of the Lived Experience of Online Relationships - <i>Carmen Froneman, Gregory Howcroft and Tania Lambert</i>	7
Parent's Perceptions of their Adolescent Children's Internet Use - <i>Zoe Butler and Greg Howcroft</i>	25
The role of social media in coping with relationship dissolution - <i>Tania Lambert, Elzaan Cothill and Gregory Howcroft</i>	38
Personality Traits and Self-Presentation on Facebook: A Systematic Review - <i>Doreen Venter, Gregory Howcroft and Tania Lambert</i>	49
Secondary school teachers' perceptions of incidences of cyber crimes among school-aged children in lagos state, Nigeria - <i>Emmanuel O. Adu and Dr. Adedayo Ige</i>	61
Towards a Cyber Safety Information Framework for South African parents - <i>Elvira Libabat Paraíso and Machdel Matthee</i>	85
An approach to managing social media risks within a South African context - <i>Hanifa Abdullah</i>	97
Digital divide, the role of awareness in the use/non-use of the internet: the experience of South African developing communities - <i>Emilia Mwim and Elmarie Kritzinger</i>	112
The Current State of Security Safeguards within South African Institutions to Achieve Compliance to Condition Seven of the POPI Act - <i>Prittish Dala and Hein Venter</i>	132
The Apple falling far from the tree? Assessing the law of encryption in South Africa - <i>Kessler Perumalsamy and Pieter Koornhof</i>	148
Bow to the King (IV)? A new era for IT governance in South Africa - <i>Hendrik Theron and Pieter Koornhof</i>	161
The impact of the cyber-environment on the natural environment - <i>Woudi von Solms</i>	174
What type of information are South African consumers really looking for on Facebook Brand Fan Pages? - <i>Kim Viljoen, Bramwell Gavaza and Langelihle Dube</i>	188

Me, my cell and I: Selfhood in the Digital Age - <i>Jessica Oosthuizen, Kevin Thomas and Elelwani Ramugondo</i>	202
Students Perceptions & Experiences of Flaming on Social Networking Sites: An Exploratory Study - <i>Willie Chinyamurindi and Pearl Maseko</i>	218
Using personas to understand city residents' information needs and evaluate city information services- <i>Judy Backhouse and Shado Masilela</i>	232

Dating in the Dark: A Phenomenological Study of the Lived Experience of Online Relationships.

C.M. Froneman, J.G. Howcroft (PhD), T. Lambert

Department of Psychology, Faculty of Health Sciences, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa carmenfroneman@gmail.com

Abstract

Online relationships are becoming increasingly popular due to the availability, accessibility, and affordability of online social networking and dating sites. Individuals are progressively moving from meeting romantic partners face to face to meeting and engaging with individuals online. There is ample evidence to support the view that individuals do initiate romantic relationships online and often these relationships progress offline. The primary focus of online research had been conducted by communication and linguistic scholars while very little research has been conducted into the psychological conceptualisation of online relationships. In addition, there is a lack of available research pertaining to the development of romantic relationships online and more so in South Africa.

The current study utilised Sternberg's Triangular model of love and the Johari window as a framework for understanding the concepts involved in online romantic relationships. The study specifically aimed to explore and describe the lived experiences of individuals who engage in online dating. The parameters of the study included the elements that comprise the online relationship, the subjective meaning attached to the relationships, and the processes these relationships encompass. The study moreover aimed to explore the progression of the online relationship.

The study used a qualitative, phenomenological approach using snowball sampling and semi structured interviews to collect data. Tesch's model of content analysis was used during data analysis while incorporating the four major processes in phenomenological research, namely (1) epoche, (2) phenomenological reduction, (3) imaginative variation and, (4) synthesis. The findings of the study generated a greater understanding of the complexities of online dating.

Themes including online relationship development, the dynamics of online relationships, how love, according to the triangular model of love, is perceived online and, self-disclosure online were identified through the participants narratives. These findings ultimately can be used for future research.

Keywords

Cyber-Romance, Johari window, online relationships, relationship development, self-disclosure online, Triangular model of love.

1. Dating in the Dark: An Introduction

From birth to death relationships are the core of human experience, individuals have a strong need to affiliate and relate to other individuals. Belonging to a group enables individuals to survive physically and psychologically (Taylor, Peplau & Sears, 2006). The Internet is one of the most popular ways to find a romantic partner. Creating and nurturing romantic relationships online are now common place in today's society mainly influenced by the various social media opportunities available to individuals (Finkel et al., 2012). The Internet is allowing individuals to meet their affiliation needs without having to meet others physically, it provides a space where individuals can bond and create relationships without meeting face to face. It can be concluded from the literature review undertaken in the present study that most of the research into online relationships has been conducted by communication and linguistic scholars; who have focused on the communication process and patterns that occur in online relationships (Cooper & Sportolari, 1997). Sternberg's triangular theory of love (1986) and the Johari window (Luft & Ingham, 1955) was defined and explored in this study to offer a theoretical understanding of relationships. These theories offered insightful interpretations in which to understand the influences of the lived experiences of online relationships.

The aim of the study was to create an in-depth understanding of the lived experiences of online relationships through the description of the subjective meaning the participants attach to relationships in an online context, and to seek common factors or patterns that emerge between the participant's involvement in these relationships.

2. Literature: Spinning a (World Wide) Web- The Online World.

From what seemed like a very futuristic concept some 20 years ago the Internet has become a modern day necessity. The computer has evolved from a large machine to a simple hand held device allowing individuals to connect to a world of information in a matter of seconds (Whitty, 2003). South Africans are one of the highest users of mobile technology and mobile social networking on the continent, however, stationary Internet and computer ownership lags (UNICEF, 2012). While there is are very few statistics available regarding Internet use in South Africa, Lampen (2010) noted that in 2010 there were 5,3 million South Africans online.

The present literature review focused on exploring the formation of relationships and examine how traditional theories of romantic relationships compare to research regarding online relationships. The core differences between relationships that occur online and relationships that occur offline was explored. The debate regarding whether healthy romantic relationships can be formed online was similarly considered and reviewed. The elements of traditional relationship development, namely, affiliation needs, similarity proximity and familiarity, as well as the theory of relationship development according to Levinger (1980) was furthermore described. A discussion of how relationships are formed online by exploring the underlying motivation for online relationships, the development of online relationships, and the risks involved with engaging in online relationships followed. The literature review concluded by looking at the different ways that online

relationships can be formed, namely via social networking sites and online dating sites, as well as the stigma of online dating and the element of control that individuals experience when using online dating sites.

3. Cyber-Love: Exploring Online Romantic Relationships

Recently the popularity of online dating as an acceptable way to meet partners has increased and has broadened out from a once marginalised and stigmatised activity, to a conventional social way of connecting with possible partners (Antheunis, 2009; Couch, Liamputtong & Pitts, 2012). Online romance, or cyber dating, has emerged as a distinct type of contemporary relationship (Hardie & Buzwell, 2006).

The second aspect within this study explored the Triangular theory of love. The triangular theory of love suggests that love can be understood in terms of three components namely intimacy, passion, and commitment (Sternberg 1986; Sternberg, 1997; Sternberg & Weis, 2006). Together these three components form a triangle that can be applied to a multiplicity of relationships. A relationship can consist of any combination of the components of the Triangle namely passion, intimacy and commitment. There are seven distinct kinds of love identified by Sternberg (1986). What can be concluded from the research is that despite many similarities, intimacy, passion, and commitment function online in a different way to which they function offline, and therefore the different types of love may also function in unique ways. The rich descriptive information shared in online-relationships is vital to the understanding of the nature of online romances (Wildermuth & Vogl-Bauer, 2007). The three components of Sternberg's triangle have been found to exist online to some extent (Van Staden, 2010). Although some studies have found that intimacy and passion can be limited online (Gonyea, 2004), other studies have highlighted the unique ways in which the Internet can make up for these deficits (Cooper & Sportolari, 1997; Couch & Liamputtong, 2008; Ross, 2005; Sprecher, 2009; Whitty, 2003). The components of the triangle interact in a unique way online and while it has been established that relationships can be formed online, the question of whether they can be maintained online and how they are perceived online is still unclear. The primary aim of this study is not to measure the perceptions of individuals regarding their online relationship, rather it aims to provide insight into the dynamics of online relationships, what they entail, and to explore the perceptions of participants regarding what type of love according to Sternberg (1986) they experience online.

The third section explored disclosure in relationships. Self-disclosure is considered an important aspect of communication in interpersonal relationships, including dating and marital relationships. It is considered a major contributor to a sense of intimacy, which is a fundamental component in relationship success (Sternberg, 1986). Verderber and Verderber (2008) agree and suggest that a healthy relationship contains an appropriate balance of self-disclosure and feedback. Self-disclosure, like intimacy, is difficult to define. It is a complex phenomenon that has many components. Essentially, self-disclosure is the telling of previously unknown information so that it becomes shared knowledge, the 'process of making the self

known to others'. Online self-disclosure has been studied predominantly by linguistic and communication scholars with a focus on the content and linguistic process of online disclosure (Baker & Hasting, 2013). There has been little research on the behavioural, emotional, and psychological implications of intimate self-disclosure online explanations for high levels of self-disclosure online is linked to the anonymity the Internet provides which facilitates a level of intimacy that is different from face to face interactions (Joinson, 2001). Self-disclosure can be considered to have the following characteristics: Firstly, it is on a continuum and most individuals have the ability to distinguish what is appropriate and what is not at any particular moment. Secondly, it involves risk and vulnerability on the part of the individual sharing the information and powerful authentic sharing occurs when one person discloses themselves in a way that allows the other to feel free to do the same. Thirdly, self-disclosure also brings with it a sense of shared humanity and vulnerability in individuals. Lastly, self-disclosure is not simply the outcome of a communication, rather, it is both a product and process of interaction, as well as a way of regulating interaction dynamically (Taylor, Peplau & Sears, 2006).

The Johari window (Luft & Ingham, 1955) provided a theoretical lens in which to explore self-disclosure in an online context. The Johari window (Verderber & Verderber, 2008) is a model containing four panes that are used to explain the roles of self-awareness and self-disclosure in relationships (du Plooy-Cilliers & Louw, 2008). Disclosure is an integral part of intimacy within relationships and is considered vital by individuals within the context of an ongoing interaction and wider context regardless of whether that interaction is face to face or online. Online self-disclosure appears to be richer and to progress faster since the Internet affords a context that can reduce feelings of discomfort one may experience in face to face relating. Factors such as anonymity, lack of gating features, and the ability to control the environment effect the level and pace of disclosure online. Trust and deception are linked online to the construction to the individuals 'self' online and individuals who disclose truthful information tend to have relationships that are lasting and can be brought to the real world. A parallel can be drawn to a study done by Gergen, Gergen and Barton (1973). This study found that when individuals interacted in a darkened room where they could not see each other, they engaged in greater self-disclosure and left the experience liking each other more than those who interacted in a brightly lit room. This study can be likened to the current study. Being in a darkened room aptly explains the phenomena of why individuals tend to disclose more online, online they are anonymous and can't be physically seen, hence they feel more open to disclosing information that would usually be undisclosed in a traditional face to face situation.

4. Methodology

The present study used a qualitative exploratory-descriptive phenomenological research design. The research design was used to elicit the quality and texture of the participants' experiences while simultaneously clarifying the meaning attached to the phenomenon through its inductive nature (Smith, 2003). As a phenomenological approach does not include a series of techniques, the understanding of phenomenological processes was incorporated into the study and provided guidance

in terms of the research design. Through the phenomenological approach and application of the four phenomenological processes, the study aimed to elicit and describe the lived experience of online relationships.

Non probability purposive sampling was utilised for the study due to the in-depth and descriptive nature of the research method. The aim of the research is to explore the phenomena as opposed to create any definitive standards. The data collection process consisted of individual, semi-structured interviews. These interviews were guided by an interview schedule but remained flexible to allow for an interactive process that was used to describe the experience of online dating. The interviews were recorded using a recording device to ensure that the data obtained through the interviews was accurately captured. Once the interviews had been conducted, the data was transcribed verbatim by the researcher into text that was used during the data analysis process. Once a preliminary data analysis had been completed, participants were contacted telephonically to verify the information obtained from the interviews.

The four phenomenological processes of epoche, phenomenological reduction, imaginative variation and synthesis of meanings was actualised through the application of Tesch's (1990) eight steps in qualitative data analysis. To ensure the credibility of the data analysis and research findings, an independent research psychologist simultaneously analysed the transcriptions using Tesch's (1990) eight steps. Once the analyses had been completed, the researcher and the independent research psychologist consulted on their findings to ensure the integrity of the findings obtained.

Research ethics provided the researcher with guidelines to establish a balance between values, the pursuit of knowledge, and the rights of those involved in the research. The researcher maintained integrity throughout the research process and took the necessary steps to prevent scientific misconduct.

5. Findings and Discussion

The data analysis produced four main categories in the lived experience of online relationships. These included, (1) dynamics of online dating, (2) online dating and relating, (3) cyberlove, and, (4) language of love: Online self- disclosure. These findings highlighted the lived experience of online relationships.

The first main category focused on the participant's perception of the dynamics that occurred while engaging in online relationships. This category provided a detailed view of the various elements that transpired during the participant's time in the online world. Within this main category seven themes emerged that highlighted the detailed aspects of which online dating comprises of. These included (1) The motivation for using a dating site, (2) triple A of online dating, (3) the unnatural world of online dating, (4) the addictiveness of online dating, (5) the sense of control online dating provides, (6) the perceived stigma of online dating, (7) online rejection.

All the participants conveyed a need to form lasting intimate relationships indicating that this is a primary motivation for joining an online dating site. The participant's descriptions conveyed seven subthemes as motivations for using a dating site, the primary motivation being the need for affiliation which was influenced by other factors including; their age, location, marital status, the time constraints experienced, as well the need to increase the dating pool.

The triple A factors namely affordability, anonymity and accessibility (Leiblum, 1997) emerged in all of the participants accounts of online dating. All of the participants initiated online relationships through paid dating sites, the affordability component was only mentioned briefly. Anonymity was a major factor in all of the participant's accounts of online dating. "In one line of text, an individual can transmit confessional self-disclosure while remaining anonymous" (Lieblum, 1997; p. 2). All participants reported that the capability to construct and control their self-presentation online was important and contributed to their overall experience online. The ability to control self-presentation online influences all aspects (including intimacy and disclosure) of an individual's dating experience (Heino, Ellison & Gibbs, 2010). There is considerable overlap between the ability to remain anonymous and the association of intimate self-disclosure. The idea that individuals have less to lose online allows them to share intimate and often risky information. If this disclosure is reciprocated, it results in intimacy.

The accessible and easy to use dating sites allowed participants in the current study to meet a wide range of individuals and allowed an avenue for romantic relationships to develop. All four participants reported that the accessibility of being able to use laptops and cell phones made it easy for them to communicate with their partners, the participants explained that it required very little effort, it had high controllability and was quicker than communicating in a face to face relationship.

The internet was also described as an unnatural world by the participants. Without a physical context, individuals online are only able to access a portion of their relationship partners and humans need a complete tactile physical presence in order to make a lasting bond (Klein, 2013; Wildermuth & Vogl-Bauer, 2007).

There is a reported feeling of the addictiveness of online dating. Online dating always has a potentiality, this combined with the accessibility of Internet dating and the instant gratification of being able to speak to anyone at any time, which is congruent with a postmodern lifestyle, emphasises the feeling of the next 'fix' (Henry-Waring & Barraket, 2008). Participants reported online dating addictiveness was linked to their self-esteem. They enjoyed the attention and flirty comments because it made them feel good about themselves. This egotism made participants want to keep dating online and looking for new potential partners who would feed them praise and compliments.

There was a sense of control that dating online provided. Participants in the current study reported that they could make decisions about when and how to disclose information about themselves as well as how to respond to messages in their own time, they also reported that they could decide how to disclose negative information

and could construct messages and then reread them before sending them. Participants indicated that they regularly self-regulated the messages and liked the ability to save messages and to disconnect from conversations at any time they wanted. Control can also be extended outward as an individual can easily block interaction and conversations if they decide they do not want to continue, or they can leave the website, log off, or merely shut down their computer (Couch, 2007). Participants reported control over which potential partner they responded to online. They reported feeling comfortable and at ease with 'blocking' individuals or ignoring messages that didn't appeal to them.

The stigma of online dating was apparent in the participant's accounts. All of the participants were apprehensive of using an online dating site at first due to the negative perception of online dating by society. Participants were open to finding love online, however sharing their experiences with their family and friends produced anxiety and hesitancy. Disapproval from family and friends toward online romantic relationships may play a significant role in how online participants assess their relationship's possibility (Wildermuth & Vogl-Bauer, 2007).

Participants reported that they still experienced rejection online, however, it was not the same as offline. The initial emotions experienced were humiliation and decreased self-confidence, but found that it was easier to recover from the 'blow' of rejection due to the fact that the individuals were anonymous. Rejection online elicits the same emotions as offline rejection, namely embarrassment and lowered self-esteem, however, it is easier to manage and recover when compared to face to face situations. Rejection at first contact is not as personal as that of face to face interaction and it becomes easier to cope with because it has less of an impact due to the anonymity factor of online dating (Couch, Liamputtong & Pitts, 2012). Social distance plays a role by providing a buffering effect, especially when it comes to dealing with rejection online (McKenna, Green & Gleason, 2002; Whitty, 2003).

The second category that was highlighted focused on the dynamics that occurred within the online relationships of the individuals. Within this category eight themes emerged that highlighted in-depth aspects that online dating comprises of. These included (1) online relationship development, (2) self-presentation online, (3) online match making, (4) duration of online relationships, (5) online dating rules, (6) online persona versus the real world individual, (7) moving from online to offline, and, (8) meeting face to face

From the stories of the participants a tangible process emerged that was mutual in all four interviews. Firstly Internet dating started with choosing a dating site and filling in forms online about oneself. The motivation for choosing a particular dating site varied from participant to participant, sites that required individuals to pay were common to all participants, the replies in these initial forms would then filter potential partners on the site for them and these would appear on the participant's profile. The next step was to sift through potential partners' profiles, both the profile picture and the biography were deemed as important factors when choosing a

potential partner. Once the participant had chosen a potential partner from the 'catalogue', they would then initiate contact with them by sending them a message, which was premeditated and was the same message for every potential partner. During this stage a simultaneous 'background' check would occur, where the respondents would look for extra information via secondary sources to validate the potential partner. These sources included Facebook, mutual friends, and Internet searches. The participants would concurrently repeat this process with more than one individual. If the response from the potential partner proved negative, the participant would then revert to the 'cataloguing' phase and cycle through the process again. If the potential partner's response was positive the participant would then engage in email communication with the individual and go through a stage of introductions and disclosure. The duration of these conversations would last between 2 to 4 weeks.

Once the individual has established an online relationship and both intimacy and trust had occurred, the participant would then meet face to face. The participant's ultimate goal was to meet offline to see if the relationship could progress any further. Once the respondents met face to face and the outcome of this meeting proved positive, a mutual agreement to remove both parties' profiles from the site was made as a form of commitment to each other (discussed in detail later in the chapter). If the outcome was negative the individual would return to the cataloguing phase or pursue the other individuals with whom they had contact with. This is congruent with Finkel et al., (2012) who proposed a nine step relationship model based on individuals who engaged in online dating sites. The focus of the present study however was aimed at determining whether any unique social dynamics occurred during this relationship development online.

While there was a process that occurred online there was still traditional social mechanisms that occurred (Initial attraction, proximity and familiarity, and similarity) to deduce whether individuals are attracted to a potential partner (du Plooy-Cilliers & Louw, 2008). The present study found these aspects occur in a unique way online.

The present author notes that physical attractiveness and initial attraction were very interesting phenomena that was revealed in the participant's stories. All of the participants agreed that the profile photo was one of the most important aspects when looking for potential partners. Similarity online is an interesting concept as the participants in the current study noted that individuals who sign up for online dating sites already have a similar interest and goal. The more specific a meeting place is online the more common interests will be shared by the individuals (Baker, 2008). This creates an automatic acceptance of others. Similar interests, values, beliefs, ideals, and attitudes between potential partners is a very important feature in interpersonal attraction (du Plooy-Cilliers & Louw, 2008). With regard to online relationships, research points to attraction being highest when the partner is perceived as being both physically attractive and attitudinally similar to oneself (Brehm, 1992; Taylor et al., 2006).

The current study's participants reported that information about a person's beliefs, interests, religious views and biographical data was available in the profiles,

consequently participants could decide whether they had a likeness with a potential partner before actually engaging with them.). All participants made it clear that in order to be able to meet face to face and continue the relationship, the component of proximity was important online. When communicating with individuals outside of their spatial proximity they perceived it as a friendship and explained that the relationship could not advance to a romantic stage albeit that intimacy, passion and intimate disclosure was present.

An important aspect highlighted by the participants was the construction of themselves online. All of the participants reported that their profiles were carefully constructed and information was deliberately added or withheld to ensure that a positive image of themselves was portrayed. Online profiles are fabricated to ensure that the individual is perceived positively and uniquely and is what the individual considers the most important aspects of themselves (Ling Huang & Ching Yang, 2013; McKenna & Bargh, 1999). All of the current participants explained their profiles as an extension of themselves and a way to attract future partners. This is congruent with the description of the Johari window (Verderber & Verderber, 2008) and how feedback effects the formation of panes on the window. As an individual receives feedback regarding their profile or their 'online self' they adapt and remodel themselves online, which is easy to achieve especially when compared to offline.

All of the participants in the study used online dating sites. What emerged from the reports from the participants was a definitive theme of filtering that the online dating site executes for the individuals. Individuals reported completing a list of questions that then filtered out potential partners and provided the individuals with the most suitable candidates. This made the process of finding a potential partner more streamlined and easier. Participants agreed that they did not look at other profiles if they were not recommended by the site and would often go online to see if there were any new matches for them. While participants considered the filtering element important to finding a potential partner, they described negative feelings toward answering the questions. These feelings linked to how others would perceive them and the fear of social judgement. Participants reported using secondary sources to do research on their potential partner before engaging with them. Secondary sources included Facebook, Internet searches and asking mutual friends, family and connected individuals. This research authenticated the person as 'real' by validating their existence and the information provided on their online dating profile.

The first message to a potential partner was also identified as a sub theme. The participants described how their first message to potential partners was usually premeditated and carefully thought out. Once constructed the same message was used for the duration of the time spent on the online dating site, with only minor changes occurring. There were no social rules when sending first messages, participants reported that they received and sent messages equally. The idea that emerged for the participant's descriptions was the more messages the participant could send to potential partners the more likely they would be to connect with someone who was interested. Once the participants met face to face the relationship

was then perceived as a traditional face to face relationship. Online interactions have an exclusive set of 'rules' that were only applicable to this context. The development of online relationships is multifaceted and complex and like all other social phenomena is bound by social contexts and cues (Zaczek & Bonn, 2006). This could be aligned with 'dating rules' that are applied to traditional face to face dating.

Participants reported their potential partners as being different individuals online compared to offline interactions. This had no link between actual deception or intentional dishonesty but more that the conversations online were remarkably different to those had offline with the same individuals. Participants reported that online individuals had more positive personality traits and were perceived more confidently, and when these individuals met face to face the same qualities that were present in previous communication were absent. The current participants reported finding it easier to communicate online and were more open to revealing intimate details about themselves. While these participants admitted to communicating differently online they did not view it as deception or dishonesty. Because individuals can edit and revise text-based messages, they have more opportunities to present themselves in a strategic manner to convey a highly socially desirable image, such strategic self-presentation might entail contextualising negative information in a positive light, selectively revealing negative information over time, actively suppressing negative information, or presenting an impression that reflects one's ideal self or true self rather than one's actual self (Finkel et al., 2012).

While relationships are formed online, it is very rare to find that relationships are maintained online. Many of the relationships formed online, in fact, progress to offline relationships where they continue to develop and function similarly to other traditional romantic relationships (Klein, 2013). The participants reported feeling that online the person did not feel 'real' and by moving to another medium it validated the person's existence. The progression in all the cases was from dating site to mobile to face to face. The importance of meeting offline clearly shows how online dating is used by one participant as a precursor to the embodied experience of dating. This connection could only be validated when meeting face to face and was often determined within the first few minutes of meeting their potential partner. All of the participants agreed that they would not be able to be in a relationship without this element. All participants also reported intense feelings of anxiety when meeting their potential partner face to face. Feelings of awkwardness and nervousness were very real and present. These emotions were absent during communication online with their partner. Participants reported worrying about whether the potential partner would like them in real life.

The third category that was explored comprised of what the participants considered online love to be. Four themes emerged namely, (1) intimacy, (2) passion, (3) commitment and, (4) online love versus offline love. The stories of the participants suggest that meaningful relationships do exist, however, they are different when compared to the offline context.

Intimacy online exclusively refers to the interaction that took place via the electronic medium. All participants reported high levels of intimacy online. The reasons for

these included aspects such as anonymity, lack of social cues, constant connection, and the ability to moderate and control their communication online. It is also important to note that the participants in the present study engaged in evaluative intimacy, or emotional expressiveness as it is sometimes known, which is an integral aspect of an intimate relationship which was achieved in a very short period of time. Participants agreed that trust was difficult to establish online. They were aware of the endless opportunities for individuals to portray themselves in the best possible light as well as the prospect of deceit and untruth. Participants in the current study explained that while they disclosed information that was very intimate after trust was formed, they were referring to the trust that their online partner would not judge or reject them and they could be sure that the information they were sharing was not going to be leaked. The participant's dyadic boundaries could not be damaged online and therefore while trust did facilitate disclosure and therefore intimacy, this was only one facet of trust within their online intimate relationship. All participants agreed that intimacy occurred rapidly online and they shared intimate details within two weeks. This is congruent with the 'boom and bust' phenomenon, when individuals reveal more about themselves earlier than they would in face to face interactions, that is, relationships develop rapidly and intensely (Whitty & Gavin, 2001). Such an accelerated process of revelation may increase the chance that the relationship will feel exhilarating at first and become quickly eroticized, but then not be able to be sustained because the underlying trust and true knowledge of the other is not there to support it (Kraut et al., 2002).

All participants reported high levels of passion in terms of sexual intimacy online. Participants explained that engaging in cybersex was the goal of some individuals on the online dating site but they always disengaged with these individuals as they were looking for something more. According to Hatfield and Rapson (1993) passion in the traditional sense refers to a state of intense longing to be with a partner. In a loving relationship, sexual needs may well predominate in this experience. However, other needs, such as those for self-esteem, nurturance, affiliation, dominance, submission, and self-actualisation, may also contribute to the experiencing of passion. Participants in the current study never reported a longing to be with their partner as they were constantly connected to the person and could communicate with them whenever they felt the need arise.

As with previous research (Finkel et al., 2012; Klein, 2013; Lawson & Leck, 2006), current participants reported that commitment was more readily accepted by individuals once they have met their online romantic partner face to face, and while engaging in online relationships there is a fairly low level of commitment. All four participants agreed that this was a negative of online dating, participants explained that it was common practice to communicate with more than one partner online and often while they developed intense romantic feelings for a particular partner they could never be sure that the partner was committed to only them. Participants did however indicate that after meeting individuals face to face and deciding to pursue a traditional relationship, taking their profiles off the dating site indicated commitment to that partner.

What can be reasoned from the participants sentiments above, online relationships do exist and can consist of components of intimacy, passion and commitment. However, these feelings were very short lived and didn't last longer than four weeks. The researcher notes that participants also struggled to identify these components because they felt they didn't occur the same as in offline relationships. When probed as to what commitment, passion, and intimacy meant, they agreed they did at times feel these, however, because they had never met the person it was difficult to accept these feelings as real. It can be concluded that participants did experience elements of love, albeit in a different manner compared to traditional dating. The participants reported the need to meet face-to-face and experience the physical side of intimacy. Without a physical component, online romantic participants are only able to access a portion of their relationship partners and humans may need a more tactile physical presence in order to make a lasting bond (Klein, 2013; Wildermuth & Vogl-Bauer, 2007).

The fourth and final category that was explored was self-disclosure online. Since online interactions have no physical components, the core of an online intimate relationship is the disclosure that occurs between partners. The main themes that were extracted were (1) intimate disclosure, (2) constant connection, (3) rapid disclosure, (4) deception and dishonesty and (5) miscommunication online. Participants agreed that communicating online was different when compared to offline communication and one participant referring to her emails as 'love letters'

All of the participants reported more intimate disclosure online than in their offline relationships. Participants attributed this intimate disclosure largely to the fact that because they were anonymous they felt they could share information with very little recourse. Participants explained feeling at ease and more open to revealing intimate details about themselves. Being able to express the individual's true self over the Internet creates empathetic bonds and facilitates the establishment of intimacy (Bargh, Mc Kenna & Fitzsimons, 2002). In terms of the Johari window (Verderber & Verderber, 2008) individuals are more open to revealing the 'secret pane' of themselves

All participants reported that due to the dating site filtering out potential partners, surface level information such as age, vocation, and interests are already disclosed in the individual's biography on their profile and therefore they don't spend time disclosing surface level information and this adds to the rapid intimate disclosure. In terms of the Johari window (Verderber & Verderber, 2008), the hidden quadrant of the window appears to be small in online relationships, the public window is large as individuals feel freer to disclose information about themselves due to the anonymity the Internet provides. There is a tendency for individuals to maintain information that portrays them in a negative light hidden. The blind window pane in the Johari window (Verderber & Verderber, 2008) can be interpreted as controlled as individuals are free to play with their self-portrayal online and explore different aspects of themselves. The safety and space available for interpersonal interactions on the Internet allows individuals a chance to experiment with putting normally inhibited parts of themselves forward (Cooper & Sportolati, 1997).

Participants reported that the ability to stay connected with their partner allowed them more intimate self-disclosure. They could send messages and connect with their potential partner any time of the day and reported talking for hours a day, every day. This is remarkably different from face to face interactions. In a new relationship face to face interactions would only take place at a prescribed time and place and for a short while.

All participants reported feeling very little dishonesty in terms of intimate disclosure and sharing of information pertaining to feelings and emotions. However, they reported high deception in how individuals online portrayed themselves. Participants reported that once they established a relationship with their partner, the personal information disclosed was truthful and honest and most of the dishonesty was experienced when physical features were not disclosed honestly.

6. Strengths of the Present Study

The present study allowed for several strengths of the research process to be identified. The first strength was the integration of the phenomenological approach and the utilisation of a semi structured interview style. From the qualitative perspective, the richness and complexity of human reality is seen as closely related to the structures and meanings of natural language. Each participant in the current study was given the opportunity to describe their experience fully, giving rich, detailed descriptions of their experience of online relationships. Unstructured conversations were utilised and organised around areas of particular interest, allowing considerable flexibility in scope and depth. This flexibility was particularly valuable in the present study as it allowed the participant to include and discuss other issues that may be used to expand their perception of online relationships.

The format, style, and setting allowed for a high degree of comfort in the interaction between the researcher and participant. The researcher also utilised her experience as a Registered Counsellor to ensure adequate rapport was established. It was found that participants wanted to talk about their experiences. Having audio-taped the conversations facilitated the phenomenological research process most appropriately. It gave the ideal opportunity to contemplate and reflect on the content that emerged through the conversation.

The sampling strategy viewed the participants as the ‘experts’ in the field under study. Participants were all relevant candidates for the phenomenon under study. In addition, all participants had a reasonable – in fact vivid – linguistic capacity. Thus, a major strength in the present study was allowing for the unstructured conversations to be viewed through the ‘phenomenological lens’ of research methodology.

Although this research contributes to psychology’s expanding body of knowledge in South Africa regarding online relationships, it has limitations.

7. Limitations of the Present Study

While a number of aspects of this research can be regarded as strengths of this study, there are some aspects that have been identified as limitations. The first limitation is related to the demographics of the research participants. The study was conducted in Port Elizabeth in the Eastern Cape. Four participants were interviewed. All of the participants were white adults, most of whom spoke English as their home language. Consequently, there is a possibility that the sample of participants in the study did not accurately represent the total population.

A further potential limitation of the study is that by making use of a qualitative study method, it is not possible to infer clear causal relationships (de Vos et al., 2011). Qualitative, exploratory research does not often yield definitive findings, and further explanatory research is needed to obtain satisfactory answers to research questions (Babbie, 2005). Romantic relationships and intimacy is also a complex phenomenon and can be understood as consisting of many components, and is also influenced by the subjective meaning attached by each individual.

A further criticism is that qualitative research lacks the objectivity of the quantitative approach (Schurink, 1998). This limitation can be understood as the differing epistemological viewpoints of these approaches. Qualitative methodology rests on the assumption that research participants understand their worlds by subjective means, and that social scientists need to explore these subjective appraisals if they are to understand human behaviour (Schurink, 1998).

The researcher also notes the limitation of the literature available on the subject of intimacy and self-disclosure in online romantic relationships. Research into the topic of online dating is relatively new and tends to focus on communication processes and not upon psychological constructs such as intimacy, passion or commitment. Journal articles are also expensive due to a majority of the articles being from international scholars, most require payment to receive a copy which limits the researcher.

8. Recommendations

To the best of the researcher's knowledge, this study is one of the few studies conducted in South African focusing on the experience and meaning ascribed to online dating and romantic relationships in the online context. In light of this, the overall broad goal was to obtain exploratory data from which further studies could be conducted. It is recommended that the findings of this study be used to generate further related studies. This study can be replicated in different contexts and with different age groups for more generalisable findings. By including a quantitative element that compares online and offline romantic relationships, more unambiguous conclusions can be reached.

The present studies identified several stages that online relationships move through, additional research into the psychological aspects and emotional components of each stage could provide researchers as well as practitioner's insight into online relationships. Further research into termination of online relationships and the controllability of online dating could similarly be possible.

9. Conclusion

In conclusion, the present study has provided an in-depth account of four participants who engage in online relationships. This qualitative, exploratory study made use of snowball sampling. Data was gathered through an online questionnaire and analysed thematically.

The aim of the study was to explore and describe the lived experience of online relationships in order to gain insight into the elements that comprise the online relationship, the subjective meaning attached to the relationships, the processes these relationships encompass, and the progression of the online relationship. The dynamics of online relationships including anonymity, self-presentation, and how the relationship progresses proved to provide valuable insight into the lived experiences of online relationships. Sternberg's Triangular Model of Love (1986) and the Johari window (Verderber & Verderber, 2008) was used to conceptualise the study.

It is the hope of the researcher that the present study provided the participants with a small opportunity to have their voices heard in the scientific community. In a relatively new field where knowledge is rapidly developing and changing it may be valuable to have such insights to balance the divergent and often extreme views of both the public and social scientists. While the study does have its limitations it provides useful information to further the exploration of online relationships in the South African context.

10. References

- Antheunis, M. L. (2009). *Online communication, interpersonal attraction, and friendship Formation*. Unpublished thesis, Amsterdam school of communication research. Amsterdam, Holland. Retrieved from <http://dare.uva.nl/en/record/299992>.
- Babbie, E., & Mouton, J. (2001). *The practice of social research*. Cape Town, South Africa: University Press Southern Africa.
- Baker, N. M., & Hastings, S. (2013). Teaching self-disclosure through an activity exploring disclosure research and online dating sites. *Communication Teacher*, 1-5.
- Bargh, J. A., Mc Kenna, K. Y. A., & Fitzsimons. G. M. (2002). Can you see the real me? Activation and expression of the true self on the Internet. *Journal of social issues*, 58(1), 33-48.
- Brehm, S. (1992). *Intimate relationships*. New York, NY. McGraw-Hill.
- Cooper, A., & Sportolati, L. (1997) Romance in cyberspace: Understanding online attraction. *Sex Education Therapy*, 22, 7-14.
- Couch, D., Liamputtong, P., & Pitts, M. (2012). What are the real and perceived risks and dangers of online dating? Perspectives from online daters. *Health, Risk & Society*, 14(7-8), 697-714.
- de Vos, A. S., Strydom, H., Fouche, C. B., & Delport, C. S. L. (2011). *Research at grassroots: For the social science and human service professions* (4th ed.). Pretoria, South Africa: Van Schaik Publishers.
- du Plooy-Cilliers, F., & Louw, M. (2008). *Lets talk about interpersonal communication*. Johannesburg, South Africa: Heinemann.
- Finkel, E. J., Eastwick, P. W., Karney, B. R., Reis, H. T., & Sprecher, S. (2012). Online dating: A critical analysis from the perspective of psychological science. *Psychology Science in the Public Interest*, 13(1), 3-66.
- Gergen, K.J., Gergen, M. M., & Barton, W. H. (1973). Deviance in the dark. *Psychology Today*, 7, 129-130.
- Gonyea, J. (2004). Internet sexuality: Clinical implications for couples. *The American Journal of Family Therapy*, 32, 375-390.
- Hardie, E., & Buzwell, S. (2006). Finding love online. *Australian Journal of Emerging Technologies and Society*, 4(1), 1-14.
- Hatfield, E. & Rapson, R. L. (1993). *Love, sex, and intimacy: Their psychology, biology, and history*. New York, NY: Harper Collins.
- Heino, R., Ellison, N. B., & Gibbs, J. L. (2010). Relationshopping: Investigating the market metaphor in online dating. *Journal of Social and Personal Relationships*, 27(4): 427-447.
- Henry-Waring, M., & Barraket, J. (2008). Dating & intimacy in the 21st century: The use of online dating sites in Australia. *International Journal of Emerging Technologies and Society*, 6(1):14 – 33.

- Joinson, A. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, 31, 177-192.
- Klein, M. C. (2013). Love in the time of Facebook: How technology now shapes romantic attachments in college students. *Journal of College Student Psychotherapy*, 27(2), 149-158.
- Kraut, R., Kiesler, S., Boneva, B., Cummings, J., Helgeson, V., & Crawford, A. (2002). Internet paradox revisited. *Journal of Social Issues*, 58, 49-74.
- Lampen, K., (2010). *Facebook usage in South Africa*. Retrieved from <http://www.socialmedialogue.com/facebook-usage-in-south-africa/302/>.
- Leiblum, S. R. (1997). Sex and the net: Clinical implications. *Journal of Sex Education and Therapy*, 22, 21-27.
- Levinger, G. (1980). Toward the analysis of close relationships. *Journal of Experimental Social Psychology*, 16, 510-544.
- Ling Huang, C., & Ching Yang, S. (2013). A study of online misrepresentation, self-disclosure, cyber-relationship motives, and loneliness among teenagers in Taiwan. *Journal of Educational Computing Research*, 48, 1-18.
- Luft, J., & Ingham, H. (1955). *The Johari window, a graphic model of interpersonal awareness*. Proceedings of the Western Training Laboratory in Group Development, Los Angeles, CA: University of California.
- McKenna, K. Y. A., & Bargh, J. A. (1999). Causes and consequences of social interaction on the Internet: A conceptual framework. *Media Psychology*, 1(3), 249-269.
- McKenna, K. Y., Green, A. S., & Gleason, M. E. (2002). Relationship formation on the Internet: What's the big attraction?. *Journal of Social Issues*, 58, 9-31.
- Ross, M. W. (2005). Typing, doing, and being: Sexuality and the Internet. *Journal of Sex Research*, 42(4), 342-352.
- Schurink, E. M. (1998). Deciding to use a qualitative research process. In A. S. De Vos (Ed.), *Research at grass roots: A Primer for the caring professions* (pp. 239-251). Pretoria, South Africa: Van Schaik Publishers.
- Smith, J. A. (2003). *Qualitative psychology: A Practical guide to research methods*. London, England: Sage.
- Sprecher, S., & Hendrick, S. S., (2004). Self-disclosure in intimate relationships: Associations with individual and relationship characteristics over time. *Journal of Social and Clinical Psychology*, 23(6), 857-877.
- Sternberg, J., & Weis, K. (2006). *The new psychology of love*. New York, NY: Yale University.
- Sternberg, R. J. (1986). A triangular model of love. *Psychological Review*, 93(2), 119-135.
- Sternberg, R. J. (1997). Construct validation of a triangular love scale. *European Journal of Social Psychology*, 27, 313-335.

Sternberg, R. J., & Grajek, S. (1984). The nature of love. *Journal of Personality and Social Psychology*, 47, 312-329.

Parents' Perceptions of their Adolescent Children's Internet Use

Z.A. Butler and J.G. Howcroft (PhD)

Department of Psychology, Faculty of Health Sciences, Nelson Mandela
Metropolitan University, Port Elizabeth, South Africa
zoebutler@axxess.co.za

Abstract

Parents' perceptions of their adolescent children's Internet use significantly influences the parental mediation strategies they choose to use with their children. The motivation for this explorative research study was to understand the impact of psychological and social influences on users of the Internet in South Africa. Both locally and internationally, there is a focus on the use of digital Internet devices to facilitate education. Access of South Africans to the Internet, whether for social or educational use does not exist in a vacuum, exempt from the bidirectional forces of the individual and the environment they use the Internet in, whether it is family or academic.

This study firstly focusses on how parents perceive their adolescent children's Internet use, and secondly, how they parent their children's use of the Internet. The common topics and themes that emerged from this study allow for the development and provision of professional services that individuals, couples, families, and groups require for the use of, or exposure to the Internet.

This study uses an explorative-descriptive qualitative research design with an interpretive paradigm and snowball sampling. The qualitative research design focussed on the concepts of self-reflexivity, context, and thick description while utilizing multivocality of 1) international and South African research on cyber citizenship, including cyberbullying, cyber harassment, and legal consequences, with 2) psychological aspects of the psychosocial developmental challenges of adolescents from the iGeneration including the benefits, risks, and dangers of using the Internet, and 3) qualitative data collected from semi-structured interviews with parents from Generation X who are raising and educating a generation of children on the other side of the Digital Divide. Tracy's 8 'Big-Tent' criteria for guiding excellence in qualitative research and Tesch's model of content analysis was used during the content analysis process. Themes and sub-themes that emerged from the analysis of the participants' narratives included 1) experiences: positive and negative, 2) observations: behavioural changes and gender differences, 3) parenting methods: parental interaction, rules, and limits, 4) concerns: risks, and 5) opinions: personal views.

This research study provides a thick description of South African and international literature and combines the literature with the voices of the participants and the researcher to produce discussions based on the findings of this qualitative study. Conclusions, recommendations, and limitations of this study informed future research on cyber citizenship by providing a detailed understanding of the context of South African parents and children, the psychosocial developmental challenges of adolescents and, how educational programmes can be best

created to effectively impact on the generations of parents, teachers and children in South Africa.

Keywords

adolescents, cyber citizenship, cyberbullying, cyber harassment, Generation X, iGeneration, Internet, legal consequences, parental mediation strategies, perceptions, psychoeducation, social comparison, social networking

1. Introduction

“We are now all connected by the Internet, like neurons in a giant brain” (Hawking, 2014, p.1). There is no doubt that the Internet has changed the lives of many individuals. For many children and adolescents the Internet has always existed, having been born into the online generation. With this electronic world comes the lawless world of the World Wide Web (Kowalski, Limber & Agatston, 2008). “Kids can be cruel. And kids with technology can be cruel on a world-wide scale” (Sullivan, 2006, pp.1).

In 2012 UNICEF, in conjunction with the social networking platform Mxit conducted research into the mobile phone usage and the youth of South Africa. This research was conducted due to concern over the particular vulnerability of the South African market. South Africa uniquely straddles a Western and African world. Many of Africa’s youth have access to mobile devices, and the Internet and yet South Africa struggles economically and educationally. In a summary of the findings of the UNICEF study, the researchers report that South African adolescents and youth are the first adopters of mobile technology with 72% of the 15 to 24-year age group owning or having access to a cell phone. This study highlighted that the primary risks faced by South African adolescents and young people online are talking to and meeting strangers, cyberbullying and sexting (UNICEF, 2012).

The Nelson Mandela Metropolitan University is currently involved in a multi-disciplinary research study, working in conjunction with the school of Information and Communication Technology. This ten-year plan is in response to a governmental expectation for research at South African universities to be responsive to societal and national needs. The research conducted is directed at the focus area of combating cyber-crimes through the development of cyber citizenship. The aim of this initiative was not only to generate research at NMMU but also to attract researchers from several of the schools at the university to focus on research in cyber-crime. Cyber citizenship is currently a core institutional research theme for the Nelson Mandela Metropolitan University. By integrating different faculties, this research should have a significant impact and influence on research being conducted on cyber psychology in South Africa.

Therefore, the motivation for this research study was to understand the impact of psychological and social influences on users of the Internet in South Africa. Both

internationally and nationally, there is a focus on the use of electronic Internet devices to facilitate education. Access of South African's to the Internet, whether for social or educational use does not exist in a vacuum exempt from the bidirectional forces of the individual and the environment they use the Internet in, whether it is family or academic.

2. Literature: The Internet – The Good, the Bad and the Ugly

The most significant innovation of the twentieth century has been the invention and development of the Internet (Aldrich, 2013). Once confined to a stationary desktop personal computer attached to a telephone line, the Internet is now accessible from smartphones, laptops, tablets, game consoles, and other electronic devices. With the growth of the Internet, access to the World Wide Web has become an available resource for most urban South African adolescents. Never before has the human race been so connected, and South Africans are amongst the highest percentage of Internet consumers in Africa (Internet World Stats, 2015).

As Internet users, South Africans may appear to be an ageless online community but according to a survey conducted by SurveyCompare ZA in 2014, 40% of South African Internet users are aged 15-24 (SurveyCompare, 2014). This large subgroup is known as the 'iGeneration' has never known the world without the existence of the Internet (Carr, 2010). In comparison, their parents form part of the 'Before and After' group also known as Generation X. These Internet users remember the experience of a time without the Internet and have adjusted to the rapid evolution of an online world.

The information reported from existing research highlights the importance of focussed future research into specific areas of Internet use to inform facets of education, psychosocial development, and human interaction. The literature included reviewing theories of social psychology such as The Lucifer Effect (Zimbardo, 2008), the Theory of Social Comparison (Festinger, 1954), social commentary and criticism from authors and journalists, and extensive anecdotal literature from individual users of the Internet.. At this time, the Internet provides opportunities for the best and worst of human nature, and although there are communities online that regulate behaviour in an attempt to maintain a safe cyber environment, the majority of the Internet remains ungoverned. The literature in this chapter highlighted the importance of developing insight and awareness of the challenges of human nature that need to be continuously brought to the forefront of the media and society. The promotion of cyber citizenship can influence individuals to treat each other with respect and dignity, and promote the very best of what is human

3. Literature: Parenting in the Web – the iGeneration

“The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.” (Schmidt, n.d.)

Through each age of humanity one generation has been tasked with teaching the next. Researchers suggest that not only has the technology and the Internet changed this pattern, but that education, work, and social interaction needs to be reassessed for the viability of functioning with the latest generation of young adults (Johnston, 2013). From 2008 to 2012 over 1500 South African university students from seven universities participated in separate research studies to create an understanding of the differences between generations, and how to approach closing the gap between the age groups to improve education strategies. The results of a review of all seven studies conducted by Johnston (2013) concluded that academics, mostly from the Baby Boomer or Generation X age group, underestimated student's preference and affinity for interactive and online learning. Students were positive about the use of mobile phones and social networking to improve learning methods, with mobile phones ranked highest in both student's daily Internet activities as well as the use of technology related to education (Thinyane, 2010).

The generation gap between parents and adolescents, parenting styles and mediation techniques all form part of the complex difficulties parents of the iGeneration face. This aspect of modern parenting appears to be filled with contradictory beliefs and misguided attempts by parents to apply older techniques established for television watching and video gaming to the very interactive and open world of the Internet. For instance, parents using restrictive mediation strategies believe that communication between parent and child regarding Internet use is important. However, the implementation of this mutual exchange very often does not exist (Shin, 2015). Parents further report that they consider their children to be mostly secure and protected online and did not fear for their current cyber safety as they perceived the restrictive mediation strategy as effective and therefore did not feel any need to add, alter or deviate from their current strategy. Liau, Khoo, and Ang et al., (2008) found that parents overestimate the degree of parental monitoring, effectiveness of restrictions and extent of parental engagement, supervision, and communication regarding their adolescent children's Internet use. They further found that parents underestimate the type of websites their children are viewing and visiting online, and the level of risky behaviour these adolescents participate in online. This level of misguided confidence handicaps parents from being able to grasp the cyber world in which their children are citizens.

Research showed that adolescent children that have positive, interactive relationships with their parents are willing to disclose more information regarding their Internet activity, and that parents trust their adolescent children more online if they perceive an open relationship with high levels disclosure, thus making this desired situation difficult to attain and maintain if both parties are not mutually committed to a relationship (Juvonen & Gross, 2008). Park, Kim, and Cho (2008)

reported that the participants in their study indicated that the quality of the parent-adolescent relationship was more important than the quantity of time spent together.

4. Methodology

To gain understanding about the online use habits and behaviours of South Africans, the researcher identified the need for insight into the iGeneration. From a psychological perspective, parents (caregivers), parenting styles, and a child's family (primary care) environment has significant psychosocial influence in a bidirectional manner on both the child and their familial (primary care) relationships (Erikson, 1968). Recognizing the broad base from which this research needed to be explored, the researcher proposed a research study aimed at exploring and describing parents' perceptions of their adolescent children's Internet use.

An explorative and descriptive design with an interpretive paradigm was used throughout the research process with emphasis on the qualitative concepts of self-reflexivity, context, and thick description (Tracy, 2013). The qualitative processes are further enhanced by the interpretive paradigm concepts of *verstehen*, *social construction*, and *hermeneutics*.

Participants were selected using a non-probability, purposive sampling method. Participants who met the inclusion criteria (through the use of a biographical questionnaire) were interviewed using face-to-face, semi-structured interviews. In order for the present researcher to provide a thick description of and gain insight into the context of the participants, the face-to-face interviews were arranged in an environment most suitable for the participant. Tesch's (1990) eight steps of qualitative data analysis to identify a category, themes and sub- themes from the data. Of importance to the present researcher were the four sub-criteria of the main criterion of credibility, as described by Tracy (2010). Thick description, triangulation, multivocality, and member reflections were highlighted by the researcher throughout the qualitative research process. The present researcher strove to present not only a thick description of the participants, their perceptions, and parenting Internet mediation techniques but also of the body of research and literature relevant to the present study.

5. Findings and Discussion

The findings were presented according to the main category, themes, and sub-themes that emerged from the semi-structured interviews with the participants. The findings highlighted the parents' perceptions of their adolescent children's Internet use and describe the mediation strategies they employed with their children regarding Internet use.

The first main theme that emerged was the experiences of parents, related to their adolescent children's Internet use. Within this theme, two sub-themes were identified, namely the positive and the negative experiences of online use. Participants perceived the Internet as an important and necessary part of their children's academic tools due to the vastness of information accessible on the Internet and the convenience of having access whenever required. When the children were younger, most participants assisted with the use of the Internet for academic purposes. However, as the children matured, most participants perceived an increasing degree of independence and autonomy with regards to Internet use, including a proficiency at finding information for academic tasks. With regards to social networking, participants recognized the benefits of online communication, specifically through social media and in particular interfamilial communication. Participants perceived a higher degree of current pragmatic contact with their children than before, with for instance arranging extra-mural activities. However, this aspect of Internet use also featured heavily in the perceived negative aspects of Internet use.

Some participants perceived social media as a contributor to disconnection in family activities. One participant, in particular, identified the pressure of needing to be 'always on', and she perceived this as an aspect of social networking that may cause emotional stress. Some participants described the negative aspects of Internet use for activities such as online gaming and as with social media, could facilitate contact with strangers online. The risk of exposure to inappropriate content and behaviour online by their adolescent children was perceived as the most negative aspect of Internet use by the participants. Participants related their understanding of the permanence of content online and how this could have detrimental effects for their adolescent children. Participants further perceived the negative aspects of the Internet mostly with concern about strangers or peers exposing their children to inappropriate material or interactions online. They also recognized that undesirable content was available on the Internet. Although they perceived their own adolescent children's behaviour as a possible risk, participants expressed varying degrees of trust in the responsibility of their adolescent children, and belief that the bidirectional communication channels of their parent-child relationships would buffer risky online behaviour. All participants could be described as both supporters and critics of Internet use for their adolescent children.

The second theme identified from the analysis process was observations by participants, of their adolescent children's Internet use. Three sub-themes emerged namely behavioural changes, gender, and general observations. The observations participants reported were based on their perceptions of their adolescent children's online use, and therefore adolescent psychosocial development was considered by the researcher but limited to a brief inclusion in the findings, as understanding what behaviour the participants attributed to Internet use was relevant and part of the objectives of the study. Amongst behavioural changes that participants observed, were the changes in face-to-face social interaction by the adolescents as they matured. At a younger age participants reported that their children appeared to be more enticed to use technology while in the social company of their peers, whereas as they matured their desire for face-to-face interaction appears to have

strengthened. However, one of the participants observed that her eldest child displayed a preference for spending time in her room, alone, when at home. The participant attributed this behaviour to the adolescent having access to the Internet in her room, and that she could watch or do what she preferred opposed to sharing TV watching time with the family. Another participant observed and attributed a change in her youngest child's emotional state after exposure to Internet use. The participant reported an increased level of agitation and aggression in her child after Internet use (mostly gaming) and the participant describes the behaviour as dissipating soon after access to the Internet was removed.

Most of the participants discussed observing differences in Internet use between their male and female children. Participants perceived their female adolescent children as more focussed on academic tasks and social networking, while their male adolescent children made use of the Internet for academic tasks but appeared less adept, possibly through a lack of interest, at digital technology use and more likely to utilize the Internet for gaming purposes, or not at all and participate in other activities. One of the participants, with same gender children, mentioned observing a difference in use patterns between her two children. The participant attributed the differences to age, maturity, and identity development.

In general, participants observed that their iGeneration adolescent children did not always prefer digital technology to paper based, for instance, text books. Participants also observed how access to social media and the Internet has allowed their children to be creative in another medium. Some participants described observations of how their adolescent children chose to resolve conflict in a face-to-face situation versus online, and how their children recognize risky online behaviour by their peers. Most of the observations described in this sub-theme stem from a base of generational difference. This suggests that participants born in Generation X perceive that adolescents from the iGeneration will prefer all interaction, communication, and information to be digital.

The third theme identified is the parenting methods used by participants to mediate their adolescent children's Internet use. The first sub-theme described parental interaction. All participants described open dialogue with their adolescent children regarding Internet use, activity, and behaviour. All participants indicated that this type of communication was established for all aspects of the parent-child relationship, and existed before the children gained access to the Internet. Therefore, it is an extension of existing behaviour and communication patterns. In describing how they discussed social media and the Internet within their families, participants reported a variation in approaches with regards to the individual needs of their children. The individual differences between their children influenced the need and frequency of formal conversations about online use and behaviour. All participants utilized direct monitoring of their adolescent children's Internet activity by viewing online activity and checking devices, but the frequency and intensity varied amongst participants. Participants indicated a decrease in direct monitoring as their adolescent children matured. Some participants highlighted the interactive use of the

Internet with their children, for instance, browsing YouTube together to watch videos, playing online games together, or assisting with homework tasks by guiding Internet searches, particularly if the topic may potentially lead to inappropriate search responses on the Internet. Participants indicated that they used the removal of digital devices as a discipline technique.

In addition to direct monitoring, most of the participants practice restrictive mediation, whereby Internet access is permitted at specified times and amounts at home. All participants observed the challenge as parents, to allow online access and develop trust in their adolescent children, but included that they understood the necessity for the development of independence, responsibility, and autonomy.

The second sub-theme that emerged from the data was that all participants had a rule about having access to their adolescent children's digital devices and passwords for applications and websites. This permitted the participants to implement further rules regarding their adolescent children's online activity. Most of the participants did not permit their children to have contacts on their devices that were people that their children did not know from face-to-face relationships. This extended to online gaming too. In addition, participants extended the rule to include no online contacts that were of an older age. Some participants had rules regarding which social networking sites their children were permitted to use. Some participants had specific rules, customized to their family, including no digital devices used during car trips, no online purchases without parental assistance, and no Internet use during the week, only on weekends.

The final sub-theme of this section focussed on the limits that participants set on their adolescent children's Internet use. These limits were more flexible than the rules and participants observed that the limits changed more over time than the rules. Some of the limits were physical, such as placement of a computer in a family living space, or a limit on data for use in a month. Participants also reflected on what would be a likely catalyst for a change in the parental methods used at present. Participants identified events that had the potential to cause physical or emotional harm to their adolescent children such as cyberbullying, abduction or high-risk Internet use.

The penultimate theme that emerged from the data concerned the risks of Internet use. These included concerns that participants had due to their perceptions of the Internet and information from other sources including the media and first-hand accounts. Participants expressed concerns about the legal consequences of risky online behaviour and the impact such behaviour could have on their children. Participants expressed concern about cyberbullying and, one participant described her concern about disturbances of adolescent sleep patterns.

The final theme identified from the data was collectively interpreted as the personal opinions of the participants. Opinions are important to the study as they are informed from the perceptions of the participants regarding their adolescent children's Internet use. Participant's opinions included the ability to use digital communication to connect with family members in distant places, the pressure of

modern life, and digital technology's positive and negative role. One participant, who has two male gender children, expressed the opinion that if she had female children, she would most likely be stricter and more conservative. The opinions that dominated this theme were about the lack of control participants felt about the Internet and in response, their opinions on understanding that because they have limited control online they have to develop the pragmatic sense that they have done what they can to protect and continue protecting their children.

6. Strengths of the present study

The study allowed for several strengths of the research process to be identified. An identified strength was the use of an explorative and descriptive design with an interpretive paradigm. The broad nature of the topic was particularly suitable to an explorative design, even though objectives of the research study were identified, the participants and the researcher were able to explore perceptions openly through the use of semi-structured interviews. This style of interviewing allowed the participants to freely discuss the open-ended questions asked by the researcher. Participants provided rich descriptions of their perceptions regarding their adolescent children's Internet use, and due to the nature of the interview, the participants and the researcher were able to converse in a manner that allowed for the participant's voice to be clearly expressed in the data.

Following the explorative nature of the design, the descriptive process integrated with the qualitative concepts of context, self-reflexivity, and thick description. The use of Tracy (2010) criterion of credibility with the four sub-criteria of thick description, triangulation, multivocality, and member reflections also guided the researcher in the research process, encouraging the provision of a thick description, requiring the use of self-reflection to gain insight and understanding into the contextual world of the participants and using the resources available to the researcher through access to literature, research, and a research supervisor.

The interpretive paradigm required the researcher to integrate the concepts of *verstehen*, *social construction*, and *hermeneutics*. The researcher attempted to gain insight into the participants' context. This permitted the researcher to empathically interpret the participants' perceptions and describe the participants' reality as constructed from their personal experience, perceptions, and context. The researcher's use of numerous sources of literature and information, including her own professional experience as a researcher of cyber psychology to provide a holistic interpretation of the data, was another strength.

Finally, the researcher's training and experience as a registered counsellor and a clinical psychologist intern are a strength of this study. Training in an institution which requires a constant awareness and adherence to ethical practice, encourages evidence-based integrative techniques, which places an emphasis on the training of self-reflection, and requires a holistic approach to psychology benefitted the

researcher throughout the research process as the qualitative research process is enhanced by these skills.

7. Limitations of the study

While some aspects of this research are considered strengths of this study, limitations have also been identified. The first limitation was related to the sampling method used to identify potential participants. The nature of snowball sampling results in not all individuals in a population being offered the same opportunity to form part of the research sample (Lund Research Ltd., 2012). This sampling method resulted in a homogenous sample of participants with similar demographics. The study was conducted in Port Elizabeth, in the Nelson Mandela Metropolitan area of the Eastern Cape. Five participants were interviewed. All participants were white, adult females, who spoke English as one of their primary languages. Due to this demographic representation the researcher acknowledges that this sample only represents a partial sub-group of persons in South Africa that could meet the inclusion criteria of the study and consequently, there is a possibility that the sample of participants in the study did not accurately represent the total population.

The researcher was unwilling to comment on the possible parenting styles of the participants interviewed due to the lack of collateral information, limited interview time (one face-to-face session), and the researcher's inability to provide an objective perspective due to the nature of the researcher's role during the qualitative research process. Identifying the parenting styles of participants would have added a layer of perspective to the descriptive and interpretive process. This is a limitation, however, the parental styles of participants was not an objective of the study, it would have informed an aspect of the second objective of identifying mediation techniques used by parents to manage their adolescent children's Internet use.

Research into the topic of cyber psychology is unpredictably complex as international research has been conducted into this field for more than a decade. However, due to the incredibly fast-paced growth and change of the Internet, research conducted ten years ago may be considerably outdated as the focus may have been on the use of outdated digital technology. The massive growth in popularity of social networking has presented many diverse research questions that are different from research conducted on Internet use before the creation of sites such as YouTube (2005), Instagram (2010), and Facebook (2004). Although some research remains very relevant, regardless of age, the rate at which the Internet and therefore, its users change, is seen as a limitation when searching for literature and information. Furthermore, journal articles are expensive due to a majority of the articles being controlled by large international publication companies. Most of these companies require payment for the researcher to access the article for a restricted period. With the exchange rate of the South African Rand the researcher found this a limitation to the access of certain peer-reviewed articles.

8. Recommendations

To the researcher's knowledge, this study is one of the few studies focussing on parental perceptions of Internet use in South Africa. From the initial proposal of this research topic, the researcher aimed at conducting a broad research study that would highlight areas of need or interest for future research. This research study can be replicated in different contexts, with varied samples of participants to produce findings that may be more generalizable to the South African population. By including a measure of parenting styles, the understanding of parental mediation techniques may be improved.

It is recommended that future research studies include the perceptions of the adolescent users of the Internet in order to integrate the findings from the parents' perceptions with that of adolescents Internet users. This will allow for the identification of discrepancies between the reports of parents and adolescents with regards to Internet use, experiences, and management. Furthermore, the researcher recommends research specifically aimed at exploring the possible effects of sleep disturbance due to the use of social networking or the Internet, and how this may impact upon adolescent mood regulation and academic performance.

Education of parents regarding the Internet is of utmost importance. Caskey (2003) reported that parents who previously reported apprehension about their ability to monitor and mediate the adolescent children's Internet use and who have negative attitudes towards technology and the Internet found that with exposure to, and involvement with, education programmes developed for parents, benefited from interaction with their children and had a more positive perception of the Internet. Therefore, the researcher's final recommendation is the development of a psychoeducation program aimed at providing information to parents and adolescents, relevant to a South African context and focussing on cyber citizenship and the consequences of risky online behaviour. The researcher recommends workshops of smaller groups of individuals, developed in an interactive manner.

9. Conclusions

The study attempted to provide a rich, descriptive interpretation of parents' perceptions of their adolescent children's Internet use. This qualitative, exploratory, descriptive study incorporated an interpretive paradigm and made use of snowball sampling. Data was gathered using face-to-face, semi-structured interviews and analysed using Tesch's (1990) eight steps of qualitative data analysis.

The aim of this study was to explore and describe parents' perceptions of their children's Internet use to gain insight and understanding of how parents perceive the Internet including the benefits, risks, and dangers. Further, the aim was to identify mediation techniques used by parents to manage their adolescent children's Internet use. Themes that emerged from the data analysis included parental perceptions,

observations, parenting methods, concern, and opinions, and provided valuable insight into how parents perceive their adolescent children's Internet use and how they manage and mediate their children's Internet access.

With the study, it was the researcher's intention to tell the stories of the participants, allowing their voices to be heard in a scientific context, integrated with contributions from other users and researchers of the Internet. Although this present study does have its limitations, it is the goal of the researcher to use the findings to inform educational needs and develop psychoeducation programmes that may assist parents and children to become productive cyber citizens.

10. References

- Aldrich, R. (2013). Neuroscience, education and the evolution of the human brain. *History of Education*, 42(3), 396-410.
- Carr, N. (2010). *The Shallows. What the Internet is doing to our brains*. New York, N.Y: W.W. Norton & Company.
- Caskey, M. (2003). Using Parent-Student Pairs for Internet Instructions. *Journal of Research on Technology in Education*, 34(3), 304-317
- Erikson, E. H. (1968). *Identity, youth and crisis*. New York, N.Y: Norton.
- Festinger, L. (1954). A theory of social comparison processes. *Human Relations*, (7), 117-140. doi:10.1177/001872675400700202
- Hawking, S. (2016). Stephen Hawking. Retrieved May 10, 2016, from <http://www.hawking.org.uk/>
- Internet World Stats. (2015, November 30). Internet Usage Statistics for Africa (Africa Internet Usage and 2015 Population Stats). Retrieved March 15, 2016, from <http://www.Internetworldstats.com/stats1.htm>
- Johnston, K. (2013). A guide to educating different generations in South Africa. *Issues in Informing Sciences and Information Technology*, 10, 261-273. Retrieved March 12, 2016.
- Juvonen, J., & Gross, E. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health*, 78(9), 496-505.
- Kowalski, R., Limber, S., & Agatston, P. (2008). *Cyber bullying*. Massachusetts: Blackwell Publishing.
- Liau, A., Khoo, A., & Ang, P. (2008). Parental Awareness and Monitoring of Adolescent Internet Use. *Current Psychology*, 27, 217-233. doi:10.1007/s12144-008-9038-6
- Lund Research Ltd. (2012). Purposive sampling. Retrieved August 5, 2015, from

<http://dissertation.laerd.com/purposive-sampling.php>

Park, S., Kim, J., & Cho, C. (2008). Prevalence of Internet Addiction and Correlations with Family Factors among South Korean Adolescents. *Adolescence*, 43(172), 895-904.

Schmidt, E. (n.d.). Quotes about Internet. Retrieved April 10, 2016, from <http://www.goodreads.com/quotes/tag/Internet>

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. *New Media & Society*, 17(5), 649-665. doi:10.1177/1461444813516833

Sullivan, B. (2006, August 9). *Cyber bullying newest threat to kids*. Retrieved 22 May 2012 <http://www.msnbc.msn.com/id/14272228/>

SurveyCompare (2014). The Internet: South Africa vs. The Rest of the World [Infographic]. Retrieved July 5, 2015, from <http://www.surveycmpare.co.za/blog/Internet-south-africa-vs-rest-world-infographic>

Tesch, R. (1990). *Qualitative Research: Analysis Types and Software Tools*. London, England: Farmer Press.

Thinyane, H. (2010). Are digital natives a world wide phenomenon? An investigation into South African first year student's use and experience with technology. *Computers & Education*, 55(1), 406-414.

Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. *Qualitative Inquiry*, 16(10), 837-851. Retrieved August 30, 2015.

Tracy, S.J. (2013). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. West Sussex, U.K: Wiley-Blackwell

Unicef New York. (2012). *South African mobile generation*. Retrieved 22 September 2013 website: http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf

Zimbardo, P. G. (2008). *The Lucifer Effect: Understanding how good people turn evil*. New York, N.Y: Random House Trade.

The role of social media in coping with relationship dissolution

Ms. T. Lambert, Mrs. E. Cothill and Prof. G. Howcroft

Department of Psychology, Nelson Mandela Metropolitan University,
PO Box 77 000, Port Elizabeth, 6031.

e-mail: tania.lambert@nmmu.ac.za

Abstract

Individuals utilise social networking sites (SNSs) such as Facebook and twitter to communicate with romantic partners and maintain relationships. SNSs also enable users to gain a better understanding of the self, develop meaningful relationships with others, share personal experiences, and utilise SNSs as a means of social support. Making use of social media could therefore also play a role in coping with relationship dissolution. The aim of the present study was to create a rich description of the role of social media in coping with relationship dissolution. The study was both qualitative and phenomenological and participants were purposively sampled. Unstructured, in-depth interviews were used to collect the data which was thematically analysed. Many polarities were found regarding the role of social media in coping with relationship dissolution. Specifically, social media was found to be both advantageous and disadvantageous in coping with relationship dissolution

Keywords

Coping, relationship dissolution, social networking sites

1. Introduction

Romantic relationships can have powerful effects on individuals' psychological and physical well-being. The termination of romantic relationships, in particular, may be associated with various negative effects (Rhoades, Kamp Dush, Atkins, Stanley & Markman, 2011). What individuals do in order to manage and cope with the distress and changes brought on by relationship dissolution was a broader focus of this study. More specifically, the authors were interested in better understanding how individuals make use of social media and social networking in order to cope with relationship dissolution.

In recent years, using social networking sites (SNSs), such as Facebook, MySpace and Twitter, have become a daily occurrence. According to previous research, SNSs play a significant role in coping in general and, more specifically, in relationship

dissolution (Bevan, Pfyl & Barclay, 2012; Marshall, 2012; Pennington, 2013; Sauti, 2012; Tong, 2013). It is therefore likely that individuals who have experienced relationship dissolution may utilise SNSs to better cope with the effects of relationship dissolution. To the authors' knowledge, no other research to date has specifically explored this phenomenon, making the present research important in its contribution to the understanding of how social media can aid or hamper coping behaviour for individuals who have experienced relationship dissolution.

The Stress and Coping Theory

According to the Stress and Coping Theory (the primary theoretical framework of the present study), stress is a mutually reciprocal relationship between the individual and the environment (Folkman, Lazarus, Gruen & DeLongis, 1986), characterised by a subjective appraisal of it taxing and exceeding the individual's resources (Lazarus & Folkman, 1984). The process of coping involves two functions: dealing with the problem when the situation can be changed (problem-focused coping), and regulating emotion when the situation cannot be changed (emotion-focused coping) (Folkman et al., 1986; Lazarus, 1993; Lazarus & Folkman, 1984). Both problem and emotion-focused coping are typically used in any given stressful encounter (Folkman et al., 1986; Lazarus & Folkman, 1984). However, when considering a stressful situation that extends over a longer period of time, coping may occur sequentially where emotion-focussed coping occurs immediately after the event and is then gradually replaced with more problem-focussed strategies (Lazarus & Folkman, 1984). In terms of the present study, relationship dissolution can be explained as the stressful relationship between the individual and the environment which is appraised as both taxing and posing a threat to the individual's well-being. A reaction to this stressful situation is mediated by cognitive appraisal and therefore a coping option is selected in order to manage the situation. This process results in change – either change in the romantic relationship dissolution (problem-focussed coping) or change in the appraisal of the romantic relationship dissolution (emotion-focussed coping).

The online self

In order to appreciate coping in the context of an online environment, it is important to distinguish between the online self and the offline self. The online self consists of multiple selves in potentially numerous SNSs, constructed in order to project a new sense of self (cyber-self) to the online community, freed from 'offline' social norms and expectations (Robinson, 2007). The cyber-self is regarded as both the subject and the object of interaction with the generalised other (the perceived or imagined audience when using SNSs) (Robinson). Identity construction and impression management are therefore also important when constructing the cyber-self (Pempek, Yermolayeva & Calvert, 2009). In choosing how to manage the generalised audience's impression, users are more likely to disclose positive experiences on SNSs, in order to create a better impression of their emotional well-being (Qiu, Lin, Leung, & Tov, 2012; Wilson, Gosling & Graham, 2012). These factors have significant implications for the way individuals affected by relationship dissolution

may use SNSs. For example, with the ex-partner in mind as the imagined audience, the individual may update their profile picture in such a way as to create the impression that he/she is coping well with relationship dissolution.

Literature review

There has been little research focus on the use of SNSs in coping with relationship dissolution; however previous research suggests that SNS usage may assist in coping when a loved one has passed on (Pennington, 2013). Other research indicates that motivating factors for using SNSs also have an effect on stress and general well-being (Teppers, Luycx, Klimstra, & Goossens, 2013; Tong, 2013; Wilson et al., 2012; Wright, 2012). However, these factors only imply their usefulness with regards to coping in general. Such implications are also demonstrated in research that suggests how SNSs might be specifically useful in coping with relationship dissolution. For example, surveillance and information-seeking behaviours related to the ex-partner may decrease feelings of attraction and longing for the ex-partner (Marshall, 2012) which could assist in overall coping. Furthermore, research indicates that some individuals choose to cut all ties with an ex-partner on SNSs during and after a breakup (Tong), and it is possible that ‘unfriending’ or deleting an ex-partner off SNSs may be a way for the individual to engage in avoidance coping, as the ultimate act of severing ties and finding closure (Bevan, Ang & Fearn, 2014). ‘Unfriending’ may also have implications for impression management and constructing the desired identity after relationship dissolution, such as by changing the relationship status on Facebook to inform the imagined audience. However, revealing or finding this type of information in such a public manner may lead to public scrutiny, jealousy and suspicion (Fox, Osborn & Warber, 2014; Marshall, Benjanyan & Di Castro, 2013).

2. Research Aim

The aim of the present study was to create a rich description of the role of social media in coping with relationship dissolution.

3. Research Methods

In order to gain a comprehensive understanding of the role of social media in coping with romantic relationship dissolution, a qualitative research approach was chosen. More specifically, an interpretive phenomenological design was employed in order to collect and analyse the data so that participants’ subjective, lived experiences of the role of social media in coping with relationship dissolution could be described. Using this approach resulted in the findings about the essence of the phenomenon, which was translated into rich descriptions of the phenomenon.

Participants

Participants were obtained by means of purposive sampling and were recruited by an advertisement placed in a local newspaper. Inclusion criteria were that participants

must be 18 years or older; and they must have experienced the dissolution of a romantic relationship, caused by either themselves or their partner, in the last 12 months. Since the interviews were face to face interviews, the participants had to reside within the local metro pole.

Instruments

Data was obtained through individual, in-depth, unstructured interviews in order to allow participants to describe their subjective, lived experience of the phenomena being studied (Englander, 2012). This is in line with the phenomenological nature of the study.

Procedure

Once inclusion criteria were verified, suitable participants were given an information letter informing them of the nature of the study, confidentiality issues and other issues pertaining to the research. Thereafter, an interview date and time was established with each participant. At the outset of each interview, a biographical questionnaire and consent form was completed by participants. After establishing rapport with the participants, an initial open-ended phrase was posed. The researcher thereafter probed in order to elicit specific descriptions of the experiences mentioned. The interviews were recorded using an audio recording device. Once the interviews were completed and data saturation reached, the recordings were transcribed verbatim by an independent transcriber. The transcribed interviews were then analysed according to phenomenological principles. Specifically, the method of thematic data analysis was utilised. Upon completion of the research study, each participant received a summary of the findings.

Data analysis

Once the data was collected from the interviewing process and transcribed verbatim, Braun and Clarke's (2006) method of thematic data analysis was used to categorise the data into codes and themes. Thematic analysis is a method utilised in order to identify, analyse and report themes within data (Braun & Clarke). In the present research, the phenomenon that was focussed on was the role of social media in coping with relationship dissolution. The aim of data analysis was to provide rich descriptions of the participants' subjective, lived experiences of this phenomenon. Six phases of thematic analysis were followed: becoming familiar with the data, generating the initial codes, collating different codes into potential themes or patterns, reviewing these themes, clearly defining and naming the various themes, and producing a report of the analysis. Vivid and compelling extract examples were selected and analysed, and the analysis was related back to the research question and literature (Braun & Clarke).

Ethical considerations

Ethical principles employed in the research included the following: institutional approval from the relevant tertiary institution, maintaining researcher integrity and competence, ensuring the exclusion of researcher bias, trustworthiness of analysis and findings, informed consent, confidentiality, and ethical dissemination of results.

4. Findings and Discussion

Two prominent main themes emerged from the data: advantages of social media use in coping with relationship dissolution and the disadvantages of social media use in coping with relationship dissolution. These themes and their subthemes were based on all participants' statements. Each of these themes and their corresponding subthemes will be discussed below.

4.1.1. Advantages of social media use.

A major theme that emerged was the advantages of using SNSs in coping with relationship dissolution. Within this theme the following five subthemes were identified: the role of social media in providing social support; social media as a source of comfort and inspiration; the role of impression management in coping with relationship dissolution; the role of social media as a distraction tool; and SNSs' usefulness in the short term.

The role of social media in providing social support. Participants reported that the use of SNSs enhanced existing offline relationships and social support. For example, Participant 1 reported that: *"Instead of phoning your parents or your sister to cope... you will post it on Facebook"* This finding was consistent with research studies emphasising the role of SNS's in providing social support (Nabi, Prestin & So, 2013; Wright, 2012). Participants also found that, by being able to see what is happening in others' lives, Facebook use can increase connectedness to friends which may, in turn, increase perceptions of social support. This subtheme finding is in accordance with research by Nabi et al. that suggests that the public nature of social media (particularly Facebook) is related to perceived social support. This finding would also reflect the emotion-focussed coping strategy of emotional social support (Lazarus & Folkman, 1984).

Social media as a source of comfort and inspiration. Related to social support, participants experienced Facebook as a source of comfort and inspiration, especially as a result of seeing others experiencing similar situations. As an example of this, Participant 1 stated:

Where positive quotes... you know it doesn't necessarily have to be their quotes but like there are positive quotes that people put on Facebook... You know like, if anyone's going through a tough time they put positive quotes and you look at it and you think, 'oh okay, you know, I've gone through such a situation,' and ja... that helped me cope.

This finding is consistent with that of Sauti (2012) who suggests that merely returning to using SNSs after a breakup may result in a sense of comfort and healing. Sharing an experience such as relationship dissolution with someone who is going through a similar situation can also result in perceptions of emotional support (Wright, 2012).

The role of impression management in coping with relationship dissolution. Another form of emotional coping was the creating of a positive online self. More specifically, posting positive images of oneself may enhance well-being. Participant 3 states in this regard:

So if you are like ja I'm feeling good so I'm going to post a good picture of myself or whatever like it does help to ... um ... feel better about yourself [okay] rather than be like oh poor me, you know?"

It can be seen that impression management of the user's online profile in this way (i.e., portraying a positive image) may be specifically geared towards lessening the emotional distress associated with the relationship dissolution, without altering its meaning (Folkman & Lazarus, 1984). Instead, Participant 3 positively reappraised the meaning associated with her profile, by posting positive images of herself. This, in turn, had a positive emotional effect on her well-being, which makes this a type of adaptive coping.

The role of social media as a distraction tool. SNSs, specifically Facebook, were also found to be a good distraction tool in coping with relationship dissolution. For instance, Participant 3 stated: *"What it does to you is it does help you to get your mind off thingsit can be a way of getting your mind shifting your focus onto something else."* This is related to avoidance and emotion-focussed coping where emotions are regulated when the situation cannot be changed (Lazarus & Folkman, 1984). Furthermore, participants regarded Facebook use as an emotional outlet for emotions experienced as a result of the relationship dissolution, and as a way to indirectly address the ex-partner as illustrated by a comment of Participant 4: *"I would go on Facebook type of thing... send statuses like 'I miss you' ... not directly to her but just as a status."*

SNSs usefulness in the short term. Although still considered emotion-focussed coping strategies by Lazarus (1993) expressing emotion and indirectly communicating with the ex-partner may be helpful, especially in the short-term. Such implications are also demonstrated in this subtheme, that using social media in general may be helpful in the short-term. For example, Participant 3 stated: *"I think it's a short-term coping mechanism... it helps you to cope now or whatever... it's like 'okay cool I feel better about me."* According to two participants, Facebook offered a unique connection with the ex-partner. Marshall et al. (2013) suggest that remaining in contact with an ex-partner may result in a sense of satisfaction and connection with the ex-partner which could be beneficial in the short term. This may be part of a reappraisal process where emotion-focussed coping strategies are used.

4.1.2. Disadvantages of social media use

Participants also found that there were disadvantages to using SNSs during and after relationship dissolution. Within this second major theme the following two subthemes were identified: social media use interferes with moving on and the negative effects of personal disclosure on Facebook.

Social media use interferes with moving on. Participants found that the use of SNSs interferes with moving on and letting go of a relationship mainly due to surveillance of the ex-partner's social media profiles. The following extract from Participant 4 demonstrates this notion: *"I just found myself going on a – on her BBM profile picture or statuses on WhatsApp and Facebook to see how she is doing and all that."* Online stalking or lurking behaviour is not unusual for SNS users, and may be found in users who are affected by relationship dissolution, especially since such behaviour helps fill the void left by the ex-partner (Darvell, Walsh, & White 2011; Tong, 2013). However, online surveillance behaviour of an ex-partner after a breakup may lead to increased levels of distress and negative emotions such as sadness, hurt, frustration, false hope, increased loneliness and being apprehensive (Darvell et al; Tong). These findings further relate to literature suggesting that surveillance behaviour may be associated with jealousy (Marshall et al., 2013), sadness, hurt and frustration (Tong) and increased loneliness (Wilson et al., 2012). Furthermore, Facebook use may prevent individuals from moving on and having a clean break after relationship dissolution, possibly due to online reminders of the ex-partner (such as photos and status updates). According to Marshall (2012) and Tong, staying connected with an ex-partner on SNS may be negatively associated with personal growth.

Another factor that prevented participants from moving on was their awareness that their ex-partners could see their updates. Participants consequently adjusted their online behaviour by keeping the ex-partner in mind. Participant 2 stated in this regard:

Like I will update my WhatsApp more than I update my Facebook. Because I suppose I know that he can see what's happening on my WhatsApp...well just I change it more frequently because I kind of want him to directly see that.

By means of impression management, a SNS user therefore constructs a new online identity that is in line with the imagined expectations the user perceives someone else to have when looking at their profile (Robinson).

Related to the impression management that SNS users may engage in in order to attract the ex-partner's attention is the fact that users mostly seek to create a positive impression. This can be done by posting pictures and status updates that portray a positive and happy image of the self. Participants in the present study had some awareness of constructing a positive online identity, as can be seen by the following comment from Participant 1: *"Just to let them know that I'm doing alright and coping."* This is consistent with findings that users are more likely to disclose

positive experiences on their SNSs in order to create a good impression of their emotional well-being (Qiu et al., 2012; Wilson et al., 2012).

Negative effects of personal disclosure on Facebook. Participants found that personal disclosure on a specific SNS, namely Facebook, was negative mainly due to the public nature of the platform lending itself to creating a certain impression of the Facebook user. Since positive online impression seems to be of importance to SNS users (Qiu et al., 2012; Wilson et al., 2012), disclosing negative information on Facebook, such as information regarding relationship dissolution, may result in a negative impression. According to the participants in the present study Facebook is not to be used to disclose personal aspects of relationship dissolution publically as suggested by the comment of Participant 3:

You have to realise that, like so whatever you're posting on Facebook is seen by, you know 800 people, or however many friends you have... you are publicly telling everyone... and that does have repercussions on the way that people think of you and your public image..

In line with this finding, Fox et al. (2014) suggest that information on SNSs after relationship dissolution may lead to public scrutiny and aggravated distress.

Facebook may restrict seeking offline social contact. As much as SNSs use may enhance offline relationships, the use of Facebook seems to prevent individuals from seeking this social support as illustrated in the comment of Participant 2:

If Facebook wasn't there maybe then it would have forced me to like go and spend time with my friends or something... which would probably been better, because I was just sitting by myself... and just being sad and lonely.

A possible reason for not seeking offline social support might be the illusion of SNSs providing support or sense of contact. Participant 2 later alluded:

So Facebook was just one thing that I could do and it kind of gives the illusion of social contact I suppose... which is what I was wanting... but it's still an illusion of a connection because it's not the real person... it's not as strong a connection.

5. Conclusion

Many polarities exist regarding the role of social media in coping with relationship dissolution. SNS use is both complex and ambiguous. For example, in the present study participants were in agreement that SNSs provide perceived social support. However, it was also reported that SNSs inhibited participants from seeking offline support. Another example of ambiguity relates to the ex-partner's use of SNSs. Participants valued the sense of connectedness that Facebook provides, but at the

same time felt that it prevented them from moving on and letting go. Both these examples could relate to the timeframe post relationship dissolution when using SNSs. The present results suggest that using SNSs as a coping strategy is more adaptive in the short-term, but that it may result in maladaptive coping in the long-term. Finally, based on the findings related to the role of social media in offering emotion-focussed coping strategies, it emerged that it is possible that problem-focussed coping strategies can be beneficial in terms of social media use and coping with relationship dissolution. Future research may allow for a better understanding of how helpful problem-focussed coping strategies are in using social media after relationship dissolution.

6. References

- Bevan, J. L., Ang, P. & Fearn, J. B. (2014). Being unfriended on Facebook: An application of expectancy violation theory. *Computers in Human Behavior*, 33, 171–178.
- Bevan, J. L., Pfyl, J. & Barclay, B. (2012). Negative emotional and cognitive responses to being unfriended on Facebook: An exploratory study. *Computers in Human Behavior*, 28, 1458–1464.
- Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77-101.
- Darvell, M. J., Walsh, S. P. & White, K. M. (2011). Facebook tells me so: Applying the theory of planned behavior to understand partner-monitoring behavior on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 717-722.
- Englander, M. (2012). The interview: Data collection in descriptive phenomenological human scientific research. *Phenomenological Psychology*, 43, 13–35.
- Folkman, S., Lazarus, R. S., Gruen, R. J. & DeLongis, A. (1986). Appraisal, coping, health status, and psychological symptoms. *Personality and Social Psychology*, 50(3), 571-579.
- Fox, J., Osborn, J. L. & Warber, K. M. (2014). Relational dialectics and social networking sites: The role of Facebook in romantic relationship escalation, maintenance, conflict, and dissolution. *Computers in Human Behavior*, 35, 527–534.
- Lazarus, R. S. (1993). From psychological stress to the emotions: A history of changing outlooks. *Annual Reviews Inc.*, 1-21.
- Lazarus, R. S. & Folkman, S. (1984). *Stress, appraisal and coping*. New York, NY: Springer .

- Marshall, T. C. (2012). Facebook surveillance of former romantic partners: Associations with post-breakup recovery and personal growth. *Cyberpsychology, Behavior, and Social Networking*, 15(10), 521-526.
- Marshall, T. C., Benjanyan, K. & Di Castro, G. (2013). Attachment styles as predictors of Facebook-related jealousy and surveillance in romantic relationships. *Personal Relationships*, 20, 1-22.
- Nabi, R. L., Prestin, A. & So, J. (2013). Facebook friends with (health) benefits? Exploring social network site use and perceptions of social support, stress, and well-being. *Cyberpsychology, Behaviour, and Social Networking*, 16(10), 721-727.
- Pempek, T. A., Yermolayeva, Y. A. & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, 30, 227-238.
- Pennington, N. (2013). You don't de-friend the dead: An analysis of grief communication by college students through Facebook profiles. *Death Studies*, 37, 617-635.
- Qiu, L., Lin, H., Leung, A. K. & Tov, W. (2012). Putting their best foot forward: Emotional disclosure on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 15(10), 569-572.
- Rhoades, G. K., Kamp Dush, C. M., Atkins, D. C., Stanley, S. M. & Markman, H. J. (2011). Breaking up is hard to do: The impact of unmarried relationship dissolution on mental health and life satisfaction. *Family Psychology*, 25(3), 366-374.
- Robinson, L. (2007). The cyberself: the self-ing project goes online, symbolic interaction in the digital age. *New Media & Society*, 9(1), 93-110.
- Sauti, G. (2012). *Anthropology in the digital age: An analysis of social interaction on networking sites* Unpublished doctoral thesis,. University of the Witwatersrand, Johannesburg, South Africa.
- Teppers, E., Luyckx, K., Klimstra, T. A. & Goossens, L. (2013). Loneliness and Facebook motives in adolescence: A longitudinal inquiry into directionality of effect. *Journal of Adolescence*, 1-9.
- Tong, S. T. (2013). Facebook use during relationship termination: Uncertainty reduction and surveillance. *Cyberpsychology, Behavior, and Social Networking*, 16(11), 788-793.

- Wilson, R. E., Gosling, S. D. & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science*, 7, 203.
- Wright, K. B. (2012). Emotional support and perceived stress among college students using Facebook.com: An exploration of the relationship between source perceptions and emotional support. *Communication Research Reports*, 29(3), 175–184.

Personality Traits and Self-Presentation on Facebook: A Systematic Review

D.Y. Venter, G. Howcroft, T. Lambert

Department of Psychology, Nelson Mandela Metropolitan University, Port Elizabeth,
South Africa
e-mail: dyventer@gmail.com

Abstract

The influence of the Internet and Computer Mediated Communication (CMC) on the ways in which individuals with different personality traits present themselves, has been brought into question increasingly as modern life requires more and more of an enmeshment with technology in everyday life. The presentation of the self on Facebook has been the focus of recent research, delivering results that vary and sometimes contradict common ideas of the effects of individuals' interaction via technology, especially in terms of how personality traits, as determined by the Five-factor model, impact upon self-presentation. A systematic review of the available literature was conducted, in order to bring about a consolidated description of the literature on the impact of personality traits on Facebook self-presentation. From 37 studies, the review found the motivation for Facebook use to be a mediating factor in the relationship between personality traits. Each personality trait in the Five-factor model impacts upon Facebook use, self-generated content, other-generated content, and the nature of the individual's self-disclosure in varied ways. Due to visible cues on users' profiles, some personality traits can be accurately detected by observers. The complexity and interrelatedness of variables involved in this relationship is highlighted by the findings of this review.

Keywords

Computer-mediated communication, dramaturgical theory of interaction, Facebook, five factor model of personality, image-management, online interaction, personality traits, self-presentation, Social networking sites.

1. Introduction

Computer Mediated Communication appears to be enmeshed with modern daily living and this brings into question how individuals make use of the tools used for communication and self-presentation purposes. The recent research that has as its focus the self-presentation of individuals in terms of their personality traits, considers a variety of variables involved and delivers conflicting results.

Current research on the topic involves quantitative as well as qualitative studies on the phenomena evident in online interaction, as well as the impact thereof upon image-management (Lang 2012; Lee et al. 2014; Robinson 2007; Rui & Stefanone 2013). Many of these studies focus on self-presentation on specific Social

Networking Sites (SNS) such as Facebook (e.g., Amichai-Hamburger & Vinitzsky, 2010; Gosling, et al., 2011; Mehdizadeh, 2010; Moore & McElroy, 2012; Ong, et al., 2011; Ross, et al., 2009). Self-presentation, specifically on Facebook, has been studied from various perspectives and was found to be impacted upon by the personality traits of the individuals who make use of the social networking site. The current body of knowledge does not give a conclusive account of this relationship, due to its vast and broad nature. To improve the understanding of the interaction between the variables involved, the present review aimed to explore and describe personality traits and self-presentation on Facebook, by making use of a systematic review of the studies available at present.

Personality Traits were conceptualised in this review by making use of the Five-Factor model, including the five main personality traits: Neuroticism (N), Extraversion (E), Openness to Experience (O), Agreeableness (A), and Conscientiousness (C) (Costa & McCrae 2010). These traits have been found to have significant relationships with certain variables in relation to Self-presentation. This concept is described by Goffman's Dramaturgical model as an act within which a performer makes use of interactional tools at his disposal to create a representation of himself for his audience to respond to (Goffman 1990). Facebook may be considered to be one such an interactional tool. This cyber environment provides a new setting for interaction, and so self-presentation, to take place. With a new setting, new perspectives may be formed in terms of dynamics and methods for self-presentation. The particular characteristics of the environment may play a role when users choose how they wish to present themselves, and may also have an unconscious effect on how representations are perceived by other users.

However, as with face-to-face interaction, motivation for self-presentation and methods used to represent the self can be impacted upon by an individual's personality (Goffman 1990). Due to the complex interaction between specific variables, and the fact that different personality traits impact upon these variables in different ways, a systematic approach had to be adhered to.

2. Methodology

The research design chosen was a systematic review to answer the research question: How does personality impact upon the self-presentation of individuals on Facebook? Sub questions were included for each of the five personality traits included in the study. An initial database search based on relevant keywords delivered 469 records on 7 August 2015. Databases that were searched on the EBSCOHost online referencing system included Academic Search Complete, Communication and Mass Media Complete, MasterFile Premier, PsychInfo, as well as the EBSCOHost eBook Collection and E-Journals section. Furthermore, additional resources were found by searching the following databases: Taylor & Francis Online, ScienceDirect, and SAGE. By screening and checking for eligibility by inclusion criteria, the sample that was reviewed consisted of 37 studies. Accepted studies were required to include content on self-presentation in relation to the Five-factor model of personality traits in the context of Facebook only. No other personality traits or social media platforms were included. Both quantitative and qualitative studies were accepted into the

review, as well as available reviews. A strictly systematic approach was followed in order to ensure the usefulness of the presentation of the data (Wardlaw 2010). The process followed guidelines suggested by Hemingway and Brereton (2009) and required of the data to be extracted and assessed, after which the results were combined and thematic analysis was utilised to describe current available knowledge. The results were then placed into context to describe the impact of each of the personality traits on the self-presentation of individuals on Facebook, before conclusions could be drawn to address the main research question:

How do personality traits impact upon the way in which individuals self-present on Facebook?

Due to the specific inclusion criteria which was applied to all of the results in this review, all 37 articles contain relevant data regarding the main aim of the review, that is, to explore and describe how personality traits impact upon the way in which individuals self-present on Facebook by means of a systematic review. To address the sub-objectives, studies were grouped into categories (Petticrew & Roberts 2006), and so each personality trait was considered separately. All but one of the included articles provided data on Extraversion (n=36). The majority of the included articles provided data on Neuroticism (n=34), and Agreeableness (n=35). Fewer of the articles provided data on Openness to Experience (n=20) and Conscientiousness (n=19). All the articles were published in English between 2008 and 2015. Quantitative studies (n=32) and Qualitative studies (n=3) were included, as well as reviews (n=2).

3. Findings

Emergent themes from the review gave an indication of the intricacies and complexities that are implicit in the interaction between variables involved in Facebook self-presentation. These included the motivations for why individuals may use Facebook, how frequently and much how they use Facebook, and the content that is published on Facebook by users and their contacts. The nature of self-disclosure was also considered, as well as the accuracy with which a user's audience could detect their personality traits by use of only Facebook content. The findings that follow are addressed for each of these themes, with specific mention of the Five-factor personality traits.

3.1 Motivation for Facebook use

The motivations that guide the use of Facebook appear to impact upon individuals' self-presentation, while personality traits have both a direct and indirect influence, as suggested by Figure 1.

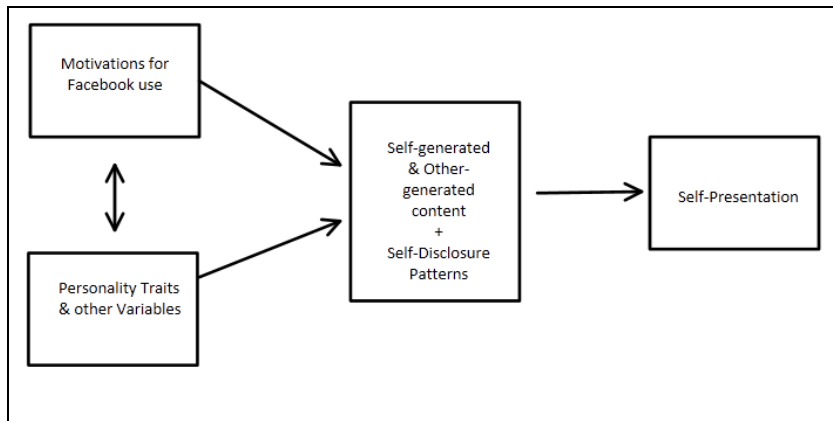


Figure 1 – Mediating effect of the Motivations for Facebook use

Table 1 represents the findings of the review in terms of the motivations for Facebook use and how personality traits play a role in this interaction. Those higher in Neuroticism appeared to make use of Facebook for self-presentational purposes (Błachnio et al. 2013; Ross et al. 2009; Seidman 2013) among 97 students in Southwestern Ontario, as well as meeting the need for belongingness in a study of 301 individuals (Hollenbaugh & Ferris 2015). The upward arrow in the table indicates the positive relationship between the trait of Neuroticism and the Need for self-presentation, while a downward arrow represents a negative relationship between traits. For the trait of Extraversion, those with higher levels were found to engage in self-exploratory and communicative behaviours online, motivated by both the need to self-present and the need for belongingness (Michikyan et al. 2014; Seidman 2013). However, the reasons why more introverted or extraverted individuals use Facebook gave rise to a zero correlation found in relation to using Facebook for socialization purposes in a sample of 804 Facebook users (Bodroža & Jovanović 2015). They suggest that more introverted individuals may use Facebook because it feels safer than intense social situations, while extraverted individuals may be motivated to meet new people and socialize.

	N	E	O	A	C
Need for Self-presentation	↑	↑	↑	↑	↓
Need for Belongingness	↑	↑↓	↓	↑	↓

Table 1: Relationship between personality traits and Motivations for Facebook use

Openness to Experience was indicative of self-presentational uses of Facebook in 233 undergraduate students (McKinney et al. 2012). Interestingly, a common motivation for those higher in Openness to Experience to use Facebook was to play online games (Wang et al. 2012) , and to experiment with identities online (Bodroža

& Jovanović 2015). Self-presentation as well as the need to belong (shown in behaviours of communication, acceptance-seeking, and connection maintenance) were positively related to higher Agreeableness in 254 college students in South California and New England (Sun & Wu 2012). Higher Agreeableness was found to be unrelated to motives of information-seeking on Facebook, as indicated by the 0 in table 2. Conscientiousness however, was negatively correlated to the use of Facebook for the purposes of self-presentation and attention-seeking, indicating that those with lower levels of this trait are more likely to make use of Facebook for

	N	E	O	A	C
Facebook Use	↑	↑	↑0	↑	0
Time spent on Facebook	↑0	0	-	-	0
Number of Facebook Friends	0	↑	-	0	↑↓

meeting these needs (Błachnio et al. 2013; Seidman 2013).

Table 2: Relationship between personality traits and aspects of Facebook use

3.2 Facebook use

The frequency and intensity of Facebook use is considered when individuals' self-presentation is explored. Personality traits appear to impact upon how often individuals use Facebook, as well as the time spent using Facebook. Furthermore, the size of a user's Facebook friend network is another variable that can be impacted upon by personality, and in turn impacts upon self-presentation.

For Neuroticism, Extraversion, Openness to Experience, and Agreeableness, higher levels are associated with higher Facebook use. Mixed results were found for the relationship between Neuroticism and actual time spent on Facebook. Motivation for Facebook use is offered as a mediating factor, as is the mobile accessibility of Facebook. No significant relationship was found between Neuroticism and the number of Friends an individual might have on Facebook (Nadkarni & Hofmann 2012; Moore & McElroy 2012; Michikyan et al. 2014). This is very different for the trait of Extraversion, which is positively related to the number of Facebook friends. Higher degrees of Extraversion are also related to high Facebook use, however it is not related to time spent on Facebook, suggesting that more extraverted individuals perform goal-orientated activities on Facebook as opposed to browsing (Błachnio et

al. 2013; Nadkarni & Hofmann 2012; Walther et al. 2011; Eftekhar et al. 2014; Hall & Pennington 2013; Michikyan et al. 2014). Low conscientiousness was not found to correlate significantly to time spent on Facebook, or frequency of Facebook use. However, it was found to predict Facebook addiction due to the dynamics of self-presentation and poor self-discipline in these individuals. Conflicting results were obtained for the relationship between Conscientiousness and number of Facebook friends (Bodroža & Jovanović 2015; Walther et al. 2011; Moore & McElroy 2012; Wang et al. 2012; Hall & Pennington 2013).

3.3 Self-generated content

The content that is published by individuals on Facebook was scrutinized in terms of self-presentation in relation to the users’ personality traits. Content that is published by users onto the Facebook platform has been frequently studied, and the implications of a user's personality traits on the broadcasted content (status updates, posts), the directed content (Facebook *Wall*, private messages), and responses to others' content (comments, likes, shares) were noted.

For broadcasted content, users can select the type of content that can be published, for example, photos or status updates. The nuances that are present for different personality traits impacted upon the results of the review in a way that mixed results were found. For Neuroticism, Extraversion and Openness to experience, higher levels of the traits were related to more frequent status updates. For Conscientiousness, a negative relationship was found. More conscientious individuals were less likely to update their status, as well as send direct messages to others (Hall & Pennington 2013; Lee et al. 2014; McKinney et al. 2012; Wang et al. 2012).

	N	E	O	A	C
Broadcast content	↑0	↑0	↑	↓↑	↓↑
Directed content	↑	↓	-	-	↓
Responses to others’ content	↓	↓	↓	↑	↓

Table 2: Relationship between personality traits and Self-generated content

Extraversion was also found to negatively correlate with making use of directed content, while Neuroticism was positively associated with making use of the Facebook *wall* (Błachnio et al. 2013). All the traits save for Agreeableness were found to be negatively related to responding to others’ content in the form of *likes*, *comments* and *shares*. More agreeable individuals *comment* more frequently on others’ content (Lee et al. 2014; Amichai-Hamburger & Vinitzky 2010) More specific phenomena were noted in users’ content that were associated with specific personality traits. The use of laughter (e.g. Haha) in status updates was found to be positively related to Neuroticism, while the use of extended letters (e.g. Hiii) was

found to positively relate to Neuroticism and Extraversion. More extraverted individuals were also more likely to make use of positive affect, emoticons, and shorthand in status updates (Hall & Pennington 2013).

3.4 Other-generated content

Other-generated content was also considered as it gives information about the individual's audience and gives clues about how the self-presentation is received and responded to. The phenomenon of *lurking* was associated with those who have higher levels of Neuroticism and those who have lower levels of Extraversion, as indicated by their motivations to use Facebook. Those higher in Extraversion, got more likes and comments on their status updates, from a higher number of unique friends. Those with higher levels of Openness to experience also had more friends comment on their status updates. More conscientious individuals were associated with the receipt of more supportive comments, although a lower number of friends would comment on their status updates (Hall & Pennington 2013).

	N	E	O	A	C
<i>Lurking</i>	↑	↓	-	-	
Likes and Comments from friends	-	↑	-	↑	↓
Unique friends who comment/like		↑	↑	-	↓
Untagging				↓	↑

Table 3: Relationship between personality traits and Other-generated content

The way that individuals deal with undesirable photos on Facebook in which they are *tagged*, can be direct (eg. Discuss with posting user) or indirect (eg. Make use of *untagging* feature). More Conscientious individuals were more likely to *untag* themselves, avoiding conflict, while agreeableness was positively associated with more direct approaches to dealing with undesirable photos (Lang & Barton 2015).

3.5 Nature of self-disclosure

The amount, depth, breadth, intensity, intent, honesty and valence of an individual's self-disclosure was categorized together to describe the nature of self-disclosure in relation to self-presentation, answering the question of how individual's self-present. Individuals higher in the traits of Extraversion and Agreeableness were found to disclose more information on Facebook (Chen & Marcus 2012; Wang 2013).

	N	E	O	A	C
--	---	---	---	---	---

Amount	-	↑	0	0↑	0
Depth	↑	↑↓	↑	-	↓
Breadth					
Intensity	-	0	0	-	↑↓
Intent	0	-	↑	-	↑
Honesty	↑0	↑↓0	↑	-	↑
Valence	0	-	↑	-	↑

Table 4: Relationship between personality traits and Nature of self-disclosure

The depth of the self-disclosure refers to the intimacy of the content and this variable was found to positively correlate with Neuroticism and Openness to Experience, and negatively with Conscientiousness. For Extraversion, mixed results were found (Amichai-Hamburger & Vinitzky 2010; Moore & McElroy 2012) Openness to Experience relates positively to a greater variety of topics covered in the published content of individuals who have higher levels of this trait (Hollenbaugh & Ferris 2015).

3.6 Accuracy of personality trait detection

Lastly, the ability to accurately detect personality traits became an interesting factor that once again provided information about the point of view of the audience and how authentic and/or effective the self-presentation of a performer can be. For all but Neuroticism, users were able to successfully detect the personality traits in other users only by looking at an individual’s Facebook profile. Users make use of certain cues that are associated with each of the personality traits, and so make assumptions about the individual’s personality. For example, Extraversion is detected by depending on information about social interaction, attempts at humour, number of friends, and posting of pictures. For Neuroticism, however, users were least accurate at detecting the trait, possibly due to the undesirability of the trait, making it more likely to be hidden or presented less by individuals on social media (Marriott & Buchanan 2014).

	N	E	O	A	C
Accurate detection	N	Y	Y	Y	Y

Table 5: Detection of the personality trait from Facebook profile content

Furthermore, the review placed importance on attempts to understand the interrelatedness of the variables involved in this phenomenon, as well as the complex dynamics between very specific sub-variables that interact with one another. Aside from the motivations for Facebook use, among the mediating factors that were detected in the review were shyness, self-esteem, collectivistic self-construal, the predisposition to trust, attitudes about SNS, Narcissism, self-efficacy, and trait combinations in various ways.

4. Discussion and Recommendations

These findings place the results of the current available knowledge into context regarding the impact of personality on the self-presentation of individuals on Facebook. No such a review had been done at the time of writing. The review may be valuable in the development of an updated theory of self-presentation, and possible models specific to online self-presentation. This knowledge may assist in the field of Psychology, and not only guide and inform further research, but also hold utility value in terms of applications in the SNS environments in terms of security, moderation, policies and other progressive applications. Furthermore, interdisciplinary relationships with law, education, philosophy and information technology sectors may benefit from these findings in various ways.

However, while the application of this review is valuable in the current context of Cyberpsychology and other domains of research, limitations should be noted and further research considered. The review restricted the inclusion criteria by focussing only on the five personality traits of the Five-factor model of personality, and restricted the SNS to Facebook only. Therefore, other possibly significant factors, such as Narcissism or Machiavellianism or locus of control, have been neglected by this review. Further research into the impact of these and other personality traits is suggested, especially in the context of deviant behaviour or deceitful self-presentation on Facebook. Other significant SNSs are possible review opportunities as well, for which the present review suggests a useful design. Interested researchers are recommended to contribute to the development of a comprehensive model that includes more variables that impact upon self-presentation on Social Networking Sites.

Furthermore, the review did not take into account that individuals present with differing levels and combinations of the five personality traits included. Therefore, phenomena associated with personality profiles and certain trait combinations were referred to in this review only in a peripheral manner. Research that takes an in-depth phenomenological approach is suggested with regards to self-presentation on Facebook, to gain a richer understanding of users' experiences on Facebook.

5. References

- Amichai-Hamburger, Y. & Vinitzky, G., 2010. Social network use and personality. *Computers in Human Behavior*, 26(6), pp.1289–1295. Available at: <http://dx.doi.org/10.1016/j.chb.2010.03.018>.
- Błachnio, A., Przepiórka, A. & Rudnicka, P., 2013. Psychological determinants of using Facebook: A research review. *International Journal of Human-Computer Interaction*, 29(11), pp.775–787. Available at: <http://www.tandfonline.com/doi/abs/10.1080/10447318.2013.780868>.
- Bodroža, B. & Jovanović, T., 2015. Validation of the new scale for measuring behaviors of Facebook users: Psycho-Social Aspects of Facebook Use (PSAFU). *Computers in Human Behavior*, 54, pp.425–435. Available at: <http://www.sciencedirect.com/science/article/pii/S0747563215300431> [Accessed September 7, 2015].
- Chen, B. & Marcus, J., 2012. Students' self-presentation on Facebook: An examination of personality and self-construal factors. *Computers in Human Behavior*, 28(6), pp.2091–2099. Available at: <http://www.sciencedirect.com/science/article/pii/S074756321200163X> [Accessed January 10, 2015].
- Costa, P.T. & McCrae, R.R., 2010. *NEO Inventories for the NEO Personality Inventory-3 (NEO PI-3), NEO Five-Factor Inventory-3 (NEO-FFI-3) and NEO Personality Inventory-revised (NEO PI-R): Professional Manual.*,
- Eftekhari, A., Fullwood, C. & Morris, N., 2014. Capturing personality from Facebook photos and photo-related activities: How much exposure do you need? *Computers in Human Behavior*, 37, pp.162–170. Available at: <http://dx.doi.org/10.1016/j.chb.2014.04.048>.
- Goffman, E., 1990. *Presentation of self in everyday Life*, London, England: Penguin.
- Hall, J.A. & Pennington, N., 2013. Self-monitoring, honesty, and cue use on Facebook: The relationship with user extraversion and conscientiousness. *Computers in Human Behavior*, 29(4), pp.1556–1564. Available at: <http://www.sciencedirect.com/science/article/pii/S0747563213000046> [Accessed August 21, 2015].
- Hemingway, P. & Brereton, N., 2009. What is a systematic review? *European Journal of Oral Implantology*, 1(April), pp.174–175. Available at: <http://www.medicines.ac.uk/bandolier/painres/download/whatis/Syst-review.pdf>.
- Hollenbaugh, E.E. & Ferris, A.L., 2015. Predictors of honesty, intent, and valence of Facebook self-disclosure. *Computers in Human Behavior*, 50, pp.456–464. Available at: <http://www.sciencedirect.com/science/article/pii/S0747563215003179> [Accessed June 7, 2015].
- Lang, C. & Barton, H., 2015. Just untag it: Exploring the management of undesirable Facebook photos. *Computers in Human Behavior*, 43, pp.147–155. Available at: <http://dx.doi.org/10.1016/j.chb.2014.10.051>.
- Lang, G., 2012. *Think twice before you post: The impact of online self-presentation on the self-concept (Doctoral Dissertation)*. The City University of New York.

- Lee, E., Ahn, J. & Kim, Y.J., 2014. Personality traits and self-presentation at Facebook. *Personality and Individual Differences*, 69, pp.162–167. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0191886914003043> [Accessed October 30, 2014].
- Marriott, T.C. & Buchanan, T., 2014. The true self online: Personality correlates of preference for self-expression online, and observer ratings of personality online and offline. *Computers in Human Behavior*, 32, pp.171–177.
- McKinney, B.C., Kelly, L. & Duran, R.L., 2012. Narcissism or openness?: College students' use of Facebook and Twitter. *Communication Research Reports*, 29(2), pp.108–118.
- Michikyan, M., Subrahmanyam, K. & Dennis, J., 2014. Can you tell who i am? Neuroticism, extraversion, and online self-presentation among young adults. *Computers in Human Behavior*, 33, pp.179–183. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0747563214000156> [Accessed October 31, 2014].
- Moore, K. & McElroy, J.C., 2012. The influence of personality on Facebook usage, wall postings, and regret. *Computers in Human Behavior*, 28(1), pp.267–274. Available at: <http://dx.doi.org/10.1016/j.chb.2011.09.009>.
- Nadkarni, A. & Hofmann, S.G., 2012. Why do people use Facebook? *Personality and Individual Differences*, 52(3), pp.243–249. Available at: <http://www.sciencedirect.com/science/article/pii/S0191886911005149> [Accessed July 10, 2014].
- Petticrew, M. & Roberts, H., 2006. *Systematic Reviews in the Social Sciences: A Practical Guide*, Malden, MA: Blackwell. Available at: <http://www.cebm.a.org/wp-content/uploads/Pettigrew-Roberts-SR-in-the-Soc-Sc.pdf> http://books.google.com.br/books/about/Systematic_Reviews_in_the_Social_Science.html?id=_Ly3aPhTkbkC&redir_esc=y.
- Robinson, L., 2007. The cyberself: the self-ing project goes online, symbolic interaction in the digital age. *New Media & Society*, 9(1), pp.93–110.
- Ross, C. et al., 2009. Personality and motivations associated with Facebook use. *Computers in Human Behavior*, 25(2), pp.578–586. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0747563208002355> [Accessed July 9, 2014].
- Rui, J. & Stefanone, M. a., 2013. Strategic self-presentation online: A cross-cultural study. *Computers in Human Behavior*, 29(1), pp.110–118.
- Seidman, G., 2013. Self-presentation and belonging on Facebook: How personality influences social media use and motivations. *Personality and Individual Differences*, 54(3), pp.402–407. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0191886912004916> [Accessed July 15, 2014].

- Sun, T. & Wu, G., 2012. Traits, Predictors, and Consequences of Facebook Self-Presentation. *Social Science Computer Review*, 30(4), pp.419–433.
- Walther, J.B. et al., 2011. The effect of feedback on identity shift in Computer-Mediated Communication. *Media Psychology*, 14(1), pp.1–26. Available at: <http://www.tandfonline.com/doi/abs/10.1080/15213269.2010.547832> [Accessed October 22, 2014].
- Wang, J.L. et al., 2012. The relationships among the Big Five Personality factors, self-esteem, narcissism, and sensation-seeking to Chinese University students' uses of social networking sites (SNSs). *Computers in Human Behavior*, 28(6), pp.2313–2319.
- Wang, S.S., 2013. "I share, therefore I am": personality traits, life satisfaction, and Facebook check-ins. *Cyberpsychology, Behavior and Social Networking*, 16(12), pp.870–7. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/23992473>.
- Wardlaw, J., 2010. Advice on how to write a systematic review. , (January), pp.1–12. Available at: <http://www.bric.ed.ac.uk/research/guidance.html> [Accessed September 14, 2014].

SECONDARY SCHOOL TEACHERS' PERCEPTIONS OF INCIDENCES OF CYBER CRIMES AMONG SCHOOL-AGED CHILDREN IN LAGOS STATE, NIGERIA

Prof Emmanuel ADU,
&
Dr Olugbenga A. Ige Ph.D.
School of Educational Studies,
University of the Free State
QwaQwa Campus,
South Africa.
olugbengaige@gmail.com

Abstract

This study investigated the perceptions of teachers on the involvement of school aged children in Cyber Crimes in Nigeria. The study was the descriptive type while a survey method was applied. The sample of the study comprised two hundred and forty four teachers (244) purposefully selected from secondary schools in Lagos State, Nigeria. The instruments used for data collection were Teachers' Questionnaire on 'Yahoo Yahoo' (TQYY) and Teachers' Interview Schedule on 'Yahoo Yahoo' (TISYY). Descriptive statistics was used to analyze the quantitative data, while constant comparison technique was used to analyze the qualitative data. Results indicated that secondary school teachers were not only aware of Cyber Crimes perpetrated by school aged children, but knew school aged children who perpetrated Cyber Crimes otherwise known as 'Yahoo Yahoo'. Most teachers became aware of incidences of Cyber Crimes perpetrated by school aged children through Newspapers and Information from in-school aged children, whose age ranges between 12years to 23 years. Scam and Identity Theft were the most committed crimes on the Internet by school aged children. The study recommended that teachers should use value education, an aspect of Civic Education and Social Studies to educate school-aged children on the consequences of involving in cyber crimes.

Keywords

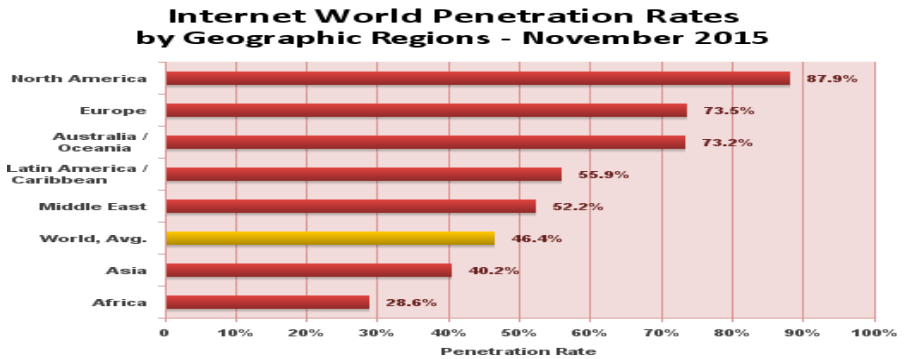
Secondary School Teachers, Cyber Crimes, School Aged Children

Introduction

The present information age is characterized with severe violent crimes perpetrated across international boundaries consequent on the evolution or emergence of the Internet. The previously 'sleepy' world is now connected is now globally linked consequent on the super highway of information gospel that has penetrated the different nations of the world. Unfortunately, individual users of the Internet have most times ignored the imminent dangers attached to the utilization of Internet to buy goods and services in the briskness to log on-line. Amosun, Ige, and Choo (2015) discovered that the Internet use and development in developing nations of the world like Nigeria, South Africa, Togo, Ghana, and Cameroon have witnessed whirling incidences of cyber crimes which rarely received governmental attention consequent on the technical nature of these crimes. The Internet Crime Complaint Centre (2014) reported that millions of people in the United States are victims of Internet crimes annually, with 'detection' which is the pivot of the extended larger Internet crime picture incomprehensible as the perpetrators could be millions of miles away in other countries of the world.

Opesade (2011) pointed out that the ever-evolving and increasing powerful Information and Communication Technology like the Internet has fundamentally transformed global relationships, sources of competitive advantage and opportunities for economic and social development, especially communication in real time across international boundaries in real time. It should be noted that this 'real time' communication does not exclude school-aged children, and by extension post primary education students. According to current statistics, seventy-seven million school-aged children regularly used the Internet in different nations of the world, while large numbers of school-aged children were observed to have utilized the Internet from home, school, and other locations, with forty-one percent logging online from any location (Child Predator Cyber Crime Unit, 2008; Amosun, et al., 2015).

Figure 1: Internet World Penetration Rates by Geographic Regions

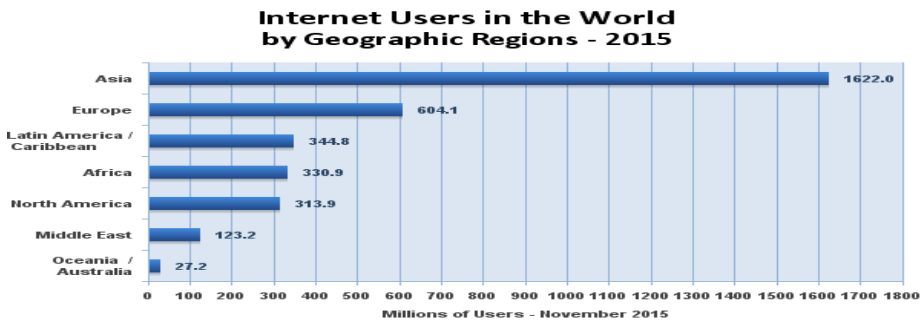


Source: Internet World Stats - www.internetworldstats.com/stats.htm
 Penetration Rates are based on a world population of 7,259,902,243 and 3,366,261,156 estimated Internet users on November 30, 2015.
 Copyright © 2016, Miniwatts Marketing Group

*The reproduction of this figure is in line the copyrights agreement of Miniwatts Marketing Group

From figure 1, North America, Europe, Australia/Oceania, South America, and the Middle East regions had above average Internet penetration rates, while Asia and Africa had paltry Internet penetration rates

Figure 2: Internet Users in the World by Geographic Regions in 2015



Source: Internet World Stats - www.internetworldstats.com/stats.htm
 3,366,261,156 Internet users estimated for November 30, 2015
 Copyright © 2016, Miniwatts Marketing Group

*The reproduction of this figure is in line the copyrights agreement of Miniwatts Marketing Group.

It could be noted from the reports of these national data agencies that the development and use of the Internet has greatly benefitted school-aged children in different nations of the world, but has also exposed them to possible negative consequences associated with Internet’s anonymity especially on-line criminal activities in African nations. The ubiquitous nature of the Internet to school-aged children’s daily exchange of information is presented on figure 1 and 2.

It could be seen from figure 2 that despite the surges in the Internet penetration rates of Euro-America and Austral-Middle East regions, Asia had the highest number of Internet users as at November 2015 (see figure 2). In addition to these, despite Africa’s low Internet penetration rates, the rate of Internet usage in Africa marginally outweighed that of North America which led the Internet penetration chart, and far outweighed the Internet usage of Middle East, and Asia put together. The differences noted in the Internet penetration rates and usage of Africa have grave implications for crimes perpetrated using the Internet in Africa. It means cyber crime would be on the increase among teeming school-aged children in Africa, should the Internet penetration rates improve. The Internet Crime Reports of year 2001 to 2010 published by the National White Collar Crime Center and the Federal Bureau of Investigation (FBI) in the United States of America show the extent to which cyber crimes have eaten deep into the economic and social fabric of Nigeria. Table 1 shows the top ten countries in the world whose citizens are involved in Internet crimes from year 2001 to 2010.

Table 1: Cyber Crime Ratings for Year 2001 to 2010

Countries	Year 2001	P	Year 2002	P	Year 2003	P	Year 2004	P	Year 2005	P	Year 2006	P	Year 2007	P	Year 2008	P	Year 2009	P	Year 2010	P
United States	87.6%	1st	76.7%	1st	76.7 %	1st	78.75%	1st	71.2%	1st	60.9%	1st	63.2%	1st	66.1%	1st	65.4 %	1st	65.9 %	1st
*Nigeria	2.7%	2 nd	5.1%	2nd	2.9%	3 rd	2.87%	3rd	7.9%	2nd	5.9%	2nd	5.7%	3rd	7.5%	3rd	8.0%	3rd	5.8%	3rd
Canada	2.5%	3 rd	3.5%	3rd	3.3%	2 nd	3.03%	2 nd	2.5%	4th	5.6%	3rd	5.6%	4th	3.1%	4th	2.6%	4th	2.4%	5th
Romania	0.9%	4 th	1.7%	4th	1.5%	7 th	0.92%	7th	0.7%	8th	1.6%	5th	1.5%	5th	0.5%	9th	-		-	
United Kingdom	0.9%	4 th	-		1.3%	8 th	2.32%	4th	4.2%	3rd	1.9%	4th	15.3%	2nd	10.5%	2nd	9.9%	2 nd	10.4 %	2nd
South Africa	0.5%	6 th	-		1.1. %	9 th	-		1.0%	7th	0.6%	10 th	0.9%	7th	0.7%	6th	0.7%	5th		
Australia	0.4%	7 th	0.9%	6th	-		-		-		-		-		-		0.5%	10 th	0.5%	10th
Indonesia	0.3%	8 th	0.5%	10th	-		-		-		-		-		-		-		-	
*Togo	0.3%	9 th	0.7%	7th	-		-		-		-		-		-		-		-	
Russia	0.2%	10 th	1.3%	5th	-		-		0.7%	8th	1.1%	8th	0.8%	9th	-		-		-	

Spain	-		0.6%	8th	2.4%	5 th	0.6%	9th	-		-		0.9%	7th	0.6%	7 th	0.7%	5th	0.8%	6th
Netherlands	-		0.6%	8th	0.9%	10 th	-		-		1.2%	6 th			-		-		-	
Italy	-		-		2.5%	6 th	2.01%	5th	1.7%	5th	1.2%	6th	1.3%	6th	0.5%	9th	-		-	
Germany	-		-		1.3%	8 th	-		-		0.7%	9th	-		-		-		-	
Greece	-		-		-		1.04%	6th	0.8%	10 th	-		-		-		-		-	
France	-		-		-		0.86%	8th	-		-		-		-		-		-	
China	-		-		-		0.58%	10th	1.1%	6th	-		-		1.6%	5th	-		3.1%	4th
*Ghana	-		-		-		-		-		-		0.7%	10th	0.6%	8th	0.7%	5th	0.7	8th
Malaysia	-		-		-		-		-		-		-		-		0.7%	5th	0.8%	6th
*Cameroon	-		-		-		-		-		-		-		-		0.6%	9th	0.6%	9th

Source: IC3 2001 – 2009 Internet Crime Reports (January 1, 2001 to December 31, 2010) prepared by the National White Collar Crime Center and the FBI

* The annual ranking of African countries in percentage (%).

*P connotes the positions of the listed countries

Table 1 shows that Nigeria was second in year 2001 among the top ten countries perpetrator with 2.7%. In year 2002, Nigeria retained the second position with 5.1% while Nigeria was third with 2.9% in year 2003. In year 2004, Nigeria still maintained the third position with 2.87%, even though this year recorded the lowest perpetration of internet crimes involving Nigerians. In year 2005, Nigeria moves to second position with 7.9%, and third repeatedly in years 2006, 2007, 2008 and 2009 with 5.9%, 5.7%, 7.5% and 8.0% respectively. In year 2010, Nigeria retains the third position with 5.8%, Table 1 shows a downward trend in the perpetration of scamming activities by Nigerians in 2010; this decline may not be unconnected with austere conditions caused by the global economic meltdown. Internet fraudsters could only thrive when the economic conditions of the target (mark) countries are in good condition. However, it should be noted that the Internet Crime Reports only show the ten most cyber lawless countries and leave out the remaining countries below the global top ten mark. This aim of this study, therefore, is to investigate the the perceptions of teachers on the involvement of school aged children in Cyber Crimes in Nigeria. This is, however, threatened by dearth of literature on the variables of interest in this study as they relate to incidences of Cyber Crimes as they relate to school age children in Nigeria.

Note: The National White Collar Crime Center and the Federal Bureau of Investigation stopped releasing statistics of top countries perpetrators of cyber crimes from year 2011.

Cybercrimes among Students

Amosun and Ige (2009) discovered in their study of secondary school students' perceptions of school-aged children involvement in cyber crimes that seven hundred and seventy-eight (778) of the nine hundred and thirty (930) students used for the study not only responded that they knew their colleagues who perpetrated cyber crimes, but were aware of the different types of crimes perpetrated by their colleagues. The analysis of the data collected reveals that students were aware that their colleagues perpetrated the following crimes on the Internet: Credit Card Fraud, which is a process of obtaining unauthorized fund from an account (59.2%); Nigerian Letter Fraud, a confidence trick in which the target (person) is persuaded to advance a relatively small sums of money in the hope of realizing a much larger gain (64.8%); Spam, unsolicited electronic mail (36.0%); Phishing, the act of sending an e mail to Internet users falsely claiming to be an established legitimate enterprise in an attempt to scam the users into surrendering private information that will be used for

identity theft (39.6%); Investment Fraud, the practice of deceiving and manipulating investors resulting in theft of capital (54.1%).

Automated Teller Machine Fraud, using special hacking software that could record the sequence of key strokes those computer users make on their key boards or infiltrate Internet banking (64.8%); Confidence Fraud, attempt to or swindling a person which involves gaining his or her confidence i.e. confidence tricks (64.8%); Identity Theft, the use of another person's name and social security number to obtain goods and services (40.3%); Espionage, stealing a trade secret, supplier agreement, personal records, and research documents on prototype plans for a new product on service (34.4%); Kidnapping children via Internet chat rooms (34.4%); Creation and distribution of viruses (51.4%); Cyber Terrorism, the use of information technology by terrorist groups and individual to further their agenda (46.1%); Scam, fraudulent e-mail that appears to be from a legitimate Internet address requesting to certify your personal information on account details (44.0%); Auction Fraud, the non-delivery of an item purchased through the Internet auction site on non-payment for goods purchased through an Internet auction site (40.0%). Child Pornography, accessing websites which depicts children engaging in sexual conduct with prohibition as child sexual abuse in most countries (64.9%); and Business Fraud, asking people to invest in a non-existent business on-line (67.0%). The researchers subsequently recommended that the reviewed Social Studies curriculum should reflect Internet crime as an emerging social problem and issue in Nigeria.

Furthermore, Adepoju (2009) carried out a study on the perceptions of incidences of Internet crimes among university students in south-western, Nigeria and discovered that tertiary institution students were aware of all the various Internet crimes perpetrated in Nigeria. The analysis shows that the most common Internet crimes they are aware of are: Spam (60.2%), Hacking (55.7%) Auction (52.0%), Financial

Institution Fraud (52.5%), Kidnapping via chat rooms (60.4%), Business Fraud (55.1%), Phishing (53.5%), Credit Card Fraud (60.9%) and Debt elimination (64.5%). Adepoju further stated that Credit Card Fraud has the highest frequency of 60.9% and that the use of credit card is a relatively new feature of the economy in Nigeria. The researcher infers that it may not be out of place to say that those being defrauded on the Internet are citizens of the developed nations of the world, and recommended that further studies be conducted in other states in Nigeria to confirm this assumption. Adepoju subsequently proposed that Internet crime prevention education should be incorporated into the curriculum of Civic Education and Social Studies to help students learn the ideals of good citizenship and shun acts that can negatively impair on the image of Nigeria.

The role of teachers in observing and mentoring school children is well documented in research (Pitzer and Skinner, 2016; Berkowitz, 2013). Gurland and Evangelista (2015) asserted that teachers constitute an important social context for students' school lives. It could be inferred from this assertion that teachers roles goes beyond enhancing the academic achievement of students as research (Wang and Neihart, 2015) has shown that several psychological and behavioral constructs have been identified to be strong enablers of students learning outcomes. It is based on the foregoing that this study evaluated teachers' perceptions of the incidences of cyber crimes among school-aged children, consequent on their in loco parentis status to school-aged children in Nigeria.

Definition of Terms

In this study, a teacher refers to a person with the Bachelor's degree in any field of study that manages lesson instruction and classes in the selected secondary schools. Cyber crime is a crime committed on the Internet, using the internet, and by means of the Internet. The local acronym for cyber crime in among students at different educational levels is 'Yahoo Yahoo'. A School-aged child in Nigeria is 5 to 17 years

old (Ademokun, Osungbade, and Obembe, 2014), he or she might have or not have direct contact with a school for about six hours daily, and up to thirteen years for overall intellectual development. However, the age of a school- aged child in school might be slightly higher than seventeen years in some exceptional cases.

Research Questions

1. Are secondary school teachers aware of the incidences of cyber crimes among school-
Aged children?
2. What are teachers' sources of information on incidences of cyber crimes among school-aged children?
3. Which of the cyber crimes perpetrated by school-aged children is commonly known to secondary school teachers?
4. Which gender of school-aged children engages most in cyber crimes?

Research Method

Research Approach and Design

The study adopted a mixed method research approach because it has both qualitative and quantitative approaches; hence the adoption of a descriptive survey design and the ethnographic research design. The study is also an ex-post facto study, because the researcher does not have a direct control of both the independent and dependent variables as their manifestations have already occurred are inherently not manipulable. The ethnographic research design was appropriate because teachers' in-depth interview and observation of the students engaging in scamming activities were conducted in selected local government areas of Lagos State.

Samples

The study sample comprised 88 male, 143 female and 13 gender anonymous secondary school teachers in Lagos State, Nigeria. In all, 244 male and female secondary school teachers were used for the study.

Instruments

The Teachers' Questionnaire on 'Yahoo Yahoo' (TQYY) was developed from the Students' Questionnaire on 'Yahoo Yahoo' (SQYY) by Ige (2008). The 'TQYY' was used to collect information on teachers' perceptions of school-aged children's involvement in 'Yahoo Yahoo', teachers' sources of information on school-aged children's involvement in 'Yahoo Yahoo' and teachers' awareness of types of cyber crimes in eliciting feedback from the teachers. It was given to other experts in the Social Science Education Department for evaluation. The final form of the items was then validated in terms of administering the instrument on 50 secondary teachers and a Cronbach Alpha of 0.98 was obtained. The second instrument used, was Teachers Interview Schedule on 'Yahoo Yahoo' (TISYY), a 5-item interview schedule developed by the researchers to collect data on teachers' awareness of 'Yahoo Yahoo'. To ascertain the validity of this instrument, the researcher made use of ten (10) teachers that were not involved in the study. Each item was discussed; two (2) items that were found difficult were removed. The instrument was further vetted and certified fit for use by a Senior Lecturer in the Social Science Education Department.

Data Analysis

The quantitative data collected was analyzed using frequency counts and percentages. The qualitative data was analyzed by the pattern of participants' response to the questions posed during the interview (i.e. directly using the language of the respondents). The

constant comparison technique was used as a means of analysis (Glaser and Strauss, 1967), all the data were ‘open coded’ to produce an initial code list, until in the opinion of the researcher, analysis had reached theoretical saturation. General trend from responses to each question was identified and examined.

Results

The study investigated secondary school teachers’ perceptions of incidences of Cyber Crimes among school-aged children. Frequencies of the teachers’ response are given in Tables 2-4 for the teachers respectively.

Research Question 1: Are secondary school teachers aware of the incidences of cyber crimes among school-aged children?

Table 2: Teachers’ Awareness of School-Aged Children’s Involvement in Cyber Crimes

S/ No	Statement	Yes		No	
		Freq.	%	Freq.	%
1.	Are you aware of ‘Yahoo Yahoo’	213	87.3	31	12.7
2.	Are school-aged children involved in ‘Yahoo Yahoo’	198	81.1	46	18.8
3.	I know some of my students’ who are involved in ‘Yahoo Yahoo’	40	16.1	204	83.6

Table 2 shows that 213 (87.3%) teachers were aware of the existence of cyber criminal acts perpetrated through the Internet, otherwise called ‘Yahoo Yahoo’, while 31 (12.7%) were not aware of these crimes that evolved in tandem with the evolution of the Internet. 198 (81.1%) teachers responded that they were aware that their students were involved in Cyber Crimes, otherwise known as ‘Yahoo Yahoo’ while 46 (18.8%) teachers were not aware. 40 (16.4%) teachers knew their students who perpetrated Cyber Crimes, while 204 (83.6%) teachers did not.

Research Question 2: What are teachers’ sources of information on incidences of cyber crimes among school-aged children?

Table 3: Teachers’ Sources of Information on Incidences of Cyber Crimes among School-Aged Children.

S/No	Sources of Information	Freq.	%
1	Newspaper	83	34.0
2	Magazines	22	9.0
3	Websites	18	7.4
4	Television	54	22.1
5	Students	50	20.5
6	Others	1	0.4
7	No Response	16	6.6
	Total	244	100.0

Table 3 shows the teachers sources of information on incidences of Cyber Crimes among school-aged children. The results show that 83 (34.0%) teachers got to know about Cyber Crimes otherwise called ‘Yahoo Yahoo’ perpetrated by school-aged children through Newspapers, 22 (9.0%) through Magazines, 18 (7.4%) via Internet Websites, 54 (22.1%) through Television, 50 (20.5%) through information from students, and 1 (0.4%) through other sources; while 16 (6.6%) did not indicate how they heard about ‘Yahoo Yahoo’ acts perpetrated by school-aged children.

Research Question 3: Which of the cyber crimes perpetrated by school-aged children is commonly known to secondary school teachers?

Table 4: Teachers’ Level of Awareness and Non Awareness of Incidences of Cyber Crimes

S/No	Types of Internet Crimes	Aware		Not Aware	
		Freq.	%	Freq.	%
1.	Nigeria letter fraud (on –line 419).	195	79.9	49	20.1
2.	Obtaining goods without paying or obtaining unauthorized fund from account (Credit Card Fraud).	204	83.6	40	16.4
3.	Spam (unsolicited electronic mail)	194	79.5	50	20.5
4.	The act of sending an email to internet user falsely claiming to be established legitimate enterprises in an attempt to scam the users into surrendering private information that will be used for identifying theft.	201	82.4	43	17.6
5.	Using special hacking software that could record the sequences of key strokes that computer user makes on their key boards or infiltrates internet banking (Financial	160	65.6	84	34.4

	Institutions Fraud).				
6.	Attempt to or swindle a person which involves gaining his or her confidences i.e. (Confidence Fraud)	183	75.0	61	32.2
7.	The use of other person's name and social security number to obtain goods and services. (Identity Theft).	212	86.9	32	16.7
8.	Stealing a trade secret, supplier's agreement personal records, to obtain goods and services (Espionage).	168	68.9	76	31.1
9.	Kidnapping children via internet chat room.	148	60.7	96	39.3
10.	Creation and distribution of Computer Virus.	152	62.3	92	48.5
11.	The use of information technology by terrorist groups and individuals to further their agenda (Cyber Terrorism).	165	67.6	79	32.3
12.	Fraudulent e-mail that appears to be from a legitimate internet addresses requesting to certify your personal information on account detail (Scam).	212	86.9	32	13.1
13.	The non-delivery of an item purchased through the internet auction site on non-payment for goods purchased through an internet auction site (Auction Fraud).	200	82.0	44	18.0
14.	Ordering an item, making payment, and receiving nothing or shipping merchandise which was never ordered and obtaining a signature on delivery (Non-Delivery, Mdse & Payment).	192	78.7	52	21.3
15.	Accessing website which depicts children engaging in sexual conduct with prohibition as child sexual abuse (Child Pornography).	183	75.0	61	25.0

Table 4 shows that ‘Scam’, which is fraudulent e-mail that appears to be from a legitimate Internet Address requesting to certify individuals’ information on account details and ‘Identity Theft’, the use of other person’s name and Social Security Number to obtain goods and services, were the most committed crimes in the Cyber Space by school-aged children.

Research Question 4: Which gender of school-aged children engages most in cyber crimes?

Table 5: Teachers’ Perceptions of Secondary School Students’ Gender Involvement in Cyber Crimes

S/No	Students’ Gender	Freq.	%
1.	Male	193	79.1
2.	Female	15	6.1
3.	No Response	36	14.8
	Total	244	100.0

From the teachers’ response in Table 5, male school-aged children {F=193(79.1%)} perpetrate economic crimes than their female counterparts {F=15(6.1%)}.

Qualitative Analysis/ Respondent Theme

Eighteen Vice-Principals in the schools selected for the study were given interview schedules as most of them declined oral interview.

Research Question 1: Are secondary school teachers aware of the incidences of cyber crimes among school-aged children?

A Vice-Principal, Mr. Remi (Not a real name) in Ogudu Senior Grammar School stated that:

He became aware of Cyber Crimes perpetrated by school-aged children from secondary school students in his school and neighborhood. They always visit the cyber cafes and engage in lavish spending after defrauding people abroad.

Ajana (not a real name), a Chief Education Officer in Ojota Senior Secondary School said:

Yes! They meet me at various times at a Cyber café. The boys' majority, few girls. I see them always at a Café in school uniforms.

An Area Education Officer who did not disclose her identity in Ojota Senior Secondary School said:

I am aware of cyber criminal acts perpetrated by school-aged children on the Internet. 'Yahoo Yahoo' is not something students hide any longer, the students discuss it openly.

Research Question 2: What are teachers' sources of information on incidences of cybercrimes among school-aged children?

Ale (not a real name), a School Counsellor and Vice Principal in Ojota Senior Secondary School said:

He became aware of school-aged children's involvement in 'Yahoo Yahoo' through 'Word of Mouth'

A Principal who did not disclose his school and identity stated that:

Through the scamming students discussions on how they have reaped foreigners of their money. When I go to the Cyber Café, I see them chatting with over ten people at a time. Some posed as girls.

Research Question 4: Which gender of school-aged children engages most in cyber crimes?

From the interview carried out among teachers, Mr. Ota. E (not a real name), an education officer II in Ogudu Grammar School, stated that:

Male school-aged children are more into online crimes than the female students.

An Assistant Director of Education who declined to state her identity and designation in United Secondary School, Ikorodu, said that:

Both male and female school aged children involved in 'yahoo yahoo' but it is mostly common among male school-aged children.

However, a Principal Education Officer, Mr. Aye (not a real name) stated that:

Males do it to increase their horizon.

Discussion

The perceptions of the selected teachers show that 213 (87.3%) teachers were aware of the existence of cyber criminal acts perpetrated through the Internet, otherwise called 'Yahoo Yahoo', while 31 (12.7%) were not aware of these crimes perpetrated through the Internet, this confirms the findings of Ige (2008); Amosun and Ige (2009); Adepoju (2009) and Oloko (2011) who found out that Cyber Crimes acts is not only peculiar to university students, but, school-aged children in Nigeria. 198 (81.1%) teachers responded that they were aware their students involved in Cyber Crimes, otherwise known as 'Yahoo Yahoo' while 46 (18.8%) teachers were not aware. Also, 40 (16.4%) teachers knew their students who perpetrated Cyber Crimes, while 204 (83.6%) teachers differ; this confirms the findings of Ige (2008) who found out that in school-aged knew their colleagues who perpetrated Cyber Crimes. Most teachers knew about school aged children's involvement in Cyber Crimes through the Newspapers and students, while others did not indicate their source of information.

The analysis of the data collected from the teachers that 'Scam' which is fraudulent e-mail that appear to be from a legitimate Internet Address requesting to certify individuals' information on account detail and 'Identity Theft', the use of other person's name and Social Security Number to obtain goods and services were perceived as the most committed crimes in the cyber space by school-aged children. The use of Social Security Number to obtain goods and services is not an economic or social feature of the Nigerian society. This confirms Amosun and Ige (2008) and Ic3 (2001-2010) findings that the people being defrauded on the Internet by school-aged children in Nigeria are residents of developed countries like Britain, United States, Germany, Canada etc. In addition to these, the qualitative and quantitative analysis of the data collected shows that males perpetrated Cyber Crimes than females. These confirm the findings of Ige (2008); Amosun and Ige (2009); Adepoju

(2009) and Oloko (2011) that male school-aged children and tertiary institution students involved in Cyber Crimes than their female colleagues.

Implications for Teacher Education

The study shows from secondary school teachers' perceptions that school-aged children are involved in cyber crimes, contrary to public perceptions that only tertiary students engaged in cyber crimes otherwise called 'Yahoo Yahoo' in Nigeria. Allied to the findings of this study is the urgent need for the African countries of Nigeria, South Africa, Ghana, Cameroon, and the Middle East countries of United Arab Emirates, Saudi Arabia, Qatar, Kuwait, Oman, and Bahrain to engage in participatory educational programmes in cyber security to protect her school-aged children.

It is, therefore, recommended that teachers should use value education, an aspect of Civic Education and Social Studies to educate school-aged children on the consequences of ill-gotten wealth. School-aged children should be made to have the mind-set for entrepreneurship activities, rather than depend on fraudulent means to sustain themselves especially in Nigeria.

References

Adepoju, O.M. (2009), "Tertiary students' perceptions of incidences of internet crimes in south western, Nigeria", *Unpublished M.Ed. dissertation*, University of Ibadan.

Ademokun, Oluwakemi M., Kayode O. Osungbade, and Taiwo A. Obembe. "A Qualitative Study on Status of Implementation of School Health Programme in South Western Nigeria: Implications for Healthy Living of School Age Children in Developing Countries." *American Journal of Educational Research* 2.11 (2014): 1076-1087.

Amosun, P.A., and Ige, O.A. (2009), "A new breed of crime among in – school aged children in Nigeria", *The African Symposium*, Vol. 9, No. 2, pp90-98, https://www.ncsu.edu/aern/symposium_main.htm, (Accessed 11 December 2015).

Amosun, P.A., Ige, O.A., and Choo, K.K.R. (2015), "Impact of a participatory cyber-crime prevention programme on secondary school students attainment in crime prevention concepts in civic education and social studies", *Education and Information Technologies*, Vol. 20, No. 3, pp505-518.

Arowosaiye, A.I. (2009), *The devastating impact of money and other Economic and Financial Crimes on the Economy of Developing Countries: Nigeria as a Case study*, [https://unilorin.edu.ng/.../arowosayeyi/The%20Devastating%20Impact%](https://unilorin.edu.ng/.../arowosayeyi/The%20Devastating%20Impact%20). (Accessed 11 April 2012).

Berkowitz, R. (2014), *Teacher and student responses to violence in school: The divergent views of bullies, victims, and bully- victims*, *School Psychology International*, Vol. 35, No. 5, pp485-503.

Cheryl, T. (2007), Keep your child safe from internet porn. <https://www.cbn.com>, (Accessed 13 February 2007).

Chiemeke C.S. and Longe O.B. (2007), *Information and communication penetration in Nigeria: Prospects, challenges and metrics*, *Asian Journal of Information Technology*, Vol. 6, No. 3, pp280-287.

Gurland, T.S. and Evangelista, J.E. (2014), Teacher-student relationship quality as a function of children's expectancies, *Journal of Social and Personal Relationships*. Vol. 32, No. 7, pp879-904.

Ige, O.A. (2008), Secondary school students' perceptions of incidences of internet crimes among school aged children in Ondo

and Oyo States, Nigeria, Unpublished M.Ed. dissertation, University of Ibadan, Ibadan.

Longe O.B., Chiemeke, S.C., Onifade, O.F.W., Balogun, F.M., Longe, F.A., and Otti, V.U. (2007), Exposure of children and teenagers to internet pornography in south-western Nigeria: Concerns, trends and implications. *Journal of Information Technology Impact*, Vol. 7, No. 3, pp197-212.

Office of the Attorney General of Florida (2008), Child predator and cyber crime unit, <http://www.childpredatorcybercrimeunit.mht>, (Accessed 30 March 2011).

Oloko, O.O. (2011), *Secondary school teachers' perceptions of incidences of economic crime among school aged children and their critical thinking dispositions in Lagos State*, Unpublished B.Ed. project, Adekunle Ajasin University, Akungba Akoko.

Opesade, A.O. (2011), Strategic, value-based ICT investment as a key factor in bridging the digital divide, *Information*

Development, Vol. 27, No. 2, pp100-108. <http://www.idv.sagepub.com>, (Accessed 6 May 2016).

Pfizer, J. and Skinner, E. (2016), *Predictors of changes in students' motivational resilience over the school year: The roles of teacher support, self-appraisals, and emotional reactivity*. *International Journal of Behavioral Development*, pp1-15. <http://www.jbd.sagepub.com>, (Accessed 6 May 2016).

PricewaterhouseCoopers (2014), Global economic crime survey, <http://www.pwc.com/gx/en/services/advisory/consulting>, (Accessed 13 December, 2015).

The National UAE. (2014, March), Cyber-attacks a growing risk in the Middle East, <http://www.thenational.ae/uae/technology/cyber-attacks-a-growing-risk-in-the-middle-east>, (Accessed 13 December 2015)

The National White Collar Crime Center. (2007), Internet crime report (January 1, 2006 to December 31, 2006), pp. 1-27. <http://www.IC3.state.gov>, (Accessed 27 April, 2007).

The National White Collar Crime Center. (2008), Internet crime report (January 1, 2007 to December 31, 2007), pp. 1-29. <http://www.IC3.state.gov>, (Accessed 3 May, 2008).

The National White Collar Crime Center. (2009), Internet crime report (January 1, 2008 to December 31, 2008), pp. 1-29. <http://www.IC3.state.gov>, (Accessed 3 May, 2008).

The National White Collar Crime Center. (2010), IC3 2009 Internet crime report (January 1, 2009 to December 31, 2009), pp. 1-29. <http://www.IC3.state.gov>, (Accessed 3 May, 2008).

The National White Collar Crime Center. (2011), *IC3 2010 Internet crime report* (January 1, 2010 to December 31, 2010), pp. 1-29. <http://www.IC3.state.gov>, (Accessed 3 May, 2008).

The National White Collar Crime Center. (2015). *IC3 2014 Internet crime report* (January 1, 2014 to December 31, 2014), pp.1-48, <http://www.IC3.state.gov>. (Accessed 13 December 2015).

Wang, C.W. and Neihart, M. (July, 2015), How do supports from parents, teachers, and peers influence academic achievement of twice-exceptional students? *Gifted Child Today*, <http://www.gct.sagepub.com>, (Accessed 3 March 2016).

Towards a Cyber Safety Information Framework for South African Parents

Elvira Paraiso
 Department of Informatics
 University of Pretoria
 u15260772@up.ac.za
paraisel@gmail.com

Machdel Matthee
 Department of Informatics
 University of Pretoria
 Machdel.Matthee@up.ac.za

Abstract

In a world where technology is increasingly used in schools, cyber safety education is the responsibility of teachers and parents or caregivers. Unfortunately, the situation in developing countries such as South Africa is that children, parents and teachers are ill-prepared for the dangers associated with the use of information technology. This paper reports on research in progress to address this problem by aiming to develop a cyber-safety information framework that can be used to inform and guide parents toward understanding and ensuring the cyber safety of their children. By following a design science research approach, we propose a framework with three interdependent components: 1) parents' information needs (determined by their digital literacy, cybersafety awareness levels and the age of their children), 2) ways of disseminating the information (videos, parents' meetings, online information or books), 3) the actual content (categorising and evaluating existing available content).

Keywords

Cyber Safety, Cyber Safety Education, Parents' Awareness of cyber safety

1. Introduction

The utilisation of the internet and communication technology devices such as cell phones, tablets in education, has increased over the last decade (Kambourakis, 2013). This innovative form of learning comes with advantages and drawbacks. It offers an unbounded learning experience since learning is no longer restricted to a classroom (Johnson, et al., 2012) and can take place anytime, in any place. Regrettably, amongst several other issues, learners especially children, are exposed to threats to their security and safety (Sharples, 2006).

In South Africa, government and service providers have launched quite a number of initiatives to implement technology usage in schools. For the children to be well

prepared for the online world, they need to be taught how to be and remain safe online. Ideally, cyber safety education needs to come from parents at home and be sustained by teachers at school. These two role players must also make sure that the education received is indeed followed by the children. Unfortunately, the situation in developing countries as well as South Africa is that children, parents and teachers are ill-prepared for the dangers associated with the use of information and communication technology (ICT). No comprehensive cyber safety initiatives are in place, and schools lack relevant curricula (von Solms & von Solms, 2014). In addition, most parents are not familiar with what is going on online or how they can assist their children (de Lange & von Solms, 2012) according to their ages and abilities. The assumption is that in the South African context the digital literacy levels and cyber safety awareness of parents vary extensively.

This paper reports on ongoing research aimed at raising the levels of awareness of cyber safety of parents. The paper proposes a preliminary cyber safety information framework. The proposed framework will be developed from existing literature during the suggestion phase of a design science methodology after which it will be refined by the feedback received from a questionnaire. This paper only focuses on the proposed framework which is presented in section 4. The next section gives an overview of existing literature.

2. Literature review

2.1. Cyber safety

Cyber safety refers to the study of the safe and responsible way in which the internet and technology devices such as tablets and cell phones should be used (Pusey & Sadara, 2011). It helps building awareness of potential issues that can be encountered while using these technologies. These issues are often referred to as cyber safety threats. The most common threats are cyberbullying, sexting/ “sextortion”, talking or meeting with strangers, accessing inappropriate content and being exposed to a breach of privacy (Beger & Sinha, 2012). A few of these threats or dangers are discussed below.

Cyberbullying: It refers the use of the internet and technology devices to harass, discriminate and disclose someone’s personal information (Belsey, 2006) with mean, false and vulgar comments with the intention of denigrating them (Burton & Mutongwizo, 2009). It can be done anonymously or not. It is prevalent amongst young people where the perpetrators are often classmates (Popovac & Leoschut, 2012).

Sexting: It can be defined as the act of sending and receiving sexually suggestive photos, videos or text messages (Burton & Mutongwizo, 2009). Sexting can also refer to the involvement of minors in sending and receiving such content, and may also be classified as child pornography or paedophilia (Youth Online Safety Working Group, 2010).

Talking or meeting with strangers: The cyberspace offers an opportunity for everyone to talk and share ideas and knowledge freely without personally knowing each other (Beger & Sinha, 2012). Unfortunately, it provides a wide platform for predators as well. The US Department of Justice (2006) reported that at any given time of the day, at least fifty thousand predators are online browsing for children.

Age inappropriate content: Youngsters might unintentionally access inappropriate, and destructive content (Australian Communications and Media Authority, 2015). Inappropriate content might appear while children knowingly access this kind of content or as pop-ups while following unknown links or mistyping online search terms.

Breach of Privacy – Identity theft: It involves individuals who seek to change their identities with bad intentions. It also includes those that act as someone else or using people's credentials without their permission.

2.2. Cyber safety skills and digital literacy

Digital literacy refers to the skill set necessary to participate in the digital era. These skills are more than the ability to use digital devices. It also includes “for example, “reading” instructions from graphical displays in user interfaces; using digital reproduction to create new meaningful materials from existing ones while considering copyrights; constructing knowledge from a nonlinear, hypertextual navigation; evaluating the quality and validity of information; and having a mature and realistic understanding of the “rules” that prevail in the cyberspace” (Eshet-Alkalai, 2004). Although cyber safety skills and digital literacy are not synonymous, Sonck, Livingstone, Kuiper and de Haan (2011) show that they are closely related. They found that amongst European children aged 9 – 16, those with high levels of digital literacy are also much more skilled in navigating online activities in a safer way. Sonck et al. (2011) imply that improved digital literacy will consequently improve cyber safety skills and vice versa. Digital literacy enables one to browse the internet safely, change privacy settings on platforms and devices, judge the quality and reliability of the information accessed and understand and apply the online norms (Telstra Corporation Limited, 2014) in order to make informed decisions.

The majority of African countries including South Africa do not have proper programs in place for cyber safety awareness for children, parents or teachers (von Solms & von Solms, 2014). In South Africa, the high level of digital illiteracy in conjunction with the access to ICT infrastructures, the language barrier and the geographic location of individuals have a strong negative impact on cyber safety awareness (Kritzinger, 2015). It is important that cyber safety material, adapted to these realities, be developed to enhance cyber safety awareness and digital literacy.

2.3. Parents and cyber safety

Parents play a crucial role in cyber safety awareness education of their children. It is essential for parents to recognise the cyber safety threats and to be able to react to them. This will minimise the impact of these threats on their children. It has globally been observed that parents are ill-prepared to take part in the cyber safety education (de Lange & von Solms, 2012). Schools should be able to help raise parents' awareness of cyber safety for active participation in the cyber safety education of their children (de Lange & von Solms, 2012). In European countries, parents with lower levels of digital literacy, tend to be more restrictive towards the use of Internet by their children and therefore also restricting the learning and online exploration by their children. Those parents' with higher levels of digital literacy tend to embrace technology with their children and guide them more efficiently (Duerager & Livingstone, 2012). If this trend also holds for developing countries, parents with lower levels of digital literacy will not be able to guide their children to discover the internet in a safe way while the parents that are more informed would be able to set rules and teach their children acceptable online behaviour (Valcke, et al., 2011).

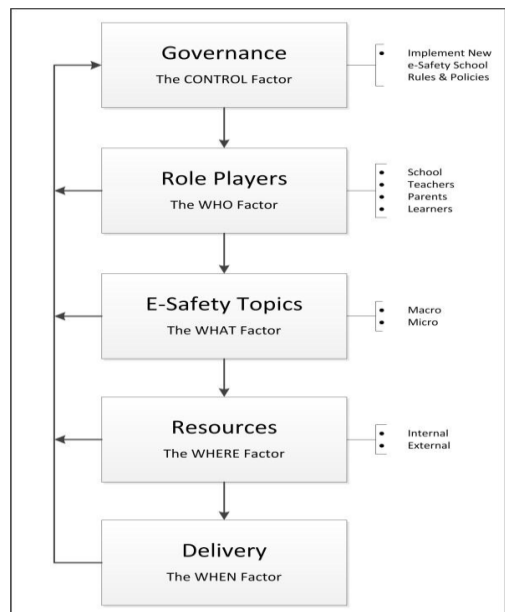
Duerager & Livingstone (2012) recommended that instead of restricting the internet usage of their children, parents need to embrace the technology and be actively part of their children's online experience. Parents need to discuss the possible dangers with their children, engage with their children's internet use and set rules according to their children's age.

2.4. Cyber Safety Information Framework

De Lange and von Solms (2012) proposed a high-level cyber safety framework in order to guide the implementation of cyber safety education in school. It comprises of five components which need to be taken into consideration for an effective cyber safety education in schools. The components are discussed briefly below.

Governance: The CONTROL Factor

This part implies that when starting any cyber safety awareness initiative, cyber safety policies and school rules must be developed and implemented. It should be flexible enough to cover diverse aspects like internet access at school, the devices used, ownership of the devices, etc. Policies should clearly state unacceptable behaviours and their possible consequences. For these policies and rules to be effective, all the role players should be aware of it and the role they play in its application. A supervision and monitoring



strategy should also be in place and applied.

Role Players: The WHO Factor

As stated earlier, all parties involved in a cyber safety implementation process should be identified. Each party should know clearly the role they need to play in the process and must be willing to work together with the others parties to make the implementation effective. The researchers have identified four role players discussed below.

Figure 2 High-Level e-Safety Framework, de Lange & von Solms

- **The School** which is seen as the entity that is responsible for developing school policies and rules. While doing so, they must take in consideration legislations and regulations and they must assume the responsibility and lead the implementation of the cyber safety strategies. To facilitate this process, if possible, the school should appoint a person with enough cyber safety knowledge and expertise to coordinate the operations.
- **The Teachers** can take four different roles. They can be *learners*, *advisors*, *teachers*, and *identifiers*. Because teachers have to be able to recognise and react to cyber safety threats, they need to receive training to prepare them. In this case, they will be seen as *learners*. Moreover, if children experience online threats and need to talk, teachers need to be ready to listen and give advice, therefore, they can also be seen as *advisors*. Teachers should be able to deliver relevant information on cyber safety to the children in the *teacher* role. Teachers must also be *identifiers* and determine any change in children's behaviour or any alarming facts that might need to be investigated.
- **The Parents** must play a major role in raising cyber safety awareness of children. As it has been observed that parents are ill-prepared for cyber safety education, they need to receive the necessary training. In this case, they will be seen as *learners*. After having received enough knowledge, they will become *teachers* as they will be required educate their children. Similarly to the teachers, they must also be ready to become *identifiers* and *advisors*, whenever it would be necessary.

- **The Learners'** needs should be determined according to their age, skill's level and comprehension facility. The cyber safety education needs to be given from a very young age to develop a cyber safety culture. Similar to Teachers and Parents, Learners can be seen as *teachers* when informing their peers, *identifiers* to spot and report any alarming fact to adults, and *advisors* to help their peers when needed.

E-Safety Topics: The WHAT Factor

Schools need to identify which topics of cyber safety need to be discussed and to which extent with each role players. Each role player needs to be directed to the place where they can find contents adapted to their specifics needs.

Resources: The WHERE Factor

These are the actual places where information about cyber safety can be found. Resources can be a teacher, or a teachers' initiative or external resources retrieved online or at the library from existing published content.

Delivery: The WHEN Factor

It is the time when the information can be disseminated. For parents, it might be during parents' meetings and for learners during computer literacy lessons.

This paper will extend and adapt this framework, focusing mainly on Parents and the how to prepare them for the role they should play in cyber safety awareness education. The proposed framework will try to establish parameters that need to be taken into consideration as well as actual content that can be given to parents to uplift their cyber safety skills for them to assist their children efficiently.

3. Research Approach

This study is a design science study. Design science research involves the conception of an innovative understanding by creating an artefact and the evaluation of such artefact by the intended users in order to improve a given situation (Vaishnavi & Kuechler, 2004). Using design science in research helps to create products that are useful to humans (March & Smith, 1995).

To simplify the use of design science in practice, a Design Science Research Methodology has been developed by Vaishnavi & Kuechler (2007). They have divided the process into five steps of which each, and how it has been or will be applied, is discussed below.

Step 1: Awareness of the problem

Section 1 and 2 highlighted the general unpreparedness of South African parents to help with cyber safety education of their children as well as the monitoring and

guiding of their children's online activities. In addition, the lead-researcher was part of a cyber safety campaign around some schools around Diepsloot. From this experience, it seems that most teachers, who are also parents, were not aware of most of the information which were shared during the campaign. They were not aware of most of the online threats and what they could do to avoid them. They appreciated the campaign and emitted the need of information which is easy to access and understand which they could use for themselves and to educate others around them.

Step 2: Suggestion

The proposed framework, which is discussed in more detail in section 4, is based on the high-level e-Safety framework proposed by de Lange and von Solms (2012) and the review of published literature. A questionnaire based on the suggested framework will be distributed amongst parents of a secondary school during a parents' meeting.

Step 3: Development

The suggested framework will be refined based on the response of the parents to the questionnaire.

Step 4: Evaluation

At this step, the refined framework will be tested and evaluated by the intended users after which changes will be made accordingly. The framework will be shared with parents for evaluation by giving examples of possible interventions. Their feedback will be used to finalise the framework.

Step 5: Conclusion

The final framework will be shared with the school, parents and service providers of the e-textbook platform. It will also be disseminated on the university platform of dissertations and theses.

4. Suggested cyber safety information framework for parents

The suggested framework can be seen as an extension of the e-Safety framework proposed by De Lange and von Solms (2012) in the sense that it focuses on one of the role players only, namely the Parents.

For the purpose of the research, parents are seen here as *learners* who need to receive an effective training in order to become *teachers*, *identifiers* and *advisors*. It is also assumed that the school has policies and rules in place so the aim of the framework would be to ensure that the parents know them.

Table 1 below shows how we have used the cyber safety framework's components of de Lange and von Solms (2012) to direct our thoughts.

Table 6 Extension criteria

E-Safety Framework Components	Our Extension Criteria
<i>Governance: The CONTROL Factor</i>	What has been done/ given to parents by the school? Do parents know clearly what role they need to play?(3)
<i>Role Players: The WHO Factor</i>	What are the parents' needs to become effective teachers, advisors and identifiers? (3)
<i>E-Safety Topics: The WHAT Factor</i>	What topics do parents need to be aware of? (1)
<i>Resources: The WHERE Factor</i>	According to their needs, how should the information be conveyed? Where can we find such information?(3)
<i>Delivery: The WHEN Factor</i>	When should the lessons take place? (2)

From these questions, three components of the adapted framework have emerged:

1) **Parents' needs** which is taken from the WHAT factor. The topics of cyber safety which need emphasis will be determined. We will simultaneously determine what information is necessary for them to be effective teachers, identifiers and advisors as in the WHO factor. Parents' levels of digital literacy, cyber safety awareness and the age of their children will also give an indication of their needs.

2) **Presentation Type** which inspired from the WHEN factor. Parents will tell when and in which format (videos, parents' meetings, online information or books) they would like to receive the information.

3) **Content** which is taken from the WHAT and CONTOL factors. We will be categorising and evaluating existing available content. We will also find out existing policies from the school and include it in the framework to make sure that the parents are aware of these rules and policies to know which role they play as in the CONTROL factor.

The components illustrated in Figure 2 below are interconnected and require equal attention.

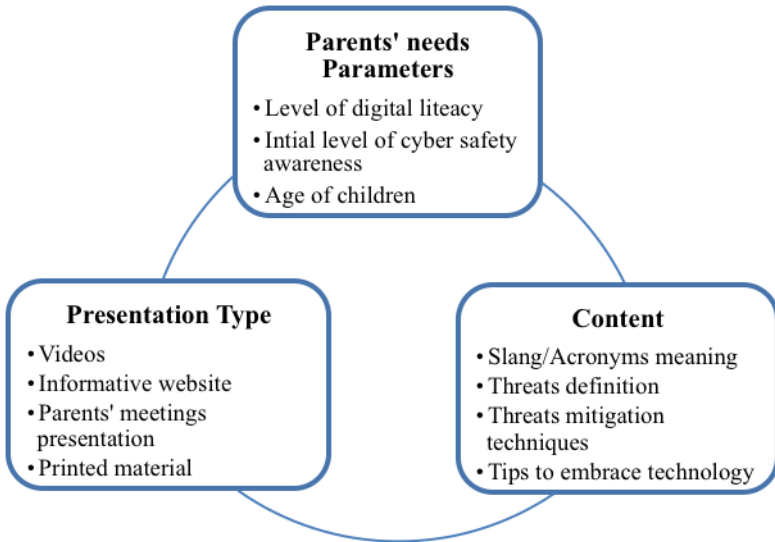


Figure 3 - Suggested Parents cyber safety awareness Framework

Each of these elements is discussed below.

4.1. Determining parents' needs

The questionnaire will be divided into three parts to match the components of the framework. Open-ended questions will be included in the questionnaire to make sure that parents have the option to share other topics with us as well.

The first part will help determine the level of digital literacy parents have according to the definition of digital literacy provided earlier. It will contribute to determining

their skills in using digital devices as well as finding and assessing online information.

The second part will focus on the parents' level of awareness of cyber safety threats and concepts as well as to what extent the school shares informational material. This will be to determine their information needs regarding cyber safety topics and in which depth they should be discussed.

The last part of the questionnaire will try to establish the parents' preference regarding information sharing of cyber safety material. Here we refer to options such as workshops, formal lectures, websites, newsletters, etc. Also, in this part, we would like to establish if they are aware of the role they should play in the cyber safety education of their children and if they know of any policies or rules that the school has concerning cyber safety.

4.2. Understanding Cyber Safety Content

Depending on the dissemination formats, there is a significant number of resources available for parents to enhance their cyber safety awareness. Von Solms and von Solms (2014) have contributed to the body of knowledge by categorising available videos according to the age of the children and their specific information needs. They have chosen to focus on Open Educational Resources (OER) because they can help African schools and houses with limited infrastructures to access a quality content. OER are advantageous because they are free. No budget needs to be organised to access the material. They do not require the creation of a specific account to access their content. The content, which covers a vast range of subjects is adapted to age ranges and is kept up to date. When searching for usable content, one needs to take these previously stated criteria in consideration.

The same should be done for parents: Content should be divided by the age of target groups as well as the levels of digital literacy. It will ensure that parents receive content adapted to the age of their children.

The formats of the resources shared need to be carefully chosen according to the audience. An example is using cartoon videos to explain specific topics to raise awareness among primary school children (von Solms et al., 2014). From the questionnaire's answers, the appropriate dissemination format for parents will be established.

5. Conclusion

This paper proposes a cyber safety information framework for parents. Its components need to be taken into consideration to produce relevant material adapted to parents. Parents' information needs should be established as well as the format in which they would like the information to be disseminated. Then they should be directed to where to find their needed information. This is research in progress and

the next step is to continue with the development of the framework. We believe that this framework will prove useful to schools as well as service providers of e-learning solutions.

6. References

- Australian Communications and Media Authority, 2015. *Parents' guide to online safety*. [Online]
Available at:
http://www.cybersmart.gov.au/~media/Cybersmart/Documents/Documents/Parents_guide_to_online_safety.pdf
[Accessed 05 June 2015].
- Beger, G. & Sinha, A., 2012. *South African Mobile Generation : Study on South African young people on mobiles*, New York: UNICEF.
- Belsey, B., 2006. *Cyberbullying: An Emerging Threat to the "Always On" Generation*. [Online]
Available at:
http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf
[Accessed 16 June 2015].
- Burton, P. & Mutongwizo, T., 2009. Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. *Centre for Justice and Crime Prevention*, Issue 8, pp. 1-12.
- de Lange, M. & von Solms, R., 2012. *An e-Safety Educational Framework in South Africa*. Fancourt, George, SATNAC.
- Duerager, A. & Livingstone, S., 2012. *How can parents support children's internet safety?*, London, UK: EU Kids Online.
- ESHET-ALKALAI, Y., 2004. Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era. *Journal of Educational Multimedia and Hypermedia*, 13(1), pp. 93-106.
- Johnson, L., Adams, S. & Cummins, M., 2012. *The NMC Horizon Report: 2012 Higher Education Edition*. Austin, Texas, The New Media Consortium.
- Kambourakis, G., 2013. Security and Privacy in m-Learning: Challenges and State-of-the-art. *International Journal of u- and e- Science*, 6(3), pp. 67-84.
- Kritzinger, E., 2015. *Enhancing Cyber Safety Awareness among School Children in South Africa through Gaming*. London, UK, Science and Information Conference.
- March, S. T. & Smith, G. F., 1995. Design and Natural Science research on Information technology. *Decision Support Systems*, 15(1995), pp. 151-166.
- Popovac, M. & Leoschut, L., 2012. Cyber bullying in South Africa: impact and responses. *Center for Justice and Crime Prevention*, Issue 13, pp. 1-16.

Pusey, P. & Sadara, W. A., 2011. Cyberethics, Cybersafety, and Cybersecurity. *Journal of Digital Learning in Teacher Education*, 28(2), pp. 82-88.

Sharples, M., 2006. *Big issues in Mobile Learning. Report Of workshop by Kaleidoscope Network of Excellence Mobile Learning Initiative*, Nottingham: Kaleidoscope.

Sonck, N., Livingstone, S., Kuiper, E. & de Haan, J., 2011. *Digital literacy and safety skills*, London, UK: EU Kids Online, London School of Economics & Political Science.

Telstra Corporation Limited, 2014. *Addressing the cyber safety challenge: from risk to resilience*. Sydney: Telstra Corporation Limited.

US Department of Justice, 2006. *Transcript of Attorney General Alberto R. Gonzales' Address to the Employees at the National Center for Missing and Exploited Children*. [Online]

Available at: https://www.justice.gov/archive/ag/speeches/2006/ag_speech_0604202.html
[Accessed 20 March 2016].

Vaishnavi, V. & Kuechler, B., 2004. *Design Science in Information systems*. [Online]

Available at: <http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf>
[Accessed 10 June 2015].

Vaishnavi, V. & Kuechler, W., 2007. *Design science research methods and patterns: innovating information and communication technology*. Boca Raton, FL: Auerbach Publications.

Valcke, M., De Wever, B., Van Keer, H. & Schellens, T., 2011. Long-term study of safe Internet use of young children. *Computers & Education*, Volume 57, pp. 1192-1305.

von Solms, A. & von Solms, R., 2014. *Towards a Cyber Safety Education in Primary schools in Africa*. s.l., HAISA 2014, pp. 185-197.

Youth Online Safety Working Group, 2010. *Interdisciplinary Response to Youth Sexting*, Rohnert Park, CA: s.n.

An approach to managing social media risks within a South African context

Hanifa Abdullah

School of Computing, University of South Africa (UNISA)
abdulh@unisa.ac.za

Abstract

Social media plays a monumental part in most people's personal and professional lives today, dramatically changing how people communicate. Many people are however unable to provide a clear demarcation between their personal and professional lives and often make statements on social media in a private capacity that could have a detrimental impact on one's professional status. The incorrect use of social media has culminated in several legal battles, in South Africa and globally resulting in the unfortunate dismissal of employees for social media misconduct.

Unfortunately, few organisations actually know the risks that come with using social media as a business tool. The absence of knowledge and experience among users can open an organisation to serious risks including disclosure of confidential information, inappropriate intellectual property distribution, employee distraction from fundamental business tasks, reputational damage to the organisation and inapt employee discussions. An inappropriate tweet or Facebook post can cause severe damage to an organisation. In order to manage the risks posed by social media, organisations should conduct a formal risk management exercise. This paper examines the use of the ISO 31000:2009 risk management standard to identify, assess and treat social media risks using a higher education academic institution, namely the University of South Africa (UNISA) for illustrative purposes.

The objective of this paper is to provide a high-level overview of what organisations can do to manage the risks of social media.

Keywords

Social media, risks, risk management, ISO 31000

1. Introduction

The use of social media for communication has grown immensely in the last few years (Wendt and Young, 2011; Delerue and He, 2012) with more than 72 percent of all Internet users regularly accessing social networking sites (Shortstack, 2014). By 2017, the global social network audience is projected to be 2.55 billion (Inc., 2013). According to Chelliah and Field (2014), every minute of every day, 100,000 tweets are sent, 684,478 pieces of content are shared on Facebook, 48 hours of video are uploaded to YouTube, 47,000 apps are downloaded from the App Store, 3,600 photographs are shared on Instagram and 571 websites are created.

Social media are, for many people, obscuring the boundary between work and private life in ways that are “legally complex and difficult to control” (Field and Chelliah, 2012). The incorrect use or abuse of social media has led to several legal battles, in South Africa and around the world where there have been arrests for cybercrimes and employee dismissals for social media misconduct (Davey, 2015). In the case of *Sedick and another v Krisray* presented before the Commission for Conciliation, Mediation and Arbitration (CCMA), the employees, operations manager and bookkeeper of the company were dismissed from work for posting an offensive statement about the owner and a member of his family on Facebook (Polity, 2011). The CCMA found that the employees were fairly dismissed. (Polity, 2011). Mushwana and Bezuidenhout (2014), outline examples of numerous other social media incidents in South Africa.

It is however impractical to restrict the use of social media tools such as Facebook, Twitter and LinkedIn by employees, because many employees (such as marketing staff) need to use social media for work-related activities (Delerue and He, 2012). Among Fortune 500 firms, 77 percent now have active Twitter accounts, 70 percent Facebook pages and 69 percent YouTube accounts (Gesenhues, 2013).

Employees’ participation in social media is vital as they exemplify an organisation’s corporate character and define its reputation by operating as dominant representatives of their organisations as “corporate advocates and brand ambassadors” (Dreher, 2014). However, the supremacy social media gives to employees’ role as “external communicators and brand ambassadors” according to Dreher (2014) does not come without risks that can cause damage to an organisation. Shullich (2011) states that exposure to social media is “considered to be a business risk”.

Organisations have to embrace a proactive risk management strategy to address social media risks before they manifest in unpleasant circumstances. The objective of this paper is therefore, to address social media risks by means of a formal risk management standard applied in a higher education context which for illustrative purposes is the University of South Africa (UNISA). To achieve this objective, this paper is structured as follows: Section 2 provides an overview of the concept of social media, section 3 promotes an understanding of the term risk and risk management, section 4 examines the process for applying the ISO 31000:2009 standard to social media risks and section 5 concludes this paper with reflections on future research.

2. Social media

Social media may be defined as “media designed to be disseminated through social interaction between individuals and entities such as organisations” by using the Internet and web-based technologies to convert broadcast media monologues (one to many) into social media dialogues (many to many) (Botha et al., 2011). Evans

(2012), defines social media as “participatory online media where news, photos, videos and podcasts are made available via social media web sites via submission”.

Social media are distinctive because they are “media rich” and endow users to share their opinions, insights, experiences, content and contacts with friends and family via multiple content forms (Du Plessis, 2010). An interesting aspect of social media lies in the ease of sharing information where the platform renders it possible to make ideas, news and conversation spread rapidly manifesting in an immediacy that can help businesses convey their message quickly, cost effectively and efficiently (Okurumeh and Ukaoha, 2015).

Social media comes in a numerous forms including “bookmarking services like Delicious, Pinterest, and Bib-Sonomy, to 3D Virtual Worlds like Second life, professional networking systems like LinkedIn, Blogging tools like Blogger, microblogging tools like Twitter, collaborative content creation tools such as Wikipedia or Wikispaces, photo sharing services like Flickr and Instagram, profile and friend/social management systems like Facebook and MySpace, video sharing services like YouTube, and micro-video blogging services like Vine” (Buzzetto-More et al., 2015). The world’s two foremost platforms are Twitter, with 230 million monthly active users, and Facebook, with 874 million monthly active users (Sims et al., 2015). According to Davey (2015), the most popular social media platforms for business in South Africa are Twitter, followed by Facebook and YouTube. While social media usage continues to grow locally and internationally because of the supremacy thereof, the risks innate in embracing this trend can never be ignored (Mushwana and Bezuidenhout, 2014).

The following sections therefore promote an overview of social media risks organisations can face by first promoting an understanding of the term risk followed by an overview of risk management and thereafter a discussion of social media risk management.

3. Understanding risk

Dali and Lajtha (2012), broadly define risk as the “effect of uncertainty on objectives” and risk management as “coordinated activities to direct and control an organisation with regard to risk”.

The term “risk” is usually applied in one of three applications, risk as a threat versus exposure, risk as a variance and risk as an opportunity (Program et al., 2012). This study examines risk as a threat versus exposure where risk considered as a threat implies potential negative events that could result in financial or reputational harm to the organisation, whereas risk considered as an exposure could result in positive exposure for the organisation (Program et al., 2012). This study focuses only on risk as a threat in the context of social media risks and does not examine the positive impact of social media exposure.

The use of an efficient, logical, easy to comprehend risk management framework is an innate part of a successful risk management process in organisations (Cardenas Davalos and Chia Chin Hui, 2010). There are several risk management frameworks, standards and guidelines including that of AS/NZS ISO 31000:2009 risk management standard, Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) 2004, the Federation of European Risk Management Associations (FERMA) risk management standard 2004, the Combined Code 2003/Turnbull Guidance 2005, the Association of Insurance and Risk Manager (AIRMIC) risk management standard, the Public Risk Management Association (ALARM) risk management standard, the Institute of Risk Management (IRM) risk management standard and Basel II (Program et al., 2012; Laakso, 2010).

For the purpose of this paper, the ISO 31000:2009 risk management standard (ISO, 2009) is used to assess social media risks because this standard provides a framework for organisations wanting to manage risk “consistently, efficiently and effectively” and provides a widely accepted, standards-based approach that can be applied to decision making (Gjerdrum, 2015; Microsoft, n.d.).

The following section provides an overview of the ISO 31000: 2009 risk management standard (ISO, 2009).

3.1 An overview of the ISO 31000:2009 risk management standard

ISO 31000 (published in the United States as ISO/ANSI/ASSE 31000) is the only international standard for the practice of risk management issued in December 2009 (Gjerdrum, 2015). According to Knight (2010), this standard sets out principles, a framework and a process for managing risk (Figure 1) that is applicable to an organisation of any type. The ISO 31000:2009 risk management process follows the path of the Australian/New Zealand 4360:2004 standard on risk management (Knight, 2010). The principles, framework and process according to Gjerdrum (2015), is the basic “architecture” of risk management, which, if applied, creates a steady and rational basis for managing the effects of uncertainty upon organisational objectives.

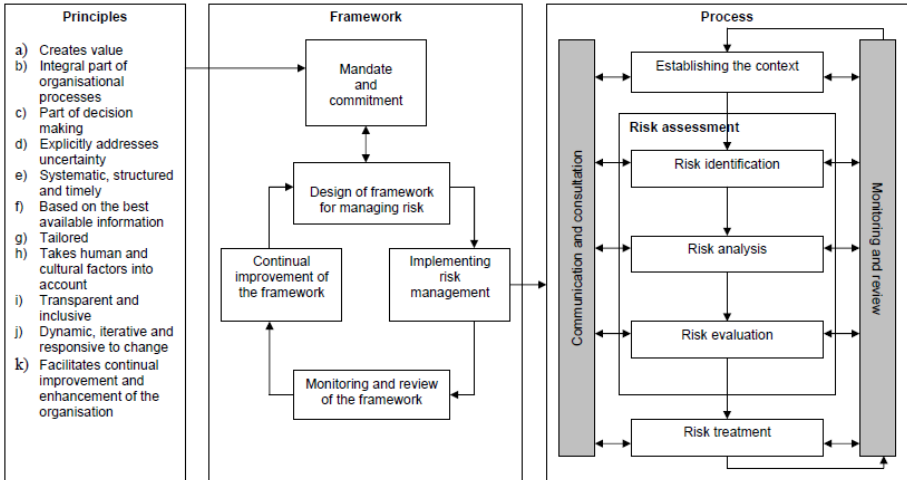


Figure 4: ISO 31000:2009 Relationship between the principles, framework and process (Government, 2011)

The principles provide guidance on the validation for managing risk and the characteristics of effective risk management (Gjerdrum, 2015).

The framework underlines integration of risk management practices throughout the value chain to support corporate decision-making (ISO, 2009). The risk management process is the focus of this research. The following section provides an overview on how the ISO 31000:2009 risk management process can be applied to address social media risks.

4. Application of the ISO 31000:2009 standard applied for social media risks

Knight (2011), aptly illustrates the detail of the risk management process in Figure 2. Each of these components is discussed on a high-level to equip organisations of any type with an understanding of how to address social media risks. This means that the actual risk analysis and evaluation is not discussed in-depth but the process and illustrative examples are provided.

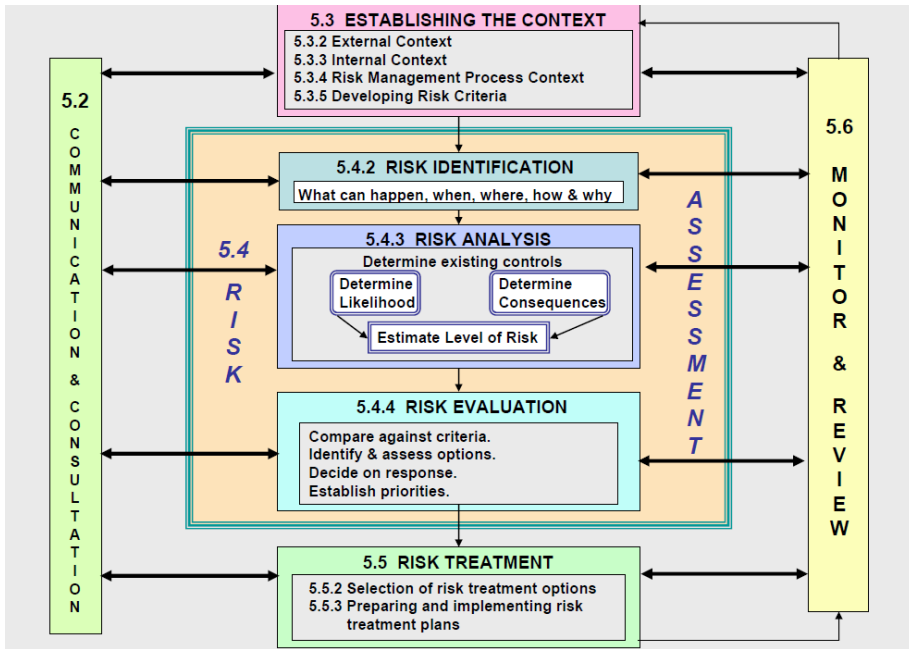


Figure 5: Risk management process in detail (Knight, 2011)

In the above diagram the overarching general processes (5.1, 5.3.1, 5.4.1 and 5.5.1) are not depicted but are explained below:

- 5.1 - This refers to the risk management process which should be a salient part of management, be incorporated within the culture and practices of the organization and streamlined to the business processes of the organization (ISO, 2009). The risk management process comprises activities 5.2 – 5.6 depicted in Figure 2.
- 5.3.1 - This is the general process for establishing the context and includes the organisation defining its objectives, the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the remaining process (ISO, 2009).
- 5.4.1 - This is the general process for risk assessment and includes risk identification, risk analysis and risk evaluation (ISO, 2009).
- 5.5.1 - This is the general process of risk treatment and includes selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls (ISO, 2009).

The following sections provide an overview of the risk management process.

The ISO 31000 standard defines the communication and consultation step as the continual and iterative processes that an organisation conducts in order to provide, share and obtain information as well as engage in conversations with relevant stakeholders regarding the management of risk (ISO, 2009).

4.2 Establish the context

By establishing the context, the organisation stipulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process (ISO, 2009).

The context for this study is an Open Distance Learning (ODL) institution, namely the University of South Africa (UNISA). UNISA (2008), defines ODL as “a multi-dimensional concept aimed at bridging the time, geographical, economic, social, educational and communication distance between student and institution, student and academics, student and courseware and student and peers.” The objective of the institution is to promote learning where learning is defined as “an active process of construction of knowledge, attitudes and values as well as developing skills using a variety of resources including people, printed material, electronic media, experiential and work-integrated learning, practical training, reflection, research, etc.” (UNISA, 2008). Since the focus on this paper is on social media, learning is examined in the context of electronic media, commonly defined as e-learning.

According to the UNISA curriculum policy (UNISA, 2010), e-learning “is learning facilitated by means of the use of ICT social technologies, communication technologies, online learning platforms and other multimedia devices”. To facilitate e-learning, the university supports a number of technology initiatives. Asynchronous technologies supported by the university include wikis, blogs, social networking facilities and e-portfolios (UNISA, 2008).

The stakeholders that are impacted include the academics and students who are at this stage bound to use the internal environment of the University which is the myUnisa learning management system to promote e-learning. This system allows academics to make use of only basic social media tools including Wikis and Blogs. Policies which academics need to be conversant include the ODL Policy and Curriculum Policy of the University. Furthermore, the roles of academics to promote e-learning must be considered as part of the internal environment.

Influences on the external environment relate to the social, cultural, political, legal, regulatory, financial, technological and economic environments within which the University operates (ISO, 2009). As an example, one can consider the social media laws of the country. It is important to consider these laws in the event an employee takes legal recourse against the University. In South Africa there is no legislation dealing specifically and explicitly with social media but the laws applicable to social media are obtained in a variety of other statutes and the common law including the Constitution of the Republic of South Africa Amendment Act, No. 108 of 1996; the

Labour Relations Act, No. 66 of 1995; the Code of Good Practice in the Labour Relations Act, No. 68 of 2008, the Electronic Communications and Transactions Act, No. 25 of 2002, the Regulation of Interception of Communications and Provision of Communication-related Information Act, No. 70 of 2002 and the Trade Marks Act, No. 194 of 1993 (Mushwana and Bezuidenhout, 2014).

Additionally, cognisance must be taken of the impact of the Protection of Personal Information Act (POPI) Act, South Africa's data protection legislation on social media. The greatest impact of POPI on social media activities is that any and all information collected via social channels will be governed by POPI just like all other customer information (Cerebra, 2014).

POPI warns all South Africans that the Act only protects one's private information, and any information shared publicly will automatically fall outside of the Act's protection (Cerebra, 2014). An example of this is sharing one's email address or telephone number on a Facebook page, rendering this information publicly available for companies to collect and use (Cerebra, 2014).

Defining risk criteria is another aspect of establishing the context for the risk assessment. This entails preparing likelihood and consequence scales and their combination into a risk matrix to determine the level of risk (Rollason et al., 2010). Another important aspect of risk criteria according to Rollason et al. (2010) is describing the level at which risk is deemed acceptable, tolerable and intolerable, with intolerable risks requiring treatment as a priority. Table 1 illustrates an example of a simple risk matrix.

	CONSEQUENCE		
LIKELIHOOD	Minor	Moderate	Significant
Unlikely	Low	Low	Medium
Possible	Low	Medium	High
Likely	Medium	High	High

Table 7: Simple risk matrix example

Having established the risk context, the next step is risk assessment which encompasses the process of risk identification, risk analysis and risk evaluation (ISO, 2009).

4.3 Identify the Risks

Risk identification encompasses a systematic process to understand what could happen, how, when, and why (Purdy, 2010).

Examples of social media risks that could manifest include reputational damage to an employer, breach of confidentiality, time wasting, third party liability, cyber bullying and ownership of social media accounts (Michalson, 2011). In the context of the University scenario, employees could use social media technologies such as Facebook to post derogatory comments about the institution resulting in reputational damage to the University. An example of this could be posting information about the incompetence of certain members of staff and management, haphazard manner of setting examination papers, poor administrative assistance to students in terms of registration and lack of quality assurance on tutorial matter.

Additional examples of social media risks include excessive use of social media during work hours resulting in lack of productivity at work, failure to use social-media marketing for fear of destructive exposure, setting up a LinkedIn group in an employee’s name and taking this group to a competitor when the employee leaves and posting of sensitive or confidential information to a social-media site (Field and Chelliah, 2012). All of these risks are applicable to the University environment. Posting of sensitive information could include posting of examination questions, examination results or even the financial status of the University by disgruntled employees.

Andreesen and Slemp (2011) succinctly short-list social media risks as Intellectual Property (IP)/Sensitive Data Loss, Compliance Violations, Reputational Loss,

Financial Loss, Safety Loss and Personal Reputation Loss. All of these risks are applicable to the UNISA context.

4.4 Analyse the Risks

In ISO 31000:2009, risk analysis is concerned with comprehending each risk, its consequences, and the likelihood of those consequences (Purdy, 2010). This information is used as an input when evaluating the risk and deciding whether risk response or treatment is necessary. A common approach for analysing risk is through the use of the risk matrix developed in the ‘establishing the context’ section.

Prior to investigating new measures, the existing controls or measures in place that may reduce the level of risk are evaluated (Rollason et al., 2010). In terms of the University scenario, UNISA already has a comprehensive social media guideline (UNISA, 2011) in place.

According to the UNISA social media guideline, social media “encompasses a variety of services delivered via the Internet and mobile platforms, including video, image or podcast hosts, instant messaging sites or chat rooms, wikis, blogs and online discussion forums”(UNISA, 2011). UNISA’s social media guidelines distinguish between private and business use scenarios for both students and employees. The private use of social media covers aspects such as identification of association with UNISA, disclaimer, use of the UNISA logo and other branding elements and respect of University time and property. The business use of social media addresses appropriate and inappropriate use of social media, notification obligation whereby employees should seek departmental or directorate permission before creating an online presence that represents UNISA business, including teaching, discipline or research-oriented initiatives, identification of or association with UNISA, branding and use of the UNISA name and logo, transparency and responsibility when participating on a social media site, reporting of non-compliance by providing UNISA’s contact centre’s e-mail address in all official social media sites for registration of complaints and monitoring of the official UNISA Facebook and Twitter Sites (UNISA, 2011).

Thus, there is some measure to address social media risks but an analysis must be done for each type of risk. For example reputational risk could manifest in negative consequences and the likelihood of this is very high.

4.5 Evaluate the Risks

In the risk evaluation phase, the results from the risk analysis are compared with risk criteria established when setting the context in order to ascertain if the risk level is acceptable or not. This facilitates in decision making regarding which risks need treatment as well as their priority (ISO, 2009). In the above example, it was

ascertained that reputational risk has a very high likelihood meaning that this risk must be treated.

4.6 Risk Treatment

The risk treatment phase concerns how to deal with social media risks that are not acceptable. Risk treatment is the process whereby existing controls are improved or new controls are developed and implemented (Purdy, 2010). Risk treatment selects the appropriate options for treating or modifying risks. Such options include: acceptance of risk to recognise competitive advantages; avoidance of risk by not carrying out the activity; reduction or removal of the impact or probability of the risk; or distribution of the risk by sharing or transferring the risk (Curkovic et al., 2013). In the example of the University, the most likely risk treatment would be risk mitigation. The following list provides treatment measure for all types of risk assuming they have a high likelihood with negative consequences.

To mitigate social media risks the following measures must be enforced (Dreher, 2014; Delerue and He, 2012; Dreyer et al., 2009; Field and Chelliah, 2012).

- Develop a formal policy to guide employees on the acceptable use of social media (Chi, 2011). UNISA already has a comprehensive social media guideline so this control is in place.
- Monitor the social web to know what people are saying about their organisations and respond accordingly. This is clearly espoused in the social media guideline of the University. UNISA's ICT may perform activities necessary to ensure the integrity, functionality and security of the university's systems (UNISA Internet, Electronic Communication and Web Management Policy, section 7: Right to Monitor) (UNISA, 2011).
- Provide education on legal issues like copyright and anti-trust as well as on social media principles. Organisations need to provide security awareness training to employees. Security awareness training should entail education on the organisation's social media acceptable use and security policy, examples of social media attacks, and proper precautions to mitigate the security threats and risks as well as the reporting of security incidents. Both personal use and business use of social media in the workplace and outside the workplace need to be mentioned in user education and training. This is something that is seriously lacking in the University as employees have very little to no knowledge on the acceptable and unacceptable use of social media as there is very little awareness or training regarding this issue.
- Update insurance policies to provide coverage for your social media work. This must be handled by management.

- Archive social media content: As employees are retrieving and sharing information on platforms such as Facebook, Twitter and LinkedIn, some organisations capture and preserve the social media content and information for legal and compliance purposes. Automated tools such as Symantec's Enterprise Vault archiving software help organisations to capture, extract and store social media information posted by employees. This is something management should take cognisance of.
- Develop a social media incident notification and response plan: Social media incidents may still occur notwithstanding security efforts. It is necessary for organisations to develop a social media incident notification and response plan to reduce or minimise negative effects of an incident. This is something management should take cognisance of.
- Have clearly defined internal-grievance procedures, forceful record-keeping procedures to document staff training in the organisation's policies and the employee's knowledge of these policies, and discipline and termination procedures to ensure that when the social-media event occurs, management is well versed to manage the situation fairly. Some of these controls procedures are embedded within the social media policy of the University. For example, the social media guidelines states that the following policies and guidelines must be read in conjunction with the social media guidelines: Internet, Electronic Communication and Web Management Policy and Guidelines, UNISA Code of Ethics and Conduct, Copyright Infringement and Plagiarism Policy, Student Disciplinary Code and Employee Disciplinary Code (UNISA, 2011). What is lacking is procedures to document staff training.

Monitoring and review is necessary so that action is taken to address new social media risks as they emerge and existing risks as a result of changes in the organisation's objectives or the internal and external environment in which they examined (Purdy, 2010).

Thus the above process provides an overview of how to formally manage social media risks and also outlines the present position of the University in managing social media risks.

5 Conclusion and Future research

This paper presents the case for the adoption of risk management of social media using UNISA as the context for the research. This paper described the process of the ISO 31000:2009 risk management standard for mitigating social media risks within a University context. Future research will encompass conducting the entire ISO 31000:2009 risk management process including the principles, framework and detailed process for social media risks. The objective of this paper was to present a very high-level overview of how social media risks can be managed. Since the ISO 31000:2009 standard is an extremely detailed and in-depth standard, this paper

provided an extremely high level overview of the potential of this standard in addressing risks so that organisations can embark on a formal process in future.

6 References

- Andreesen, T. & Slempe, C. (2011), "Managing risk in a social media-driven society": Protiviti, <https://www.protiviti.com/en-US/Documents/Insights/Managing-Risk-in-a-Social-Media-Driven-Society.pdf>, (Accessed 15th April 2016).
- Botha, E., Farshid, M. & Pitt, L. (2011), "How sociable? An exploratory study of university brand visibility in social media", *South African Journal of Business Management*, Vol. (42),No. 2, pp. 15-23.
- Buzzetto-More, N. A., Johnson, R. & Elobaid, M. (2015), "Communicating and sharing in the semantic web: an examination of social media risks, consequences, and attitudinal awareness", *Interdisciplinary Journal of e-Skills and Lifelong Learning*, Vol. (11),No., pp. 47-67.
- Cardenas Davalos, A. D. & Chia Chin Hui, W. (2010), "How is risk assessment performed in international technology projects", Vol.,No.
- Cerebra. (2014), "The impact of POPI on Social Media in South Africa", <http://www.cerebra.co.za/resources/impact-popi-social-media-south-africa/>, (Accessed 17th June 2016).
- Chelliah, J. & Field, J. (2014), "Managing the risks of social media: Ways to ensure that online behavior is always appropriate", *Human Resource Management International Digest*, Vol. (22),No. 5, pp. 39-41.
- Chi, M. (2011), "Security Policy and Social Media Use": The SANS Institute, (Accessed 11th March 2016).
- Curkovic, S., Scannell, T. & Wagner, B. (2013), "ISO 31000: 2009 Enterprise and Supply Chain Risk Management: A Longitudinal Study", *American Journal of Industrial and Business Management*, Vol. (3),No. 07, pp. 614.
- Dali, A. & Lajtha, C. (2012), "ISO 31000 Risk Management—"The Gold Standard"", *EDPACS*, Vol. (45),No. 5, pp. 1-8.
- Davey, R. (2015), "Firms need social media policy for staff", <http://www.bowman.co.za/FileBrowser/ArticleDocuments/Firms-need-social-media-policy-for-staff.pdf>, (Accessed 10th May 2015).
- Delerue, H. & He, W. (2012), "A review of social media security risks and mitigation techniques", *Journal of Systems and Information Technology*, Vol. (14),No. 2, pp. 171-180.
- Dreher, S. (2014), "Social media and the world of work: A strategic approach to employees' participation in social media", *Corporate Communications: An International Journal*, Vol. (19),No. 4, pp. 344-356.

Dreyer, L., Grant, M. & White, L. T. (2009), "Social Media, Risk, and Policies for Associations", <http://www.socialfish.org/wp-content/downloads/socialfish-policies-whitepaper.pdf>, (Accessed 30th May 2016).

Du Plessis, T. (2010), "Theoretical guidelines for social media marketing communication", *Communicare: Journal for Communication Sciences in Southern Africa*= *Communicare: Tydskrif vir Kommunikasiewetenskappe in Suider-Afrika*, Vol. (29),No. 1, pp. 1-20.

Evans, D. (2012) *Social media marketing: An hour a day*, John Wiley & Sons, International Standard Book Number: 1118240545.

Field, J. & Chelliah, J. (2012), "Social-media misuse a ticking time-bomb for employers: Robust policies and procedures needed to reduce the risks", *Human Resource Management International Digest*, Vol. (20),No. 7, pp. 36-38.

Gesenhues, A. (2013), "Social Media Use Growing Among Fortune 500 List With 77% Tweeting & 70% On Facebook", <http://marketingland.com/fortune-500-companys-social-media-use-on-the-rise-52726>, (Accessed 12th April 2016).

Gjerdrum, D. (2015), "Risk Management's Standard of Practice – An Overview of ISO 31000", <http://www.ajg.com/media/1697375/overview-of-iso-31000-2015.pdf>, (Accessed 11th March 2016).

Government, Q. (2011), "A Guide to Risk Management", <https://www.treasury.qld.gov.au/publications-resources/risk-management-guide/guide-to-risk-management.pdf>, (Accessed 2016 12th April).

Inc., e. (2013), "Social Networking Reaches Nearly One in Four Around the World,"", <http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976>, (Accessed 7th June 2016).

ISO. (2009) ISO 31000:2009, Risk Management—Principles and Guidelines. Geneva.

Knight, K. W. (2010), "AS/NZS ISO 31000: 2009-the New Standard for Managing Risk", *Keeping good companies*, Vol. (62),No. 2, pp. 68.

Knight, K. W. (2011), "Applying ISO 31000:2009 in Regulatory Work", Australia, http://www.unece.org/fileadmin/DAM/trade/wp6/ExtendedBureauMeetings/2011_May/ApplyIngISO3100inRegulatoryWork.pdf, (Accessed 14th June 2016).

Laakso, P. (2010), "ERM-from Risk Management to Leading the Opportunities", Vol.,No.

Michalson, L. (2011), Legal Risks posed by Social Media. *Social Media Law* [Online]. Available from: <http://www.michalsons.co.za/blog/legal-risks-posed-by-social-media/9067> [Accessed 4th April 2016].

Microsoft. (n.d.), "Assessing compliance & risk for cloud computing deployments", <http://az370354.vo.msecnd.net/publicsector/government/MIC0675%20Cloud%20Field%20Booklet%20A4%20S6R1.pdf>, (Accessed 14th April 2016).

Mushwana, G. F. & Bezuidenhout, H. C. (2014), "Social media policy in South Africa", Vol.,No.

Okurumeh, O. & Ukaoha, K. (2015), "Information security issues surrounding use of social media networks in organizations: an appraisal", *Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS)*, Vol. (6),No. 3, pp. 227-232.

Polity. (2011), "What you say on Facebook can get you fired", <http://www.polity.org.za/article/what-you-say-on-facebook-can-get-you-fired-2011-11-07>, (Accessed 11th February 2016).

Program, A. C. R., Administration, U. S. F. A., Consulting, M. R., Corporation, H. & Direct Effect Solutions, I. (2012) *Application of Enterprise Risk Management at Airports* (Vol. 74), Transportation Research Board, International Standard Book Number: 0309258510.

Purdy, G. (2010), "ISO 31000: 2009—setting a new standard for risk management", *Risk analysis*, Vol. (30),No. 6, pp. 881-886.

Rollason, V., Fisk, G. & Haines, P. (2010) Applying the ISO 31000 Risk Assessment Framework to coastal zone management. In: Proceedings of the 19th NSW Coastal Conference, 2010. 10-12.

Shortstack. (2014), "The Growth of Social Media in 2014:40+ Surprising Stats [Infographic]", <http://www.socialystacked.com/2014/01/the-growth-of-social-media-in-2014-40-surprising-stats-infographic/#sthash.t4GoW1Bc.KxNuUnDR.dpbs>, (Accessed 15h May 2016).

Shullich, R. (2011), "Risk Assessment of Social Media", Swansea, UK.: The SANS Institute, (Accessed 11th June 2016).

Sims, K., Weber, E., Bhaduri, B., Thakur, G. & Resseguie, D. (2015) Application of Social Media Data to High Resolution Mapping of a Special Event Population. In: Proc. 13th Int. Conf. GeoComp, 2015.

UNISA. (2008) Open distance learning policy.

UNISA. (2010) Curriculum Policy.

UNISA. (2011) UNISA Social Media Guidelines.

Wendt, J. T. & Young, P. C. (2011), "Reputational risk and social media", *Miss. Sports L. Rev.*, Vol. (1),No., pp. 97.

Digital divide, the role of awareness in the use/non-use of the Internet: the experience of South African developing communities

Emilia Mwim
University of South Africa
mwimen@unisa.ac.za

Elmarie Kritzinger
University of South Africa
Kritze@unisa.ac.za

Abstract

Efforts have been made by researchers to comprehend the nature and factors that contribute to the digital divide in developing countries and several attempts have been made to bridge this divide. Literature mostly investigates Internet non-use in relation to lack of access to information and communication technology (ICT), lack of skills on the use of the Internet and the informed decision to reject the use of the Internet. There is rarely any literature on the effect of the "awareness factor" in the digital divide on developing communities in South Africa. This paper focuses on Internet non-use resulting from a lack of awareness of Internet benefits among people living in developing communities in Gauteng, South Africa. A survey was conducted in four developing communities in Gauteng, South Africa, among three Internet-user types namely: Current-users; Lapsed-users; and Non-users. The survey was conducted to determine the participants' level of awareness of the Internet benefits and to investigate the influence of awareness on their use/non-use of the Internet. The result of this research shows that non-users lack awareness of most benefits of the Internet and this affects their non-use of the Internet in comparison to current-users and lapsed-users. Employment status was also identified to have some influence on participant non-use of the Internet. Some respondents do not make use of the Internet due to lack of awareness of some of the essential benefits of Internet.

Keywords

Awareness, developing communities, digital divide, Internet, user-type, South Africa

1. Introduction

The Internet has the capacity to have a tremendous transformational impact on society and commerce (Kelly, Kennedy, Britton, McGuire, & Law 2016). For years it has been accepted as an essential mechanism for transforming various aspects of

human life, for instance in the medical, social and economic spheres (Baker et al, 2003; Chavula, 2013). Around the globe, the Internet is considered an important aspect of people's lives and it continues to transform the way people work, socialize, as well as how they discover and share information (Lange et al, 2012). Although it is difficult to predict its evolution, research shows also that the Internet has a tremendous effect on the way human beings resolve their educational, social and economic desires (Harris, 2015).

Human beings in this "information age" experience diversified information needs in their daily lives and the ability to realize those needs depends on their level of knowledge, awareness and use of the Internet (Reitz, 2010, Ting 2014). The Internet contains information, which is considered a vital resource that is necessary for realization of people's desire and improvement of their lives (Mtega, 2012). The information offered by the Internet plays a vital role in social equality, human development and successful socio-economic improvement of any community (Weiss, 2011; Oyedemi, 2015). Therefore, the use of the Internet, as a source of obtaining information, is relevant for the realisation of human needs and it has become progressively more popular as more people go online. The importance and the role of the Internet in the lives of people have become a social reality (Selwyn, 2003; Alam & Imran 2015). However, in order to enjoy the enormous benefits offered by the Internet, a person must be aware of such benefits and consequently participate in the use of the Internet (Dodge, & Kitchin, 2001; Talmud, & Mesch, 2003). Study available on the impact of awareness on the use/non-use of the Internet in rural communities was conducted outside the context of Africa (Ting, 2016). The current research however presents a unique South African perspective on the factor of awareness.

This research therefore investigated the role of awareness of Internet benefits on the use/non-use of Internet among three user-type groups (current, lapsed & non-Internet users) in South Africa developing communities. In this research, the term "developing community" includes township and location which is referred to as informal settlement or semi-rural area according to (Housing development Agency (HAD), 2012; Oyedemi, 2015). The research also investigated the variables that influence perceptions on the impact of awareness on the use/non-use of the Internet. Although the investigated communities are not completely a representatives of all the developing communities in South Africa, the fact that they all have similar structural decompositions and do not fall within the urban/cities areas makes the communities relevant to this research.

2. Literature review

2.1. The Internet and digital divide

As Internet penetration in developed countries begins to expand, the interest in the digital divide, in relation to access to the Internet, has declined and is no longer form the main object of debate (Helsper, 2008; van Deursen, 2010; Helsper & Reisdorf, 2013). There has been a shift in research focus, from an interest in Internet penetration to more of a focus on patterns of Internet usage, including the higher order digital inequalities that exist, which influences the realization of the benefits of the Internet in society, skills, and awareness (Hargittai, 2002, 2008, 2010; Helsper & Reisdorf, 2013 Zillien, & Hargittai, 2009; Wei, & Hindman, 2011; Van Deursen, & Van Dijk, 2014; Ting, 2016. There are few studies on non-users of the Internet (Ting, 2016 and the majority of these studies focus on the demographics of non-users, inequality in physical access, skills, and attitudinal factors that influence adoption behaviour (Selwyn, 2003, 2006; Verdegem, & Verhoest, 2009; Helsper, & Reisdorf, 2013; Alam & Imran, 2015).

Studies on Internet usage in South Africa indicates that there has been an increase in the number of people that can access the Internet, particularly because access can now also be gained through the use of mobile phones (Lewis, 2005; Kreutzer, 2009; Longe et al, 2009). Internet penetration in South Africa has flourished in the past few years, particularly with regard to mobile access and use (Lewis, 2005; Kreutzer, 2009; Longe et al, 2009; Insight Africa, 2012). However, research has shown that the digital divide is still a problem in developing countries and that more effort is required, particularly in Africa to minimize this problem (Kouadio, 2008; Penard et al, 2015). Research also demonstrates that non-use of the Internet in South Africa is an issue that affects particularly people living in rural areas and informal settlements (Beger et al, 2012; Oyedemi, 2012, 2015). In the same vein, recent research and findings, by Ting (2014) also indicate that there are still large populations of non-users of the Internet (Ting, 2016 resulting in digital divide.

The origin of digital divide dates back to the mid-1990s (Srinuan & Bohlin 2011) and since then, has become a popular area of interdisciplinary concern (Hacker, & Van Dijk, 2000; Srinuan & Bohlin, 2011;). Though the term digital divide is considered one of the most discussed social phenomena, it still remains indistinct due to many underpinning factors (Gunkel, 2003). Due to its impact on society and on

economic development (Alam & Imran, 2015; Harris, 2015), the digital divide is still recognised as an important research topic (Srinuan, & Bohlin, 2011).

It is also a polysemous concept with multiple meanings (Bornman, 2016). Though there is no universally accepted definition of the term Digital Divide, many of the widely accepted definitions share a common origin (Gebremichael & Jackson, 2006). Various researchers view the concept of the digital divide differently and thus their definition of the concept varies (Mwim & Kritzinger, 2016). Some researchers define the digital divide as a gap in access to computer device while others defines it as a divide in terms of access or no access to ICT device or the Internet (Belden, 2004; Ferro, Helbig, & Gil-Garcia, 2011). The term digital divide is defined in this research as an inequality in access to ICT device and the Internet that exist between countries, individuals, households, businesses and geographic areas at different socio-economic levels (oecd, 2001; Srinuan & Bohlin; Mwim & Kritzinger, 2016). This definition was adopted in this research because the researchers believe that the digital divide is gap that exists in both the computer itself and the Internet (Information and device view). Thus, the divide can exist within the two digital aspects, namely in the information and communication technology (ICT) devices on the one hand and the Internet on the other.

Digital divide or digital inequality as well as Internet non-use is still a global problem. However, this research tackled the problem of digital inequality from South African perspective. The terms digital divide and digital inequality are used interchangeably in this research.

Many people living in South Africa developing communities still do not use the Internet due to limited Internet access among other factors (Oyedemi, 2015). As a result therefore, people experience the effects of digital inequality and miss out on the benefits of the Internet. Research shows that the use of the Internet has a clear potential for improved quality of life and social inclusion among users (Oyedemi, 2015; Kelly, Kennedy & Britton, McGuire & Law, 2016). InternetInternet.

2.2. Awareness: a factors of digital divide

The use of the Internet offers potential for improved human development. It supports social inclusion, improves quality of life, and facilitates communication as well as

self-management, however significant barriers regarding distribution of the Internet still exist (Alam & Imran, 2015; Kelly et al, 2015). The unequal distribution of the Internet is caused by economic and non-economic factors which have been discussed in a wide range of literature (Oyedemi, 2015; van Deursen & van Dijk, 2014; Fuchs, & Horak, 2008; Kouadio, 2008; Haseloff, 2005). Awareness was identified as one of the underlying factors affecting the level of the Internet non-use in developing communities (Ting, 2016). Other factors that may impact on the Internet usage and connectivity include language, access and skill.

The majority of literature on factors of digital divide in developing countries has focused on bridging the access and skills divide in relation to the usage pattern of information technology (Oyedemi, 2015; Fuchs, & Horak, 2008; Kouadio, 2008; Akinsola et al, 2005;). Notwithstanding the immense body of research on the digital divide, as well as on digital exclusion, study on 'non-user' tends to be an exception (Ting, 2016). There has not been an extensive research that focuses on non-users' demographics and the attitudinal factors that affects adoption behaviours towards the use of the Internet (Ting, 2016). Some of the studies conducted in the area of 'non-use' focus on non-users' self-reported reasons for staying offline, with particular reference to access and skills (Verdegem, & Verhoest, 2009; Selwyn, 2006). Other studies on non-use of the Internet identified some demographic and personal factors that contribute to 'non-use' of the Internet for example in Britain (Helsper, & Reisdorf, 2013) which outside the continent of Africa.

It is revealed that those individuals who have never used the Internet are most likely to cite lack of need as the reason for 'non-use', while the ex-users of the Internet are likely to refer to cost and access as inhibiting factors (Helsper, & Reisdorf, 2013). Though recent literature is beginning to move away from the exclusion barriers, namely access and skills, to accommodate other factors contributing to the digital divide (Ting, 2016, there has not been any evidence in the literature on the awareness divide in developing country like South Africa. Therefore, this research investigates the role of awareness of the Internet benefits on the 'non-use' of the Internet in South African developing communities.

In order to achieve the objective of the research, the following research questions were asked:

Does awareness of Internet benefits have an impact on the use of the Internet in South African developing communities? And if the answer is "Yes" what factors

cause awareness of Internet benefits to be viewed as problematic?” The methodology employed in answering these research questions is discussed in the next section.

3. Research methodology

The research strategy used for data collection in this study was surveys. The survey was conducted with 173 participants in four developing communities in Gauteng, South Africa. The four communities where data was collected are: Attredgeville and Soshanguve which are located to the west and north of Pretoria; and Diepsloot and Tembisa located to the north of Johannesburg. The communities are summarised in table 1.

Table 1: Summary of the data collected communities

Developing community	Province	City
Diepsloot	Gauteng, South Africa	Johannesburg
Tembisa	Gauteng, South Africa	Johannesburg
Soshanguve	Gauteng, South Africa	Pretoria
Attredgeville	Gauteng, South Africa	Pretoria

A combination of two types of sampling, namely cluster sampling and random sampling, were used in selecting the developing communities. The two methods of sampling are referred to as probability sampling (Oates, 2006). Probability sampling was chosen in this research because, according to Manion (1994), non-probability samples are not suitable for describing a population (Manion, 1994). The choice of the province and communities was based on the following reasons: (1) According to the 2012 report by the Housing Development Agency (HAD) on the informal settlement status in South Africa, Gauteng is the province with the second highest (76%) number of households living in informal settlement (HAD, 2012). (2) Due to time and financial constraints, the researcher focused only on the four selected

communities in the province. (3) Gauteng is the province where the researcher resides.

The population of this research consists of mature people (consisting of anybody, both male and female from 18 years of age) residing in the specified developing communities in Gauteng Province. The participants were either current, reluctant or non-Internet users. The survey was conducted using questionnaires which were physically distributed in the communities where data was collected.

To ensure the validity of the data collected in this research, the questions used in the questionnaires were carefully designed and constructed with the help of literatures that have measured the perceived benefits of the Internet (Bonfadelli, 2002, Hargittai, 2010, Hsieh, et al, 2008 & Venkatesh & Brown, 2001) and the role of awareness on the use/non-use of the Internet (Ting, 2016. For comprehensibility of the questionnaire used in measuring awareness, Ting (2014) broke down the perceived benefits of the Internet to include: facilitation of learning, work or study; online transactions; obtain/search general information; maintaining contact; and entertainment (Ting, 2016. Since this research also investigated the role of awareness (though in a different context) as a factor of digital divide on the non-use of the Internet, the questionnaire were designed based on Ting (2014) specified items of perceived Internet benefits by asking questions to determine if the respondents were aware of each of the benefits.

The questions used in the questionnaire were simplified in order to match the different levels of respondents' reading skills and their levels of comprehension of English. The data collection process also required a lot of monitoring to accommodate various users. The respondents were given reasonable assistance while completing the questionnaire, in case they wanted some clarity. The rigorous processes followed in collecting the data and amount of time spent in assisting the respondents contributed to low number of questionnaires completed.

To test the internal consistency reliability of the research instrument, a Cronbach alpha coefficient is calculated. Cronbach alpha coefficients serve as indicator of internal consistency reliability. It is calculated to ensure that an instrument measures what is supposed to be measured. Cronbach alpha values vary between 0 and 1.0 and a value in the range of 0.7 or greater indicates acceptable level of internal consistency reliability. The standardised Cronbach alpha value for the awareness section of the questionnaire is 0.81.

A quantitative data analysis is employed on the collected data using SPSS statistical software. The strength of quantitative data analysis is that it allows generalizability and is reliable.

The researcher obtained a permission to conduct this research by submitting a written application to the necessary authority and an ethical approval certificate was awarded. Informed Consent letter was used to inform the participants of the research purpose and also to inform them of their rights.

The fact that the questionnaire used for data collection was not translated into the mother tongues of the participants could be considered a limitation in this research. The researcher did not use the translated version of the questionnaire because she was of the impression that the meaning of the questions would change and she will find it difficult understanding or explaining the translated version.

4. Results

The results of the data-analysis and interpretation thereof are discussed in the remainder of the paper. This section starts with a summary of the demographic information of the respondents, followed by the results of participants' awareness of the different Internet benefits measured. Finally analysis of variance were used to present the statistical significant of the research.

4.1. Demographic information of the respondents

Demographic information helps in forming a picture of the profile of the respondents who participated in the research. Table 2 presents the demographic information of the respondents referring to user-type, gender, age, employment status and areas/communities.

Table 2: Biographic description of the respondents

Community respondents by User type, gender, age, employment status and area	
User type	
Current users	35%
Lapsed users	6%
Non-users	59%
Gender	
Male	53%
Female	47%
Age	
18-29	31%
30-39	28%
40-49	30%
50+	11%
Employment status	
Full-time	58%
Part-time	14%
Non-employed	28%
Area/Communities	

Attredgeville	34%
Diepsloot	22%
Soshanguve	27%
Tembisa	17%
Community respondents by User type, gender, age, employment status and area	

A total of 173 respondents completed the questionnaire, among them, 59% are non-users of the Internet, 35% are current-users of the Internet and 6% are lapsed (also known as reluctant users) users of the Internet.

‘Non-users’ of the Internet refer to respondents who had never used the Internet in their lifetime. This group of users consists of ‘absolute non-users’ and ‘rarely Internet users’ according to (Kingsley, & Anderson, 1998; Selwyn, 2006). The group was also known as nonuser by (Helsper & Reisdorf, 2013). In this study, however, ‘non-users’ mainly represent those respondents who have not used the Internet in their lifetime.

The ‘current users’ denote those respondents who are up-to-date with the use of the Internet (currently make use of the Internet) while ‘lapsed users’ are respondents who had used the Internet in the past, but have ceased to do so at the time of the data collection – for example where the Internet have not been used for the past 12 months or more (Selwyn, 2006). Lapsed users are referred to as ex-users according to (Helsper & Reisdorf, 2013).

The above distribution in relation to ‘user-type’ indicates that user groups are not equally represented in the sample. Lapsed users are under-represented, while non-users are highly represented in this sample. Since participants were randomly selected, this research argues that the reported proportions reflect unequal representation of non-users in comparison with users of the Internet in the target population of this research. The large proportion of non-users in the research sample is, however, a positive sign for this research, since this reflects the concern projected in this study and supports the identification of a need to work towards bridging the digital divide. The percentage of non-users, which is a substantial proportion of the

target population of this research, motivates the need for this study. It signifies that digital divide is still a problem that confronts developing countries like South Africa.

According to table 2, male and female representations of the sampled respondents are good. From 173 respondents a total of 53% were male and 47% were female for all user categories. This constitutes a balanced user groups by gender representation. Age groups are also well represented in the sample. It is shown that 31% of the respondents fall within the 18-29 years age bracket, while 30% of the respondents fall between 30-39 years of age. The 28% of the respondents fall within the 40-49 years group and the remaining 11% of the sampled participants were reportedly older than 49 years. A reason for the lower percentage of older people in the sample could be that the 50+ group of mature adults were slightly reluctant to complete the questionnaires. Some of them started, but were not able to complete the questionnaire or made some serious mistakes resulting in the questionnaires either been thrown away or destroyed.

Area distribution indicates that 34% and 22% of the respondents are from Attredgeville and Diepsloot respectively while 27% and 17% are from Soshanguve and Tembisa respectively. All these communities are part of the developing communities in South African context.

Overall, table 2 shows that majority 72% of the respondents that took part in the survey were employed either full time or part time and only 28% were reported as unemployed. Survey shows that 58% of those who are employed were full time while 14% were employed on a part time basis.

4.2. Participants' response on the awareness of the Internet benefits

Table 3 reports participants' response on the items that measured awareness on the benefits of the Internet. In comparison with current and lapsed users, table 3 indicates that non-users have lower levels of awareness in all the items of Internet benefits except for maintaining contact with others and personal development. Some of the results of the Internet benefits appearing in table 3 below are in consistent with the literature that measures awareness (Ting, 2016).

Table 3: Percentage of respondents aware of the Internet benefits and risks

Internet benefits	Current Users (n=)	Lapsed Users (n=)	Non-users(n=)
Internet Facilitate online Transaction	67.24%	64.4%	6%
Internet Promote Personal development	89.7%	82.4%	60.4%
Internet Facilitate work	33.6%	9.1%	7%
Internet Facilitate in maintaining contact with other	91.4%	91.1%	72.3%
Internet Facilitate information search	98.3%	100%	35%
Internet Facilitate entertainment	93.8%	100%	33.3%

According to table 3 above, only 6%, 7%, 35% and 33.3% of the non-users are aware that the Internet can facilitate online transactions, work, information search and entertainment respectively. In the findings, participants in general reported positively on the benefits of the Internet with regard to maintaining contact with others and personal development. This probably might be attributed to the fact that mobile device allow people the opportunity to use different charting applications like WhatsApp, Mix-it and BBM. The possible future work intends to determine the impact of mobile devices in maintaining contact with others.

The data in table 3 generally suggests lack of awareness of Internet benefits on the part of non-users. This could be an indication that there is lack of awareness of Internet benefits resulting in 'non-use of the Internet. Literature suggests that most non-users are not well informed on the benefits of the Internet, when compared to other categories of Internet users (Ting, 2016 and the findings of this research, as indicated in table 3, confirms this view.

The probability (of the Chi-square statistic assuming a value of 591.57 under the null-hypothesis of no difference in response patterns over the various awareness) is $< 0.0001^{***}$, indicating that some responses patterns for Internet-awareness differ statistically significantly from other question-response patterns. The next section analysis of variance present more on statistical significant of this research.

4.3. Analysis of variance

This section describes the results of the analysis of variance (using the general linear model approach) that were conducted on benefit awareness scores to determine which demographic properties of participants (including user-type) impact the perception that Internet benefit awareness affects Internet use. Analysis of variance is a technique that splits the total variation in a data-set into ‘variance-components’ that are explained by the various explanatory effects (independent variable – for example the biographical properties and user-type) in the model. These individual variance components are then compared against the total variance component, and if a particular component is found to be ‘substantial’ (evaluated against a calculated F-statistic), in other words, statistically significant, the explanatory variable (that explained the particular component) is then identified as an effect that affects perceptions.

In this research, a particular type of analysis of variance was conducted, namely General Linear Model (GLM) analysis. This was done to accommodate the fact that the numbers of entries per category of biographical properties were not equal. Table 4 reports the independent variables that statistically significantly affect the perception on the relevance of Internet-benefit-awareness to the use/non-use of the Internet.

Table 4: Analyses of variance conducted on the awareness-factor

Source	DF	Sum Squares	of Mean Square	F Value	Pro > F
Model	10	34.57539144	3.45753914	13.63	<.0001
Internet-User	2	10.06664877	5.03332438	19.84	<.0001
Employment-Status	2	2.80012964	1.40006482	5.52	0.0048
Area	2	0.38988177	0.19494088	0.77	0.4654
InternetUser*Area	4	3.20057876	0.80014469	3.15	0.0158
Error	158	40.07454495	0.25363636		
Corrected Total	168	74.64993639			
R-square = 0.46					

Column 1 (Source) of table 4 indicates the biographical properties evaluated for their effect on perception of awareness. In this table the effect of user-type, employment status, and geographical area was evaluated (the other biographical properties not listed were included in the 'error' term of the model because they proved to be not significant in earlier preliminary runs conducted on the awareness scores). Column 2 contains the degrees of freedom associated with each effect. Columns 3 and 4 report on the variance component associated with each effect or source included in the model while columns 5 and 6 report on the calculated F statistic and P probability associated with each variance component.

The analysis of variance was used in the study to identify variables that statistically significantly affect perceptions on the relevance of the Internet awareness benefits on the Internet use. Table 4 indicates that employment status and user-type influence how participants perceive awareness of Internet-benefits as impacting Internet use. The general significance (F probabilities) attached to the analysis is 0.1% and the statistical significance attached to the employment status and user type effects are 1% and 0.1%, respectively. This shows that employment status and user-type are statistically highly significant. The effect of geographical area alone is not statistically significant because the probability attached to it is greater than 0.05. However the combination (intersection) of users-type and area have statistically significant effect on awareness of Internet benefit. Table 4 identify variables that statistically significantly affect perceptions on the awareness benefits but do not indicate how the identified effect influences perceptions on Internet use. Table 5, Bonferroni multiple comparisons of means tests are therefore also conducted and presented with the relevant analyses of variance tables to indicate how perceptions differ. (The SAS/STATS module of the SAS version 9.3 software package – the PROC GLM procedure - was used to conduct these analyses)

Table 5 Bonferroni multiple comparisons

Means with the same letter are not significantly different.			
Lsd = 0.34			
Bon Grouping	Mean	N	Internet User
A	3.0497	100	non user
B	2.2392	58	current user
B	2.2238	11	lapsed user

Means with the same letter are not significantly different.			
Lsd=0.27			
Bon Grouping	Mean	N	Employment Status
A	2.8627	100	full time
B	2.5715	45	not employed
B	2.3881	24	part time

Bonferroni multiple comparisons of means test results – Table 5 is presented on the mean-scale between 1- 5 (the higher the scale the more the participants are in disagreement that their awareness of the Internet-benefits affect Internet use and the lower the point of scale the more participants are in agreement of their awareness of the Internet benefit affect Internet use). Table 5 reflects the mean score of 3.04 for non-user which is more into disagreement. This implies that non-users are not in agreement that they are aware of Internet benefits. The mean-score for current-users and lapsed-users who participated in the survey are 2.23 and 2.22 respectively. Current and lapsed users are in agreement that they are aware of Internet benefits. The mean-score of ‘2’ reflects agreement while the mean-score of 3 and above depict disagreement. With respect to employment status the mean-score of full-time, part-time and unemployed participants are 2.86, 2.38 and 2.57 respectively. More on the data presented in this section are discussed in the next section.

5. Discussion

The finding of this research reveals that lack of awareness of Internet benefits influences the use of the Internet among non-users compared to current and lapsed users in developing communities in Gauteng South Africa. The implication of this finding is that, in comparison with non-user, certain user groups’ benefits more from the use of the Internet because of their knowledge of and exposure to Internet benefits (This was depicted in Table 3 and was proven statistically significant in table 5).

The findings also reveal that non-users lack awareness of the Internet benefits are particularly in the area of online transactions, work facilitation, information search and entertainment. The findings show that 94% and 93% of the non-users are not aware that the Internet can be used for online transactions and work facilitation respectively. Over 60% of non-users lack awareness that the Internet can facilitate entertainment and more than 67% are not aware that Internet can be used to search and obtain information. The general perception of the non-users participants is that awareness of Internet benefits affects their non-use of the Internet. The current and

lapsed users were in agreement that they are aware of the benefits of the Internet. Their perceptions are that awareness does not generally influence their use/non-use of the Internet. The research identified no significant difference between current and lapsed users (mean-score for both is '2'). They are both aware of the Internet benefits which means that awareness of the Internet benefits does not affect their use/non-use of the Internet.

Bonferroni multiple comparisons mean-score of 2.86 (approximately 3) for full time participants suggests a perception of undecidedness. The participants who were employed fulltime are undecided as to whether awareness of Internet benefits affects their use of the Internet. Participants who were unemployed and those employed part time (with mean score of 2), suggests a perception of agreement. These two groups are in agreement that awareness of Internet benefits affects their use/non-use of the Internet. It can be reasoned that employed participants are more exposed to the Internet and its use (they are familiar with the benefits of the Internet). No significant difference was identified between part time and unemployed participants.

The survey shows that digital divide is still a problem in our society. The finding of this research reflects the kind of digital divide that exists in our environment. In the continent Africa where digital divide is considered a serious problem, this perception can be changed by being proactive in making people aware of benefit of the Internet as a means to encourage them to use the Internet.

6. Conclusions

This paper investigated the impact of awareness on the use/non-use of the Internet. Lack of awareness of the Internet benefits was identified in research as a factor that contributes to the digital divide. It is shown in this paper that lack of awareness has not received sufficient attention in the developing communities. The findings of the survey data provide evidence that non-user of the Internet in South Africa developing communities lack awareness of the Internet-benefits and this affects their use/non-use of the Internet in comparison with current and lapsed users. Employment status was identified to have influence on participants' perception of awareness benefits and the use of the Internet. The imbalance signifies that there is a digital divide in the targeted population, which has both social and economic implications. Lack of awareness of Internet benefits among the participants (particularly the non-users) in developing communities, have negative implications for humanity and how the various human activities are carried out in this information age.

Further research would repeat the study in the remaining South African developing communities for uniqueness or commonality; to investigate and understand which other variables might affects awareness of the Internet benefits and to find possible solutions to bridge this divide.

Research indicates that the traditional three sites of socialisation are the family, peer group and school. The future research also plan to investigate the Internet usage of the non-users family members and peer group in order to determine the correlation that exist in that regard (to understand if the various sites of socialization use the Internet and why the non-users are not).

7. References

- Alam, K., & Imran, S. (2015). The digital divide and social inclusion among refugee migrants: A case in regional Australia. *Information Technology & People*, 28(2), 344-365.
- Akinsola, O., Herselman, M., & Jacobs, S. J. (2005). ICT provision to disadvantaged urban communities: A study in South Africa and Nigeria. *International Journal of Education and Development using ICT*, 1(3), 19 - 41.
- Baker, L., Wagner, T., Singer, S., & Bundorf, K. (2003). Use of the Internet and e-mail for health care information. *Journal of American Medical Association (JAMA)*, 289(18).
- Beger, G., Sinha, A., & Pawelczyk, K. (2012). South African mobile generation: Study on South African young people on mobiles. *Digital Citizenship Safety, UNICEF*.
- Bonfadelli, H. (2002). The Internet and knowledge gaps a theoretical and empirical investigation. *European Journal of communication*, 17(1), 65-84.
- Bornman, E., (2016). Information society and digital divide in South Africa: results of longitudinal surveys. *Information, Communication & Society*, 19(2), pp.264-278.
- Chavula, H. K. (2013). Telecommunications development and economic growth in Africa. *Information Technology for Development*, 19(1), 5-23.
- Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches*. Sage.
- De Lange, M., & Von Solms, R. (2012). An e-safety educational framework in South Africa. In *Proceedings of the Southern Africa Telecoms and Network Applications Conference*.
- Dodge, M., & Kitchin, R. (2001). *Mapping cyberspace* (pp. 65-80). London: Routledge: pp. 65-80.
- Fink, C., & Kenny, C. J. (2003). W (h)ither the digital divide? *info*, 5(6), 15-24.
- Fuchs, C., & Horak, E. (2008). Africa and the digital divide. *Telematics and informatics*, 25(2), pp.99-116.

- Gebremichael, M. D., & Jackson, J. W. (2006). Bridging the gap in Sub-Saharan Africa: A holistic look at information poverty and the region's digital divide. *Government Information Quarterly*, 23(2), 267-280.
- Gunkel, D. J. (2003). Second thoughts: Toward a critique of the digital divide. *New media & society*, 5(4), pp.499-522.
- Hacker, K. L., & van Dijk, J. (Eds.). (2000). *Digital democracy: issues of theory and practice*. Sage.
- Hargittai, E. (2008). The digital reproduction of inequality. *Social stratification*, pp.936-944.
- Hargittai, E. (2010). Digital na (t) ives? Variation in Internet skills and uses among members of the "net generation". *Sociological inquiry*, 80(1), pp.92-113.
- Harris, M. (2015). The Educational Digital Divide: A Research Synthesis of Digital Inequity in Education.
- Haseloff, A. M. (2005). Cybercafés and their potential as community development tools in India. *The Journal of Community Informatics*, 1(3), pp.53-65
- Helsper EJ. (2008) Digital inclusion: an analysis of social disadvantage and the information technology society. Department for Communities and Local Government.
- Helsper, E. J., & Reisdorf, B. C. (2013). A quantitative examination of explanations for reasons for Internet non-use. *Cyberpsychology, Behavior, and Social Networking*, 16(2), pp.94-99.
- South African: Informal settlements Status (2013). Research report, Housing Development agency (HAD).
- Hsieh, J. P. A., Rai, A., & Keil, M. (2008). Understanding digital inequality: Comparing continued use behavioral models of the socio-economically advantaged and disadvantaged. *MIS quarterly*, 97-126.
- Kelly, H., Kennedy, F., Britton, H., McGuire, G., & Law, J. (2016). Narrowing the "digital divide"—facilitating access to computer technology to enhance the lives of those with aphasia: a feasibility study. *Aphasiology*, 30(2-3), 133-163.
- Kingsley, P., & Anderson, T. (1998). Facing life without the Internet. *Internet Research*, 8(4), pp.303-312.
- Kouadio, Y. M. (2008). The digital divide still an issue, 1-20.
- Lenhart, A. (2003). *The ever-shifting Internet population: a new look at access and the digital divide*. Pew Internet & American Life Project.
- Lewis, J. A. (2005). Aux armes, citoyens: cyber security and regulation in the United States. *Telecommunications Policy*, 29(11), pp.821-830.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal uses of information & communication technologies in sub-Saharan Africa: trends, concerns and perspectives. *Journal of Information Technology Impact*, 9(3), pp.155-172.

Manion, M. (1994). Survey research in the study of contemporary China: Learning from local samples. *The China Quarterly*, 139, pp.741-765.

Mtega, W. P. (2012). Access to and usage of information among rural communities: a case study of Kilosa District Morogoro Region in Tanzania. *Partnership: the Canadian Journal of Library and Information Practice and Research*, 7(1).

Mwim, E. N., & Kritzinger, E. (2016). Views of Digital Divide: A Literature Review. In Proceedings of ACIST, 5th-6th July 2016, Accra, Ghana.

Oates, B. J. (2005). Researching information systems and computing. London, Sage

Oecd, (2001). Understanding the digital divide. *Industrial law journal*. 6, 52-54.

Oyedemi, T. D. (2012). Digital inequalities and implications for social inequalities: a study of Internet penetration amongst university students in South Africa. *Telematics and Informatics*, 29(3), pp.302-313.

Oyedemi, T. (2015). Participation, citizenship and Internet use among South African youth. *Telematics and Informatics*, 32(1), 11-22.

Penard, T., Poussing, N., Mukoko, B., & Piaptie, G. B. T. (2015). Internet adoption and usage patterns in Africa: Evidence from Cameroon. *Technology in Society*, 42, 71-80.

Selwyn, N. (2003). Apart from technology: understanding people's non-use of information and communication technologies in everyday life. *Technology in society*, 25(1), pp.99-116.

Srinuan, C., & Bohlin, E. (2011). Understanding the digital divide: a literature survey and ways forward. In 22nd European Regional ITS Conference, Budapest 2011: Innovative ICT Applications-Emerging Regulatory, Economic and Policy Issues (No. 52191). International Telecommunications Society (ITS).

Selwyn, N. (2006). Digital division or digital decision? A study of non-users and low-users of computers. *Poetics*, 34(4), pp.273-292.

Strover, S. (2003). Remapping the digital divide. *The Information Society*, 19(4), pp.275-277.

Talmud, I., & Mesch, G. S. (2003, August). Virtual social capital and network density among Israeli adolescents. In *International conference on computer networks as social networks, Haifa, Israel*.

Ting, C. (2016). The role of awareness in Internet non-use: experiences from rural China. *Information Development*, 32(3), pp. 327-337.

Deursen, A.V. (2010) *Internet skill: vital assets in an information society*. Enschede, University of Twente.

Van Deursen, A. J., & Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), pp.507-526.

Venkatesh, V., & Brown, S. A. (2001). A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges. *MIS quarterly*, 71-102.

Verdegem, P., & Verhoest, P. (2009). Profiling the non-user: Rethinking policy initiatives stimulating ICT acceptance. *Telecommunications Policy*, 33(10), pp.642-652.

Wei, L., & Hindman, D. B. (2011). Does the digital divide matter more? Comparing the effects of new media and old media use on the education-based knowledge gap. *Mass Communication and Society*, 14(2), pp.216-235

Williams, K. (2001). What is the digital divide? In *d3 workshop (digital divide doctoral students)*, Ann Arbor. August

Wyatt, S., Thomas, G., & Terranova, T. (2002). They came, they surfed, they went back to the beach: Conceptualizing use and non-use of the Internet. *Virtual society*, 23-40.

Zillien, N., & Hargittai, E. (2009). Digital distinction: status-specific types of Internet usage. *Social Science Quarterly*, 90(2), pp.274-291.

The Current State of Security Safeguards within South African Institutions to Achieve Compliance to Condition Seven of the POPI Act

P.Dala and H.Venter

Department of Computer Science, University of Pretoria, Pretoria, South Africa

e-mail: xprittishx@gmail.com and hventer@cs.up.ac.za

Abstract

Privacy entails controlling the use and access to place, location and personal information. In South Africa, the first privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by South African institutions and specifies the minimum requirements in twelve chapters, which includes eight conditions for lawful processing of personal information. Condition Seven of the POPI Act makes specific provision for security safeguards to ensure confidentiality and integrity of personal information. In a previous research paper, the authors proposed a framework that included a selection of security safeguards across 3 domains (management, technical and operational) from several leading practices to facilitate the achievement and maintenance of compliance with Condition Seven of the POPI Act, with a specific focus on confidentiality and integrity of electronic personal information stored, processed or transmitted. However, the applicability, extent of implementation and completeness of the security safeguards across the 3 domains has not been explored. Hence, this paper, through an assessment of the current state of security safeguards done via participants from South African institutions, provides an evaluation of applicability, extent of implementation and completeness of the security safeguards across the 3 domains, previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

Keywords

Protection of personal information, POPI Act, POPI Act research survey, electronic personal information, security safeguards.

1. Introduction

The currency of the digital world and the “oil” of the Internet is personal data (Kuneva, 2009). Personal data can be bought, sold and traded creating economic value (Ali *et al.* 2013). Hence, the global risks identified by the World Economic Forum (2014) included data loss as a result of data fraud as a major risk within the technology domain. This is due to the advent of the information age which has presented new challenges in terms of preserving personal information (Saunders and Zucker, 1999).

Privacy entails controlling the use and access to place, location and personal information (Moore, 2008). The value of personal information has increased significantly due to the advent of the information age (Saunders and Zucker, 1999) and this has subsequently resulted in the most prevalent crime of the new millennium known as “identity theft” (Hoar, 2001). This rampant form of crime according to the Information Systems Audit and Control Association (ISACA) (2014) largely occurs when criminals electronically “break into” information systems (such as those owned by institutions) to gain access to databases, which allows them to steal personal information such as financial account numbers, addresses or identity numbers.

As a result, legislation in the ambit of the protection of personal information aims to protect individuals against identity theft and offers wide-ranging institutional benefits such as the protection of an institution’s brand, image and reputation, enhancing the credibility of an institution as well as promoting consumer confidence and goodwill (Titus, 2011).

From a South African perspective, legislation in this area took the form of the Protection of Personal Information (POPI) Bill which was first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill (2009) was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act (2013). Condition Seven of the POPI Act (2013) specifies the need for security safeguards to ensure confidentiality and integrity of personal information.

In a previous research paper (2015), the authors proposed a framework that included a selection of security safeguards across 3 domains (management, operational and technical) from several leading practices to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. However, the applicability, extent of implementation and completeness of the security safeguards across the 3 domains (management, operational and technical) has not been explored. Applicability explores if the security safeguard is used within an institution. The extent of implementation assesses if the security safeguard is fully implemented, partially implemented or is being considered for implementation. Lastly, completeness assesses if there are any additional security safeguards, which the authors may not have considered to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. Hence, the contribution of this paper, through an assessment of the current state of security safeguards done via participants from South African institutions, is to provide an evaluation of applicability, extent of implementation and completeness of the security safeguards across the 3 domains (management, operational and technical), previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

This paper is one of a series of papers associated with the authors' research relating to the POPI Act, which focuses specifically on the confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, namely:

A framework of security safeguards for the confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, which has been presented and published.

The extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including eight privacy principles, which has been presented and published.

Understanding the level of compliance by South African institutions to the POPI Act, which has been completed and submitted.

The current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act, which is this paper.

A model of operation to guide the implementation of the security safeguards, as required by Condition Seven of the POPI Act, which is a forthcoming paper.

The paper is structured as follows: Section 2 provides a background of the POPI Act as well as the selection of security safeguards across the 3 domains (management, operational and technical), previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information, as required by Condition Seven of the POPI Act. An overview of the research methodology, research group and research survey results followed by an analysis of the research survey responses received is provided in Section 3. Section 4 provides key findings and recommendations. Section 5 concludes the paper and also presents future work.

2. Background

This section provides a background of the POPI Act as well as the selection of security safeguards across the 3 domains (management, operational and technical), previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

2.1. South African Protection of Personal Information Act

The POPI Act (2013) promotes the protection of personal information by South African institutions and specifies the minimum requirements in 12 chapters, which includes 8 conditions for lawful processing of personal information. Although the POPI Act was signed into law on 26 November 2013 the enforcement date of the Act is still to be announced.

2.2. Selection of Security Safeguards

Condition Seven of the POPI Act (2013) specifies the need for security safeguards to ensure confidentiality and integrity of personal information.

In a previous research paper, the authors (2015) proposed a framework that included a selection of security safeguards across management, operational and technical domains, to facilitate the achievement and maintenance of compliance with Condition Seven of the POPI Act, with a specific focus on preventing unauthorised disclosure (maintaining confidentiality) and modification (ensuring integrity) of electronic personal information stored, processed or transmitted. The management domain accounted for 5 security safeguards, namely information security governance, risk management, information security policy, supplier and service level management and business continuity management. This was followed by the operational domain which accounted for 6 security safeguards, namely security procedures and processes, baseline infrastructure security standards, security awareness and training, security monitoring, incident and reporting, security assessment and disaster recovery. The remaining 9 security safeguards formed part of the technical domain, namely network segmentation, encrypted data channels, server and network component security, workstation and laptop security, file integrity, firewalls, physical and environmental security, centralised audit logging, data loss prevention.

3. Research survey and analysis

This section provides an overview of the research methodology, research group, and research survey results followed by an analysis of the research survey responses

received via participants from South African institutions in terms of the applicability, extent of implementation and completeness of the security safeguards across the management, operational and technical domains.

3.1. Research methodology

The research methodology encompassed a quantitative inferential approach (Kothari, 2004), which aims to draw conclusions about a group based on a sample in the form of a research group. This approach was driven by the use of a research survey, which was located at <https://www.surveymonkey.com/r/SAPOPI> and was launched from 1 October 2015 to 15 December 2015. The research survey was anonymous and participants were not requested to provide any identifying information such as personal information (title, name, surname and email address) or to disclose the name of their institution. Participants electronically provided consent before participating in the research survey.

3.2. Research group

The research survey specifically targeted participants at South African institutions who store, process or transmit electronic personal information and who, as a result, are impacted by the POPI Act.

The participants were informed of the research survey via an email that included a link to the research survey as well as social media (Twitter and LinkedIn posts) and the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the research survey link to members of the South African chapter. Participants were also able to share the link within their network. As such, CIBECS assisted by distributing the research survey link to participants who were targeted for the 2012 *State of Business Data Protection in South Africa* survey that assessed, amongst other aspects, how prepared South African institutions were to comply with the forthcoming protection of personal information legislation, which at that stage took the form of the POPI Bill.

3.3. Research survey results

181 participants completed the research survey. However, only 167 research survey responses from participants were considered valid (participants were required to represent a South African institution that maintains electronic personal information and as a result is affected by the POPI Act).

3.4. Research survey response analysis - Applicability of security safeguards

In terms of assessing the applicability of security safeguards, participants were asked if the security safeguards across the 3 domains were applicable (that is, used within their institutions) or not applicable to their institutions, as it relates to ensuring confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, as illustrated in table 1 below:

Security safeguard domain	Security safeguard applicable to my institution (response count)	Security safeguard applicable to my institution (response percentage)	Security safeguard not applicable to my institution (response count)	Security safeguard not applicable to my institution (response percentage)
Average - Management	165.00	98.80%	2.00	1.20%
Average - Operational	163.17	97.70%	3.83	2.30%
Average - Technical	164.56	98.54%	2.44	1.46%
Overall Average - All Domains	164.25	98.35%	2.75	1.65%

Table 1: Applicability of security safeguards

As per table 1 above, an average of 98.35% of participants stated that the security safeguards across the management, operational and technical domains were applicable to their respective institutions in that these are either being considered for implementation or already partially or fully implemented. However, an average of 1.65% participants stated that security safeguards across the management, operational and technical domains were not applicable to their respective institutions.

3.5. Research survey response analysis - Extent of implementation of security safeguards

The extent of implementation of the security safeguards across the 3 domains in terms of full implementation, partial implementation or being considered for implementation, applicable to the average of 98.35% of participants is illustrated in table 2 below:

Security safeguard domain	Security safeguard considered (response count)	Security safeguard considered (response percentage)	Security safeguard partially implemented (response count)	Security safeguard partially implemented (response percentage)	Security safeguard fully implemented (response count)	Security safeguard in place and fully implemented (response percentage)
Average - Management	28.40	17.01%	79.00	47.31%	57.60	34.49%

Security safeguard domain	Security safeguard considered (response count)	Security safeguard considered (response percentage)	Security safeguard partially implemented (response count)	Security safeguard partially implemented (response percentage)	Security safeguard fully implemented (response count)	Security safeguard in place and fully implemented (response percentage)
Average - Operational	34.17	20.46%	87.83	52.59%	41.17	24.65%
Average - Technical	46.56	27.88%	81.67	48.90%	36.33	21.76%
Overall Average - All Domains	38.30	22.93%	82.85	49.61%	43.10	25.81%

Table 2: Extent of implementation of security safeguards

An average of 49.61% of participants, as per table 2 above, revealed partial implementation of the security safeguards across the 3 domains within their institutions. In addition, an average of 25.81% of participants stated that the security safeguards across the 3 domains were fully implemented in their institutions. However, an average of 22.93% of participants stated that the security safeguards across the 3 domains are still being considered within their institutions for implementation.

3.6. Research survey response analysis - Completeness of security safeguards

To assess completeness, the 167 participants were asked to assess if there are any additional security safeguards to the selection of security safeguards, which the authors may have not considered to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. 150 participants (89.8%) did not provide additional safeguards that are being considered or implemented (partially or fully) by their institutions. However, 17 participants (10.2%) indicated that there were security safeguards that their institutions are considering or implementing (partially or fully) in addition to the selection of security safeguards proposed by the authors. From these 17 responses, 6 were invalid in that they did not provide accurate and sufficient information for further consideration. However, the remaining 11 of the 17 responses, as listed in table 3 below, provided accurate and sufficient information for further consideration:

No.	Safeguards suggested by participants	No.	Safeguards suggested by participants
1	Database level encryption	7	Next generation firewall
2	Encryption	8	File integrity hashing value validation
3	Payment card industry data security standard (PCI DSS)	9	Firmware embedded basic input output system (BIOS) based persistent and remote asset tracking Data and device security
4	International standards and frameworks	10	We acquired an enterprise wide IT system to protect the electronic information
5	Security standards	11	Wi-Fi networks
6	Mobile device management		

Table 3: Security safeguards suggested by participants

An impact analysis of the 11 valid responses (table 3 above) as depicted in table 4 below was conducted to assess the completeness of the security safeguards proposed by the authors, to ensure confidentiality and integrity of electronic personal information. The impact analysis entailed grouping similar responses from the 11 valid responses and then assessing the responses in terms of either impacting or not impacting the security safeguards proposed by the authors. A response was considered to impact the security safeguards proposed by the authors, if it introduced new security safeguards or resulted in changes to the name of a security safeguard or an update of the description associated with a security safeguard. In comparison, a response was considered not to have an impact on the security safeguards proposed by the authors, if it resulted in no change at all as the current selection of security safeguards adequately address the information provided by a response. The result of the impact analysis for each grouping of responses was supported by a rationale. Furthermore, all responses considered to impact the security safeguards proposed by the authors, was supported by a relevant action aimed at capturing the change required to the affected security safeguards.

Security Safeguards Suggested by Participants	Impact (Yes/No), Rationale and Action Required (Yes/No)
Response 1: Database level encryption	Impact (Yes/No): Yes - Current security safeguards (Encrypted data channels) Rationale: Encryption is only addressed from a data channel perspective by the encrypted data channels security safeguard.
Response 2: Encryption	Action Required (Yes/No): Yes - Rename the “Encrypted data channels” security safeguard to “Encryption” and update the description to address encryption holistically from a data security perspective to cover data transmission (data channels) and storage (databases).
Response 9: Data security	
Response 3: Payment card	Impact (Yes/No): No Rationale: Credit card information is considered personal information however

Security Safeguards Suggested by Participants	Impact (Yes/No), Rationale and Action Required (Yes/No)
industry data security standard (PCI-DSS)	<p>PCI-DSS is a standard specifically for credit card information (PCI Security Standards Council, 2016) and does not apply to institutions who have personal information such as names, surnames and email addresses of clients but no credit card information. As a result, PCI-DSS will not result in an additional security safeguard or an amendment to the security safeguards proposed. However, compliance to the PCI-DSS standard will encompass the implementation of the majority of the security safeguards proposed.</p> <p>Action Required (Yes/No): No</p>
<p>Response 4: International standards and frameworks</p> <p>Response 5: Security standards</p>	<p>Impact (Yes/No): No</p> <p>Rationale: The baseline infrastructure security standards safeguard addresses security standards. Furthermore, the security safeguards includes the need for an information security policy, security procedures and processes as well as baseline infrastructure security standards, which should ideally be based on international standards and frameworks to prevent re-inventing the wheel. For example, the information security policy may be based on International Standards Organisation (ISO) 27001.</p> <p>Action Required (Yes/No): No</p>
<p>Response 6: Mobile device management</p> <p>Response 9: Device security</p>	<p>Impact (Yes/No): Yes - Current security safeguards (workstation and laptop security as well as data loss prevention).</p> <p>Rationale: Workstation and laptop security makes no provision for mobile devices. Furthermore, data end points for data loss prevention are limited to workstations and laptops.</p> <p>Action Required (Yes/No): Yes - Rename the security safeguard “Workstation and laptop security” to “Workstation, laptop and mobile device security” and update the description of the security safeguard to include security of mobile devices. In addition, update the description of the “Data loss prevention” security safeguard to include mobile devices as data end points.</p>
<p>Response 7: Next generation firewall</p>	<p>Impact (Yes/No): Yes - Current security safeguards (file integrity).</p> <p>Rationale: Firewalls independent of vendor or technology is addressed by the current security safeguards (firewall).</p> <p>Action Required (Yes/No): No</p>
<p>Response 8: File integrity hashing value validation</p>	<p>Impact (Yes/No): No</p> <p>Rationale: File integrity is addressed by the file integrity security safeguard, with no provision for hash value validation.</p> <p>Action Required (Yes/No): Yes - Update the description of the “File integrity” security safeguard to include hash value validation.</p>
<p>Response 9: Firmware embedded basic input output system (BIOS) based persistent and remote asset tracking</p>	<p>Impact (Yes/No): Yes - Current security safeguards (Security monitoring, incident and reporting, workstation and laptop security as well as data loss prevention).</p> <p>Rationale: Yes - Security monitoring, incident and reporting safeguard as well as the workstation and laptop security and data loss prevention safeguards did not take into account asset tracking.</p> <p>Action Required (Yes/No): Yes - Update the description of the security monitoring, incident and reporting safeguard to include persistent and remote asset tracking. In addition, the workstation and laptop security safeguard description to be updated to include firmware BIOS based tracking on supported workstations, laptops and mobile devices. Furthermore, the data loss prevention safeguard to enable tracking of assets via data end points, if firmware BIOS based asset tracking is not supported on workstations, laptops or mobile devices.</p>
<p>Response 10: We acquired an enterprise wide IT system to</p>	<p>Impact (Yes/No): No</p> <p>Rationale: Enterprise wide IT system is open to interpretation and could be a data loss prevention (DLP) system or a security incident event and monitoring (SIEM) system. Both the DLP and SIEM systems are addressed by the current security</p>

Security Safeguards Suggested by Participants	Impact (Yes/No), Rationale and Action Required (Yes/No)
protect the electronic information	safeguards (Data loss prevention and security monitoring, incident and reporting). <i>Action Required (Yes/No):</i> No
<i>Response 11:</i> Wi-Fi networks	<i>Impact (Yes/No):</i> Yes - Current security safeguards (network segmentation as well as server and network component security).
	<i>Rationale:</i> The network segmentation as well as the server and network component security safeguards do not make a distinction between wired and wireless networks.
	<i>Action Required (Yes/No):</i> Yes - Update the description of the “Network segmentation” and “Server and network component security” safeguards to state that the security safeguards are applicable to any form of network may it be wired and wireless or a combination thereof.

Table 4: Impact analysis of the security safeguards suggested by participants

As a result of the aforementioned impact analysis in table 4 above, based on the 11 valid responses, 5 responses had no impact on the security safeguards previously proposed by authors as supported by the rationale provided. However, 6 of the 11 valid responses had an impact on the selection of security safeguards previously proposed by authors, in that it did result in updates to the security safeguards but no additional security safeguards were identified.

4. Critical evaluation of the analysis

This section provides a critical evaluation of the analysis performed in section 3 of this paper by way of key findings and recommendations.

4.1. Applicability of security safeguards

An average of 98.35% of participants stated that security safeguards across the management, operational and technical domains, proposed by the authors, were applicable to their respective institutions (either being considered for implementation or already partially or fully implemented). An average of 1.65% of participants stated that security safeguards across the management, operational and technical domains were not applicable to their respective institutions. Certain security safeguards may not be applicable in the event where the institution has compensating safeguards (other alternative security safeguards to ensure confidentiality and integrity of electronic personal information) in place. However, in the event that the confidentiality and integrity of electronic personal information may be compromised due to the lack of a security safeguard, it is recommended that the security safeguards identified as not applicable to the institution across the management, operational and technical domains be re-considered for implementation to mitigate the risk of disclosure and modification of electronic personal information as well as to ultimately ensure compliance to Condition Seven of the POPI Act.

4.2. Extent of implementation of security safeguards

At the time of the research survey being conducted an average of 25.81% of the 98.35% of participants stated that security safeguards across the management, operational and technical domains were fully implemented in their institution. However, security safeguards across the management, operational and technical domains were partially implemented (average of 49.61% of the 98.35% participants) or being considered for implementation (average of 22.93% of the 98.35% of participants). Given that the POPI Act is not yet enforceable, the progress made by South African institutions is considered acceptable in that the implementation of certain of the security safeguards account for a combined average of 75.42% of the 98.35% of participants (partial implementation - 49.61% and full implementation - 25.81%). South African institutions should aim to achieve full implementation of the security safeguards in order to contribute towards the achievement of ensuring compliance to Condition Seven of the POPI Act as well as the overall POPI Act. As a result, the security safeguards that have been fully implemented can be continuously monitored to ensure that the confidentiality and integrity of electronic personal information is preserved, while the security safeguards that have been partially implemented should be fully implemented. Similarly, the security safeguards that are being considered for implementation should be prioritised and implemented in the most effective and efficient manner in order to achieve compliance to Condition Seven of the POPI Act as well as the overall POPI Act.

4.3. Completeness of security safeguards

From a completeness perspective, no additional security safeguards were added to the selection of security safeguards previously proposed by the authors to ensure confidentiality and integrity of electronic personal information. However, based on the information provided by participants in terms of the responses received, driven by themes such as encryption, mobile devices and asset tracking, the names of 2 security safeguards (workstation and laptop security changed to workstation, laptop and mobile security as well as encrypted data channels changed to encryption) were updated. In addition, the description associated with 7 security safeguards were updated. The aforementioned updates are illustrated in *italics* within table 5 below:

Update Description	Security Safeguard Name	Current Safeguard Description	Updated Safeguard Description
4.3.1.1. Update to the security safeguard description	4.3.1.2. Security monitoring, incident and reporting	4.3.1.3. All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal information.	4.3.1.4. All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal information. <i>Security monitoring to include persistent and remote asset tracking.</i>
4.3.1.5. Update to the security safeguard description	4.3.1.6. Network segmentation	4.3.1.7. Application and database servers that respectively process and store personal information are located on a dedicated network segment that is separated from the rest of the corporate network.	4.3.1.8. Application and database servers that respectively process and store personal information are located on a dedicated network segment (<i>may be a wired or wireless network or a combination thereof</i>) that is separated from the rest of the corporate network.
4.3.1.9. Update to the security safeguard name and description	<i>Encryption</i> (previously encrypted data channels)	4.3.1.10. All electronic personal information flowing into and out of the dedicated network segment, is encrypted and access to the data channels is strictly monitored and controlled.	4.3.1.11. All electronic personal information <i>transmitted</i> (flowing into and out of the dedicated network segment) <i>and stored</i> , is encrypted and access to the data channels and storage (databases) is strictly monitored and controlled.
4.3.1.12. Update to the security safeguard description	4.3.1.13. Server and network component security	4.3.1.14. All server and network components are configured to implement the defined baseline infrastructure security standards.	4.3.1.15. All server and network (<i>may be a wired or wireless network or a combination thereof</i>) components are configured to implement the defined baseline infrastructure security standards.
4.3.1.16. Update to the security safeguard name and description	<i>Workstation, laptop and mobile security</i> (previously workstation and	4.3.1.17. Workstations and laptops are configured to implement the defined baseline infrastructure security standards and are locked	4.3.1.18. Workstations, laptops and <i>mobile devices</i> are configured to implement the defined baseline infrastructure security standards and are locked

Update Description	Security Safeguard Name	Current Safeguard Description	Updated Safeguard Description
	laptop security)	down to prevent the user to change the configuration or install additional applications.	down to prevent the user to change the configuration or install additional applications. <i>In addition, firmware basic input output system (BIOS) based tracking should be enabled on supported workstations, laptops and mobile devices (for non- supported workstations, laptops and mobile devices asset tracking should be implemented through the data loss prevention security safeguard)</i>
4.3.1.19. Update to the security safeguard description	4.3.1.20. File integrity	4.3.1.21. All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations.	4.3.1.22. All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations via hash value validation.
4.3.1.23. Update to the security safeguard description	4.3.1.24. Data loss prevention	4.3.1.25. The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations or laptops.	4.3.1.26. The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations, laptops and mobile devices. Furthermore, track assets via data end points, if firmware basic input output system (BIOS) based asset tracking (Workstation, laptop and mobile security safeguard) is not supported on workstations, laptops or mobile devices.

Table 5: Updates to the security safeguard names and/or descriptions

The updates to the security safeguard names and descriptions as reflected in table 5 above will be taken in account when the model of operation to guide the implementation of security safeguards to ensure confidentiality and integrity of electronic personal is to be defined by the authors.

5. Conclusion and future work

In this paper, the applicability, extent of implementation and completeness of the security safeguards across the management, operational and technical domains, proposed by the authors, through an assessment of participants from South African institutions was explored.

From an applicability and extent of implementation perspective, the security safeguards across the management, operational and technical domains, proposed by the authors, were widely used by South African institutions in that an average of 98.35% of participants stated that security safeguards across the 3 domains were applicable to their respective institutions and the security safeguards are either being considered for implementation (average of 22.93% of the 98.35% of participants) or already partially (average of 49.61% of the 98.35% of participants) or fully implemented (average of 25.81% of the 98.35% of participants).

In terms of the completeness of the security safeguards proposed by the authors, no additional security safeguards were added to ensure confidentiality and integrity of electronic personal information. However, the names and descriptions of specific security safeguards were updated based on the information provided by participants. These updates are to be factored, as part of future work, into the model of operation which aims to guide the implementation of the security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed and transmitted, as required by Condition Seven of the POPI Act (2013).

6. Acknowledgements

Thank you to all of the participants who completed and further distributed the research survey. Furthermore, thank you to the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the research survey link to members of the South African chapter as well as CIBECS who assisted by distributing the survey link to participants who were targeted for the 2012 *State of Business Data Protection in South Africa* survey.

7. References

Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013), "Data as the New Currency - Government's Role in Facilitating the Exchange", *Deloitte Review*, Issue 13, p.19.

CIBECs. (2012), "State of Business Data Protection in South Africa", <http://offers.cibecs.com/state-of-business-data-protection-in-sa>, (Accessed, 6 May 2016).

Dala, P. and Venter, H. (2015), "A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information", *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS) 2015*, Kruger National Park, South Africa, pp.415-424.

Hoar, S.B. (2001), "Identity Theft: The Crime of the New Millennium", *Oregon Law Review*, Vol.80, No.4, p.1423.

Information Systems Audit and Control Association (ISACA). (2014), "Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study", *Information Systems Audit and Control Association (ISACA) Journal*, Vol.2, p.14.

Kothari, C.R. (2004), "Research Methodology: Methods and Techniques", New Age International, p.5.

Kuneva, M. (2009), "Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling", p.2, http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf, (Accessed 27 June 2015).

Moore, A.D. (2008), "Defining Privacy", *Journal of Social Philosophy*, Vol.39, No.3, p.425.
PCI Security Standards Council (PCI-SSC). (2016), "PCI Security", https://www.pcisecuritystandards.org/pci_security/, (Accessed 3 June 2016).

Republic of South Africa. (2009), "Protection of Personal Information (POPI) Bill", Cape Town and Pretoria: Government Printer, pp.1-50.

Republic of South Africa. (2013), "Protection of Personal Information (POPI) Act (Act 4 of 2013)", Cape Town: Government Printer, No.37067, pp.2-146.

Saunders, K.M. and Zucker, B. (1999), "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act", *International Review of Law, Computers & Technology*, Vol.13, No.2, p.183.

Stein, P. (2012), "South Africa's EU-style Data Protection Law", *Without Prejudice*, Vol.12, Issue 10, pp.48-49.

Titus. (2011), "Protecting Personally Identifiable Information (PII) with Classification and Content Inspection", *Titus White Paper*, p.5.

World Economic Forum (WEF). (2014), "Global Risks 2014", Insight Report, 9th Edition,

pp.12-13, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, (Accessed 3 June 2016).

The Apple Falling Far From the Tree? Assessing the Law of Encryption in South Africa

KC Perumalsamy and PGJ Koornhof

Department of Mercantile and Labour Law, University of the Western Cape

kperumalsamy@uwc.ac.za; pkoorhof@uwc.ac.za

This work is based on the research supported in part by the National Research Foundation of South Africa for the grant, Unique Grant No. 99180. Any opinion, finding and conclusion or recommendation expressed in this material is that of the author(s) and the NRF does not accept any liability in this regard.

Abstract

In this article we investigate the legal framework for encryption in South Africa and the instances in which it may be legitimate for a court to compel the decryption of encrypted information to protect the interests of the state. Part I introduces the problems posed by encryption and the challenges it faces today after briefly setting out its historical use. Part II will consider modern encryption, expound upon the terminology germane to encryption and its regulation under the Electronic Communications and Transactions Act 25 of 2002 and The Regulation of Interception of Communications and Provisions of Communications-Related Information Act 70 of 2002. Part III will evaluate the jurisprudence both domestic and foreign on the instances in which governments have sought to have encryption bypassed against challenges of the privilege against self-incrimination and Part IV will evaluate the domestic implications for bypassing encryption with particular regard to the constitutional privilege against self-incrimination.

Keywords

Encryption; security; right to a fair trial; right against self-incrimination

1. Introduction

The use of encryption in protecting information or data is not something that is new or dispositive to modern technological advances. There is evidence which suggests that its use stretches as far back to ancient Egypt nearly four thousand years ago where it was used to protect a variety of secretive information (Wiseman, 2015). Throughout history encryption has been used to keep religious information secret, protect military secrets, and shelter communication that is politically precarious (Wrixon, 1998).

Technological advances today have compounded its use. It covers a wider variety of interests, which often protects the ordinary individual's security and privacy, particularly in an age where an almost inextricable link exists between technology,

our privacy and security. The proper functioning of the internet is reliant on encryption as it permits transactions which are both private and secure; it assists in preventing fraud and impersonation, and without it, it would be impossible to safely purchase and do banking over the internet (Wiseman, 2015). Yet, the efficiency of cryptography may also be used to protect illegal activity including fraud, gambling and loansharking (*U.S. v Scarfo*, 180 F.Supp.2d 572 [2001]). It has facilitated the construction and expansion of illicit markets for the purchasing of drugs and even hit men and has been used to conceal child pornography (Farivar, 2011; see also *U.S. v Gavegnano*, 205 Fed.App 954 [4th Cir 2009]). The recent dispute between Apple and the FBI has strengthened the gaze on the regulation of encryption and the circumstances under which it may be bypassed (*In Re Order Requiring Apple INC to Assist In the Execution Of A Search Warrant Issued By this Court* 15-MC-1902 [JO] ["Apple case"]). Additionally, mobile applications such as Whatsapp and Viber have installed end-to-end encryption, which seemingly signals a victory for privacy over security interests (Nordrum, 2016). The extent to which encryption may be bypassed has thus become the subject of significant debate. In many reported decisions, the specific issue of compelling decryption where it may assist the state with criminal investigations and proving the guilt of an accused has been dealt with against the backdrop of the privilege against self-incrimination. The Apple Case illustrates the novel problem of guarding state security where technological advancement seemingly undermines it: in contrast to the usual request for decryption the United States' Federal Bureau of Investigation (FBI) sought to compel Apple Inc. to build software that would allow it to bypass the encryption on a mobile phone device. Both of these circumstances will be considered in respect of South Africa's encryption regulations and likelihood of a court granting such a request in light of our encryption framework.

2. Terminology, Modern Encryption and its Regulation

Encryption is an electronic process that protects data by using a formula to transform readable data into unreadable data. An algorithm called a cipher is used to convert the readable data called the plaintext into unreadable data known as the ciphertext (Reis & Simek, 2012). The reverse process of this is known as decryption, where a key is used to transform the encrypted data back into readable data. The process of encryption may be used to protect both data at rest and data in motion. Data at rest refers to inactive data usually desktops, laptops and servers, whilst data in motion conversely relates to wired or wireless networks and the Internet (Reis & Simek, 2012).

Cryptography and the breaking of codes have always been vital for military applications (Wiseman, 2015). In South Africa, the military have historically used and controlled the encryption of hardware and software by requiring a permit or licence where a product is used for military purposes in terms of the Armaments Development and Production Act of 1968 (now repealed by Act 41 of 2002) (Michalsons Attorneys, 2015). During the Second World War cryptography and the

breaking of codes played a crucial role in the victory of the Allied forces as well (Wiseman, 2015).

Today, multiple forms of cryptography exist, but almost all are exclusively dealt with through computers. It is common for most encryptions to be secured by passwords; however, other forms of cryptographic keys may be used instead of, or in addition to passwords. Usually, this is done through a keyfile, the content of which is used as part of the encryption process, and is often stored separately from the encrypted document. A user is required to identify the correct keyfile out of all the files on the device, which provides additional protection together with the password. Modern forms of encryptions can be divided into two groups: symmetric and asymmetric keys. Symmetric key encryption concerns the same key being used to encrypt and decrypt a device, whilst asymmetric key encryption (sometimes known as public key encryption) relates to two keys being created, one private and one public. In order to encrypt messages the public key is used allowing publishing and distribution to the world without undermining the private key. This allows the private key to be kept secret while decrypting files encrypted by the public key (TrueCrypt Foundation, 2012). One prevalent algorithm used for public key encryption is the RSA, which is named after Ron Rivest, Adi Shamir and Leonard Adleman. The RSA underlies a significant amount of security for Internet communications, particularly because public key encryption is integral to the functioning and security of online commerce and private communications over the Internet (Wiseman, 2015; See also Bright, 2013).

It may be possible to penetrate the encryption without the key through attacking the cryptographic system directly, usually by trial and error or by other means (Wiseman, 2015). Many modern encryption systems are however, for the most part, impenetrable because the use of force to unlock an encryption cannot be achieved within a reasonable timeframe. Another way of unlocking the encryption is by listening to the sounds emitted by the central processing unit- usually undertaken by security researchers in laboratories (Bright, 2013). Perhaps the most effective, and contentious, method of acquiring the key is to compel the holder of the key to provide it, as in the case of *U.S. v Scarfo* and many others discussed below, including, most recently, the Apple Case.

In South Africa the principle regulation for encryption is found in Chapter 5 of the Electronic Communications and Transactions Act of 2002 (ECTA). Section 29 of ECTA mandates the establishment of a register with all cryptography providers by the Director General of the Department of Communications, which records the names and addresses of all cryptography providers, a description of the type of cryptography service or product, and particulars that are necessary for the identification and location of the cryptography provider and their products or services (s 29(1)-(3), ECTA). Failure to register a cryptographic service carries the penalty of an unspecified fine or imprisonment for a maximum of two years.

There are many challenges created by the nebulous composition of Chapter 5. For example, it has been argued that the Act is unclear as to who may be a “cryptographic provider”, what constitutes a “cryptographic service” and what exactly a “cryptographic product” is (Vermuelen, 2016). It is submitted however, that the most contentious aspect of section 29, particularly for the future regulation of encryption, concerns the unclear extent of protection given towards it. Section 29 (3) provides that a cryptographic provider is not required to disclose confidential information or trade secrets in respect of their cryptography services and products. The first reported South African case to consider this aspect, albeit only tangentially, was the *Diners Club* case (*Diners Club Pty Ltd v Singh and Another* 2004 (3) SA 630 (D)). In the case it was held that witnesses were not required to give evidence before the court related to encryption services offered to the plaintiff, notwithstanding the challenge posed by the defendant that foregoing such testimony would violate their constitutional right to a fair trial through cross-examination..... The judge held that not allowing the evidence could be justified on grounds of public policy and the limitation found in section 36 of the Constitution. This judgment seemingly offers authority for the argument in favour of strong encryption protections.

The Regulation of Interception of Communications and Provisions of Communications-Related Information Act 70 of 2002 (RICA) makes provision for an application to be made to a Court in which the decryption key holder is required to disclose the decryption key or to provide assistance in respect of encrypted information (ss 1 and 21 RICA). This is known as a “decryption directive” which a judge may issue provided s/he is satisfied that any indirect communication relating to an interception direction, in whole or in part, concerns encrypted information; that the person specified in the application to the court is in possession of the encrypted information and has the decryption key thereto, and that it is not reasonably possible for the person authorised to execute the interception direction to obtain possession of the encrypted information in intelligible form without a decryption directive (s 21(4)(a)(i-iv) RICA). The wording of section 21 creates a *numerus clausus* on the considerations over which a decryption directive may be issued. This is evident by the use of the word “only” in outlining the instances in which it may be issued. Section 21(b) additionally appears to bolster encryption protections by providing that the designated judge must consider the nature of the encrypted information and whether there would be an adverse effect in issuing the decryption directive against the business of the decryption holder or against the decryption holder him or herself. Section 21 read together with section 29(3) of ECTA, which provides that a cryptography provider may not be compelled to disclose confidential information or trade secrets in respect of its cryptography products seemingly offers proficient support for encryption protections.

What then would be the effect of these provisions when the state seeks a decryption directive for the purposes of criminal investigations, where the holder claims that such a directive would violate the privilege against self-incrimination? Additionally, would RICA and ECTA preclude requests not just to decrypt but to build a mechanism that would allow for decryption as in the *Apple Case*? Section 29 of

RICA sets out the degree of assistance that must be provided by the holder of the decryption key. Ordinarily, this section provides that the decryption key holder must disclose the decryption key or provide assistance in disclosing the decryption key (s 29 (1)(a) and (b) RICA). Section 29 goes on to provide that the holder of the key need not provide any other information not covered by the decryption direction (s 29(2)(c) RICA), but section 29(5) provides an interesting proviso where the person to whom the decryption key is addressed is not in possession of the key or information relating thereto. This section provides that such a person, to whom the directive is addressed, must 'endeavour to comply to the best of his or her ability with the decryption direction'. Thus, it would stand to reason that if the state makes a request to formulate a mechanism for decryption, and such an instruction is ignored it may appear on its face to be in contravention of section 29(5) of RICA.

3. Bypassing Encryptions under Court Scrutiny

The recent dispute between Apple and the FBI, has made requests for decryptions a focal point in the debate on encryption protections. This dispute, however, is not the first time requests for encryptions have been considered by a Court in the United States. One differentiating aspect between the Apple Case and the majority of other cases which consider decryption requests is that for the first time a request not just to decrypt but to build software that would allow passcodes to be bypassed was made by the FBI. Apple, who has assisted the government before on many occasions where a lawful Court order was made to do so, objected this time on the grounds that the effect of the FBI's request would be tantamount to building a master key that would unlock any device, and, that in any event, it does not have the capabilities of doing so (Apple case)

The government's request failed on the grounds that it fell short of one of the three requirements of its main authority, the All Writs Act. A party wishing to invoke the All Writs Act to persuade a court to make a competent order based on the powers conferred on the Courts through the Act - in this case, to make an order requiring Apple Inc. to build software that would allow decryption for an important interest of the state - must show that such request is (a) in aid of the Court's jurisdiction; (b) necessary or proper and (c) agreeable to the usages and principles of the law. Whilst the court accepted that the first two requirements were satisfied it rejected that it was agreeable to the usages and principles of the law on the basis of an interpretive absurdity and possible constitutional invalidity rendered by the FBI's submissions on instructive legislation (Apple case). A provision akin to that of section 29(5) of RICA would have invariably been of greater assistance to the FBI in the relief it sought, rather than relying on general authority permitting courts to make competent orders where it sees fit. The importance of drawing this distinction is that in South Africa, a direct challenge may be launched where the directive is issued to a person. Even if they are unable to decrypt the information, they are under an obligation to assist the authorities to the best of their ability, which may include assistance at a future date when they are able to construct the technological ability to do so.

Scrutiny of requests for encryptions has largely been done through the prism of the right against self-incrimination in the United States, where the vast majority of authority on encryptions exists. The Fifth Amendment in the United States' constitution provides protection against the abuse by officials to extort a confession and upholds the accusatorial system of justice rather than an inquisitorial one, through recognising the right of an accused person not to incriminate themselves (Wiseman, 2015). It has also been argued that the right provides a degree of protection for an accused's dignity and privacy (Dann, 1970). The effect of this right is that it prevents the accused from having to choose between perjury, contempt or providing evidence against him or her (Amae & Lettow, 1995). The majority of judicial opinion on this subject appears to be out of sync on the circumstances in which forced decryptions may occur.

In Re Grand Jury Subpoena Duces Tecum it was held that the right against self-incrimination under the Fifth Amendment protected the right to refuse to decrypt one's hard drives. During a child pornography investigation, law enforcement officials seized a number of digital media from the accused's hotel room, but were unable to decrypt them after making several attempts. They applied to a Court requesting an order to compel the accused to decrypt the hard drives. In deciding the matter the Eleventh Circuit expressed that Fifth Amendment is ignited when there is compulsion for a testimonial communication or act, which is incriminatory. Additionally, it held that the files in question were testimonial in nature. In order for evidence to be considered testimonial in nature it must "require the use of the contents of [one's] mind and cannot be fairly characterised as a physical act" (*In Re Grand Jury Subpoena Duces Tecum* 670 F.3d). This is distinguishable from physical acts which are not afforded the protections of the Fifth Amendment as in the case where a Court may compel blood samples be taken without consent, or compelling an individual to provide handwriting samples for analysis (see *Gilbert v California* 388 U.S. 263 (1967) and *Schmerber v California* 388 U.S. 757 (1966)). Additionally, even communications, which are testimonial in nature, may be compelled when they form part of what is considered to be a "foregone conclusion". In terms of this doctrine, when the government already knows of the existence of the evidence in question, where it is stored and can show the authenticity of the documents through means other than the testimony of the accused, then such testimonial evidence may be admitted irrespective of the Fifth Amendment (*Fisher v The United States* 425 U.S. 391 (1976)).

In Re Boucher, decided four years before *Duces Tecum*, the District Court of Vermont had to decide whether the Fifth Amendment would exclude evidence of child pornography on the accused's computer. Sebastian Boucher's laptop had been inspected whilst crossing into the United States from Canada. The officer had found files on his computer, which at the time did not require a password or the removal of any encryption to access it, with names that suggested child pornography (*In re Boucher No.2 D. Vt. Feb 19, 2009*). After further investigation by another officer, more files had been found, however, when the evidence was re-evaluated it was found that portion of the hard drives which contained the incriminating files were

encrypted. The encrypted files were nearly impossible to penetrate by specialists, and access was impossible without the password. Boucher was accordingly subpoenaed to decrypt the encrypted files. On appeal to the district court, he sought to quash the subpoena based on the Fifth Amendment. The district court observed that the contents of the laptop are not testimonial; however, there are circumstances in which producing documents may be testimonial even when the documents themselves are not testimonial. This is true because the act of production implies that the files do exist, that the producer had control over them and that they were in some sense authentic. The Fifth Amendment could offer protection to the production of such material because it applies to actions, which directly imply an incriminating fact. However, since the foregone conclusion doctrine may compel a defendant to produce files where the government already knows of its existence and location, the request to quash the subpoena was accordingly denied (See also *Doe v U.S.* 487 U.S. 201 (1988); *Fisher v The United States* 425 U.S. 391 (1976); *U.S. v Hubbell* 530 U.S. 27 (2000)). Four years later, in the Friscosu case, the government had seized six computers from Friscosu's house in the execution of a search warrant (*U.S. v Friscosu* 841 F.Supp. 2nd 1232 (2012)). Having failed in its efforts to decrypt the computer without the assistance of the defendant, the government then recorded a conversation between Friscosu and his wife, which provided evidence for the fact that the incriminating information on the laptop was password protected. The government sought a writ requiring Friscosu to assist it following a warrant requiring him to produce an unencrypted version of the files. In accordance with the logic in Boucher the Court concluded that Friscosu was either the owner of the computer, or failing that, the primary user of it, and that he had access to the encrypted data on the computer. Additionally, the fact that the government knew of the location and existence of the files on the computer was also seen as relevant. (*U.S. v Friscosu* 841 F.Supp. 2nd 1232 (2012))

Despite the varied outcomes apparent in decisions to decrypt before courts in the USA, an ostensible link exists between all of the cases mentioned above. Where the evidence in question reveals new testimonial facts to the state, the decryption of such information may not be compelled, as it would affront the Fifth Amendment. A recent example confirming this is the case of *Commonwealth v. Gelfgatt* where it was held that knowledge of computers being used for fraudulent activities does not warrant the protection of the Fifth Amendment as it does not reveal new testimonial facts (*Commonwealth v. Gelfgatt*, 468 Mass. 512 (Mass. Sup. Ct., 2014)). This also explains the rationale for the exception created by the foregone conclusion doctrine, to evidence that would, on the face of it, have the protection of the privilege against self-incrimination. In South Africa, it is submitted that unlike our American counterparts, considerations on the exclusion of evidence which potentially undermines the privilege against self-incrimination, is not contingent on whether it would reveal new testimonial facts to the state but whether the admission of such evidence would render the trial unfair or otherwise be detrimental to the administration of justice. Even though it may reasonably be argued that the broader South African standard could include such aspects as the negative effect of revealing new testimonial facts to the state, it will be shown that this is unlikely to merit the

exclusion of evidence when balancing competing considerations. A narrower standard, such as the American one is thus more likely to provide greater protection to encrypted information. Before considering this standard in light of the South African privilege against self-incrimination, it is first necessary to consider the constitutional implications of the right to privacy in respect of decryption directives.

4. Comparative Assessment between Foreign Approaches and the South African Approach to Self-Incrimination

Prior to the adoption of our Interim Constitution, the position on the admissibility of evidence was governed solely by its relevance. This position comes from our English law tradition which makes relevance the only consideration notwithstanding that such evidence may have been obtained illegally (Hogg, 2005). The American position occupies the opposite of the spectrum when compared to the position under English law. The exclusionary rule as developed by American Courts has held that evidence acquired in violation of its Bill of Rights is to be considered inadmissible and thus excluded (*Mapp v Ohio* (1961) 367 U.S. 643). Many common law jurisdictions such as Canada, New Zealand, Australia, Ireland and South Africa approach admissibility with considerations of both the American and English extremes to reach a middle ground approach. In South Africa, similar to the approach taken in Canada, the rule governing the admission of evidence that violates a right in the Bill of Rights is that it must be excluded where it would render the trial unfair or otherwise be detrimental to the administration of justice (s 35(5) Constitution of the Republic of South Africa, 1996).

In *Zuma v The State*, Kentridge AJ recognised the exclusion embraced in section 35(5) (then section 25 (3) of the interim Constitution) as one that comports with notions of “substantive fairness” (*Zuma v The State* 1995 (2) 642 (CC)). In doing so, he contrasts the previous position reflected in precedent with the one to be taken now. In *S v Rudman and Another*; *S v Mthwana* the Appellate Division held that the function of the Court in criminal matters was to enquire into whether there was an irregularity which departs from the formal rules and principles of procedure, without considering whether the trial was unfair in accordance with the notions of basic fairness and justice (*S v Rudman and Another*; *S v Mthwana* 1992 (1) SA 343 (A)). The Constitution requires an assessment of whether the admission of evidence would undermine the right of an accused to have a fair trial, and whether the administration of justice would be detrimental should the evidence be admitted (*Qozoleni v Minister of Law and Order* 1994 (1) BCLR 75 (E)).

Accordingly, the way American courts would approach forced decryption against the privilege against self-incrimination is fundamentally different to the South African approach, due to the divergent standards on the admission of evidence. The American approach may be summarised as follows: there are three requirements for the operation of the Fifth Amendment. When a statement or action of the individual is compelled, testimonial and incriminating it would be considered objectionable on the grounds of the Fifth Amendment (*Fisher v U.S.* 423 U.S. 391 (1976)). A great

deal of attention has been paid to what constitutes “testimonial evidence” by American Courts. This is because a court may compel physical acts for the purposes of investigations but not evidence that is testimonial in nature (*Duces Tecum* case). Accordingly, the Supreme Court has found that a blood sample may be taken without consent (*Schmerber v. California* 348 U.S. 757 (1966)), that an individual may be compelled to turn over a key to a strongbox (*U.S. v. Hubbell*, 539 U.S. 27 (2000)) and that an accused may be compelled to provide handwriting samples for analysis (*Gilbert v. California*, 388 U.S. 263). Thus, once considered to be testimonial in nature, the Fifth Amendment protects it (*Fisher* case). In *Doe Tecum*, the court held that (in the context of decryption) the evidence in question would be considered testimonial in nature, where it would “require the use and contents of Doe’s mind and could not fairly be characterised as a physical act, and it would reveal his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives, and of his capabilities to decrypt the files.” The court went on to say that it is precisely when an act of production requires the individual to use the contents of his own mind to provide a statement of fact that it becomes testimonial (Doe). There are however instances, as outlined in the discussion in Section III above, where even evidence that is testimonial in nature may be admitted against considerations of the Fifth Amendment. This is where the “foregone conclusion” doctrine applies (*Fisher* case). Where the government already knows of the existence of the evidence in question, where it is being stored and can show the authenticity of the documents through means other than the testimony of the accused, then such evidence will be admitted (Wiseman, 2015).

In the Canadian case of *R v Collins*, Lamer J too draws a distinction between real and testimonial evidence (*R v Collins* [1987] 1 SCR 265). This distinction has since been deemed unnecessary in a number of decisions (*R v Burlingham* (1995) 28 CRR (2d) 244; *R v Ross* (1989) 37 CRR 369). It is submitted that the distinction is without value as the real consideration is whether the admission of the evidence would bring the administration of justice into disrepute. For purposes of section 35(5), it would be unnecessary for that distinction to be drawn because the primary concern of this section is to consider whether the admission of the evidence in question would either render the trial unfair or would otherwise be detrimental to the administration of justice. It is common cause, as was recognised in *S v Tandwa and Others* that where the admission of evidence renders the trial unfair it would also be detrimental to the administration of justice (*S v Tandwa and Others* 2008 (1) SACR 613 (SCA)).

Where it is claimed that a decryption directive would violate the privilege against self-incrimination, the first inquiry is to establish whether compelling the decryption would render the trial unfair. If this leg is satisfied, then the second inquiry on whether it would be detrimental to the administration of justice need not be fulfilled. In *Tandwa* it was held that when considering whether the admission of evidence would render the trial unfair, the court must take into account competing social interests. The court must exercise its discretion by weighing the competing concerns of society on the one hand to ensure that the guilty are brought to book against the

protections afforded to the accused in terms of the constitution. The standard of the community was considered in Canadian precedent but has since been done away with because of its subjectivity and uncertainty in application (Hogg, 2005). In *Rothman v. Queen* it was held that where the admission of evidence would shock the community, it must be excluded (*Rothman v. Queen* [1981] 2 S.C.R. 640). The case of *Collins* has done away with this standard on the basis that section 24(2) of the Canadian Charter, which recognises the exclusion of evidence that would be detrimental to the administration of justice, requires a lower standard because the section recognises that a violation of a fundamental right has already occurred (*R v Collins* [1987] 1 S.C.R. 265).

The more nebulous standard of bringing the administration of justice into disrepute requires greater scrutiny as what may be detrimental to the administration of justice may be a matter of great subjectivity. For example, Professor Peter Hogg, commenting on the case of *Collins*, opines that a consideration of disrepute differs between people: what could bring the administration of justice into disrepute could differ between a police officer and a law professor (Hogg, 2005). Nevertheless, the majority of the Court in *Collins* found that the standard in question concerns disrepute to the community at large. Instead of indicating what a Court should look at when reaching this conclusion, the notion of a reasonable person was proposed by Lamer J. Thus, a trial Court would have to consider what, in the eyes of a reasonable person of the community, would bring the administration of justice into disrepute.

As regards what informs the definition of “disrepute”, three factors were weighed up by a Court: (1) the nature of the evidence; (2) the nature of the conduct by it was obtained and (3) the effect on the system of justice of excluding the evidence. Aspects such as the unreliability of evidence, the methods in which evidence was discovered and other rights violations, will inform the nature thereof. Other aspects such as the deliberate violations, the absence or presence of good faith and other extenuating circumstances will inform the nature of the officials conduct (Hogg, 2005). In South Africa, we have accepted the standard set out in *Collins* (*Pillay v The State* [2011] ZASCA 111).

Despite the general acceptance of the standard of disrepute in *Collins* by our courts, it has been overturned in Canada by *R v Grant*. *Grant* established three new factors to be considered: (1) The seriousness of the Charter-infringing State Conduct, which places the focus on the severity of the state conduct which caused the Charter breach; (2) The Impact on the Charter-Protected Interests of the Accused which focuses on the effect of the violation on the accused person because of the State’s conduct, including inquiries into the intrusion into an individual’s privacy and the direct impact on the right not to be forced to incriminate oneself, and the effect on human dignity; (3) Society’s interest in an Adjudication on the Merits, which focuses on the reliability of the evidence in light of the Charter breach (*R v Grant* [2009] 2 S.C.R. 353). It is submitted that the approach taken in *Grant* is a more satisfactory standard that places equal weight in consideration of the rights of the accused against the

interests of the community, and, accordingly, is the more appropriate constitutional inquiry in terms of s 35(5).

In summation, when a court issues a decryption directive in terms of section 21 of RICA, and the directive is challenged on the grounds of the privilege against self-incrimination, it will likely require forced decryption where the interests of the state are concerned, even when the state does not have prior knowledge of evidence concerned. This highlights the distinction we, along with countries such as New Zealand, Canada and Ireland, follow against the strict exclusion of evidence in contravention of a right followed by America.

5. Conclusion

This article has sought to consider two instances in which decryption may be compelled by a court in order to further the interests of the state. The first concerns the question posed in the Apple Case on whether a company may be required to build a mechanism that allows the state to decrypt information. In this decision it was held that the instructing legislation does not grant the state such a right based on its incorrect interpretation of the All Writs Act relied upon by the FBI. In South Africa, a more direct provision exists in respect of the assistance required by the decryption key holder. Here the decryption key holder is required to assist the state to the best of its abilities even where they are not in possession of a decryption key. A national security interest may induce the application of this section possibly requiring the creation of such a mechanism. Admittedly, the chances of this arising are doubtful, yet the legal authority for this is more certain than that of our American counterparts.

The second consideration evaluates the extent to which the privilege against self-incrimination acts as a bulwark against forced decryptions by a court. The narrow American approach has certainly seen the exclusion of evidence based on the Fifth Amendment that would probably not occur under the South African construction. This is because the exception of prior knowledge of evidence in the American legal system is irrelevant to the South African standard which concerns whether the admission of evidence would render the trial unfair or would otherwise be detrimental to the administration of justice. In all of the cases before American courts on encryption, concerning the concealment of files with fraudulent activities and child pornography, it is submitted that our courts would admit such evidence as it does not thwart the thresholds in rendering a trial unfair or destructing the administration of justice.

6. References

Books

- Currie & De Waal, *The Bill of Rights Handbook* (Juta Publishers, Cape Town 2013)
 SBN/ISSN/Product Number 20797095
 F Wrixon Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and

Breraking Secret Messages From Hieroglyphs to the Internet (Black Dog & Leventhal Publishers, New York 1998) SBN/ISSN/Product Number 1579120407
 J Neethling et al *Neethling's Law of Personality* (Butterworths, Durban 1996).
 SBN/ISSN/Product Number 0409061247, 9780409061246
 PW Hogg, *Constitutional Law of Canada* (Thomson Canada Ltd, Ontario 2005)
 SBN/ISSN/Product Number: 978-0-7798-1337-7

South African Case Law

Bernstein v Bester NO 1996 (2) SA 751 (CC)
Diners Club Pty Ltd v Singh and Another 2004 (3) SA 630 (D)
Hyundai Motor Distributors Pty (Ltd) v Smit NO 2001 (1) SA 485 (C)
J Pillay v The State [2011] ZASCA 111
Magwaza v The State [2015] ZASCA 36
Mistry v Interim National Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)
National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC)
Qozoleni v Minister of Law and Order 1994 (1) BCLR 75 (E)
S v Mayekio en Andere 1996 (2) SACR 298 (C)
S v Rudman and Another; S v Mthwana 1992 (1) SA 343 (A).
S v Tandwa and Others 2008 (1) SACR 613 (SCA).
Zuma v The State 1995 (2) 642 (CC)

Foreign Case law

Census decision 65. BVerfGE. 1 (1983)
Commonwealth v. Gelfgatt, 468 Mass. 512 (Mass. Sup. Ct., 2014)
Doe v. U.S. 487 U.S. 201, 209 (1988)
Fisher v The United States 425 U.S. 391 (1976)
Gilbert v California 388 U.S. 263 (1967)
Hein v. North Carolina 574 US (2014)
In re Boucher, No.2 (D. Vt.Feb.19,2009).
In Re Grand Jury Subpoena Duces Tecum 670 F.3d
In Re Order Requiring Apple INC to Assist In the Execution Of A Search Warrant Issued By this Court 15-MC-1902 (JO)
Mapp v Ohio (1961) 367 U.S. 643.
R v Burlingham (1995) 28 CRR (2d) 244
R v Collins [1987] 1 S.C.R. 265
R v Grant [2009] 2 S.C.R. 353.
R v Ross (1989) 37 CRR 369
Rothman v. Queen [1981] 2 S.C.R. 640
Schmerber v California 384 U.S. 757 (1966)
U.S. Gavegnano, 205 Fed.Appx.954 (4th Cir 2009).
U.S. v Scarfo, 180 F.Supp.2d 572 (D.N.J. 2001)
U.S. v. Friscosu, 841 F.Supp.2nd 1232 (D.Colo.2012).
United States v. Hubbell, 530 U.S. 27,36 120 S.Ct. 2037, 147 L.Ed.2nd 24 (2000)

Journal Articles

A Amae and R Lettow 'Fifth Amendment First Principles: The Self-Incrimination Clause' (1995) 93 *Mich.L.Rev* 857.
 D Reis and J Simek 'Encryption made Simple for Lawyers' (2012) 29 *GPSolo* 18.

M Dann ‘The Fifth Amendment Privilege Against Self-Incrimination: Extorting Physical Evidence from a Suspect (1970) 43 S.Cal.L.Rev. 597.

T Wiseman ‘Encryption, Forced Decryption and the Constitution’ (2015) 11 *ISJLP* 525.

Online Articles

A Nordrum ‘In Privacy versus Security, End –To-End Encryption is Definitely Winning’ available at <http://bit.ly/1SyYbFg> (Last accessed 13 June 2016)

C Farivar, Feds Say Silk Road Suspect Computer Shows He Plotted 6 Murders available at <http://bit.ly/2cRtUCq> (Last accessed 13 June 2016)

J Vermuelen ‘Strong Encryption in SA: Is it Legal?’ available at <http://bit.ly/2d3qtvz> (Last accessed 13 June 2016)

L Michalson ‘Cryptography Laws in South Africa’ available at <http://bit.ly/2chw6F2> (Last accessed 13 June 2016)

P Bright ‘Locking the Bad Guys Out with Asymmetric Encryption, ARSTECHNICA <http://bit.ly/2cBziIR> (Last accessed 13 June 2016)

TrueCrypt Foundation, TrueCrypt User’s Guide 2012 <http://bit.ly/2cyY3ah> (Last accessed 13 June 2016)

Legislation

Criminal Procedure Act 51 of 1977

Electronic Communications and Transactions Act 25 of 2002

Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002

The Armaments Development and Production Act, 57 of 1968

Bow to the King (IV)? A new era for IT governance in South Africa

HF Theron & PGJ Koornhof

Department of Mercantile and Labour Law, University of the Western Cape
3350140@myuwc.ac.za; pkooornhof@uwc.ac.za

This work is based on the research supported in part by the National Research Foundation of South Africa for the grant, Unique Grant No. 99180. Any opinion, finding and conclusion or recommendation expressed in this material is that of the author(s) and the NRF does not accept any liability in this regard.

Abstract

Information Technology has become pervasive. No business can function efficiently without embracing the opportunities that dynamic IT practices present. A number of recent hacking and other IT related scandals illustrate that companies can't afford to be blind to the risk that poor governance in this arena presents. IT is no longer part of doing business but business itself, and IT governance can no longer hover on the periphery of corporate culture. It speaks to the very core of modern corporate governance and risk management. In general, IT governance seeks to regulate and govern areas such as the electronic privacy of customers and employees, the productive use of IT in business; the protection of the online presence of business structures and minimum security standards. In the South African context, the 2009 King Report was notable for its inclusion of an entire Chapter dedicated to IT governance, one of the only self-regulatory codes to speak to it in such detail directly. Currently a fourth version of the report is being prepared, and its recently published draft shows a marked departure from previous versions, being a much more pared-down document. Significantly, the IT governance chapter has been removed, seemingly because principles related thereto have been disseminated throughout the draft report. This contribution assesses the state of IT governance before comparing King III to the Draft King IV Report. It is concluded that the move to less direct recommendations on IT governance is in line with foreign corporate governance codes, and that companies tend to adopt international standards in relation to this aspect.

Keywords

Information Technology Governance; King Report; Sustainable Business Practices; Information Security; Corporate Governance

1. Introduction

Information Technology has become so entangled in our daily lives that it is difficult to fathom a situation where it is not present, and businesses have become especially reliant on IT in the day-to-day running of their operations and in generating profit. (Boar, 2002) With the implementation of IT comes great power to expand and enhance business. (Enoch & Green, 1997) The impact of IT on the operation of firms has both strengthened the ability to monitor internal complexity, but also comes with new risks that did not previously exist, such as issues relating to information security. As such, if IT is properly managed, it simplifies business tremendously – but if not, it increases potential liability to the same extent. (Wixley & Everingham, 2010)

IT governance can be defined as a framework that supports the effective and efficient management of information resources to facilitate the achievement of corporate outcomes. The focus, as such, is on the measurement and management of IT vis-a-vis its associated risks and costs. (Naidoo, 2009; King III, 2009) It seeks to regulate and govern, *inter alia*, electronic privacy of customers and employees; the productive use of IT in the business structure; the protection of the online presence of business structures; protection against litigation; cyber security of business structures; the protection of intellectual property in its digital form and the management of electronic data and records in accordance with the law. (Giles, 2016)

Countries have differing approaches to corporate governance in general, with some adopting self-regulatory codes, others legislation, or a hybrid thereof. (Koornhof, 2013; Wixley & Everingham, 2010) In South Africa, the first notions of IT Governance specifically came to the fore in 2009 in the form of the King Report on Corporate Governance – at this stage already in its third iteration. (King III, 2009) The King Report on Corporate governance is a self-regulatory code researched and drafted by the King Committee on Corporate Governance. The three iterations of the King Report were published in 1994, 2002 and 2009 respectively. The jump from the second to the third King Report was of particular significance, not only due to the inclusion of principles relates to IT Governance, but also because it coincided with the introduction of the new Companies Act, 71 of 2008. (Naidoo, 2009) While it does not have legislative power, the King Reports are granted an elevated status through section 7 of the JSE Listing Requirements which requires listed companies to apply its principles and recommendations. (Wixley & Everingham, 2010) In developing jurisprudence, courts are also recognising its importance (See *South African Broadcasting Corporation Ltd and Another v Mpofu* [2009] ZAGPJHC 25).

Recently, the highly anticipated first draft of King IV was released for comment. It is expected to come into operation in November 2016. The draft report is bold in its undertaking, seeking to become the benchmark for good governance not only in public companies – its traditional field of application in practice – but also smaller ones, as well as the public sector. This was also a stated goal of King III, but the draft Report deals with this aspect in a far more express and nuanced manner both in

its explanatory introduction, its principles, and the general language used in it. The Draft Report also includes supplements for how the principles may apply differently in sectors such as municipalities, SMEs, NPOs, and SOEs. (King IV Sector Supplements, 2016) As such, the Report's coming into effect may have far-reaching implications for what is seen as best practices and good governance all around.

While King III dealt with IT Governance in isolation, it has been stated that King IV seeks to approach and deal with this in a much more holistic manner given the pervasive effect of IT on business. (Draft King IV Report, 2016; Giles, 2016) This article seeks to consider IT governance in South Africa by looking at the current position in King III and comparing it to the new position proposed in the draft of King IV. This will be done in the light of developments both in foreign countries and international standards, along with critical commentary on King III itself. In doing so, a general overview of IT Governance principles and practices will be given, before moving on to a discussion of international instruments and the position in foreign countries. Subsequently, the focus will be moved to a critical comparison of IT Governance principles in King III and the draft King IV before concluding.

2. An Overview of IT Governance Practices and Principles

The general principle of IT governance is that management and the board should ensure that IT projects and systems are in line with overall objectives of the company, and that the risks and complexity related to these aspects are sufficiently managed. Given the great costs related to IT and the fact that mismanagement often creates systems that are unsuitable, principles of IT governance seek to assess whether or not related company processes are fit and proper in relation to their stated purpose. As such, individuals managing and measuring these processes should have the appropriate skill and awareness. (Wixley & Everingham, 2010; Cassim et.al, 2012)

Aspects relating to protection of information, the management of information and the protection of personal information processed by companies are considered key when assessing the sufficiency of IT governance practices. IT systems without proper, sophisticated, adaptive controls and security mechanisms can easily fall prey to cybercrimes, such as denial of service attacks and unauthorised access to sensitive information. (Naidoo, 2009; Ragan, 2013; Etsebeth, 2005) If ever there was doubt about the inherent importance of the above aspects, it has been wiped away clean by recent tech-scandals such as the hacking of Sony Pictures Entertainment and the Ashley Madison data breach. The 2014 Sony Pictures hack was a supposed retaliation by North Korea to the intended release of film 'The Interview' in the same year. The hack brought about a leak of approximately a hundred terabytes of sensitive information. (Better, 2014) The Ashley Madison data breach of 2015 was a situation where a group set about leaking some twenty-five gigabytes of company data which it had gathered by hacking company servers. Ashley Madison is an enabling website for extramarital affairs. The data in question was extremely sensitive information of approximately thirty-seven million customers. This was

vastly damaging to the company, resulting in the company's withdrawal from listing publicly with an intended \$200 million initial public offering. Prominent members of society were also embarrassed as a result. (Thomsen, 2015; Krebs, 2015)

A variety of approaches to the implementation of corporate governance, of which IT governance is a subset, can be identified. As stated above, certain countries have adopted self-regulatory codes, while others have introduced legislative interventions – more informally referred to as soft law and hard law respectively. While some countries lean towards the former approach and others to the latter, most have effectively opted for a hybrid approach. Examples of foreign self-regulatory codes include the FRC Corporate Governance Code of the United Kingdom, the ASX Corporate Governance Principles in Australia, and the NYSE and NASDAQ Rules in the United States, as well as the OECD Corporate Governance Principles. Examples of legislation include the Sarbanes-Oxley Act in the United States along with several EU directives notably dealing with governance in the financial sector. Provisions relating to corporate governance are also found in the company legislation of Australia and South Africa. (Koornhof, 2013)

When comparing the above hard law and soft law, the most notable difference is the required standard of compliance, with the former generally adopting a strict application, and the latter comprising a more lenient and flexible approach. The so-called 'comply or else' standard is most effectively showcased through enactment of the US Sarbanes-Oxley Act in 2002. This is a strict and somewhat harsh response to a large array of corporate scandals in the USA during the early 2000s. All corporate entities are required to comply, with no exceptions. This model of corporate governance has been praised for holding all corporate entities equally accountable and critiqued in that it isn't applicable all the time given that the scale of business carried out by companies may vary too considerably. (Hill, 2006; Koornhof, 2013)

In contrast to the above, the 'apply or explain' or 'comply or explain' standard is generally associated with self-regulatory codes. In essence, entities are given a set of standards, principles and/or recommendations to follow, but are not mandated to follow all of them necessarily. Instead, they may choose what is most appropriate to them and explain their non-compliance accordingly. This was the model applied by earlier versions of the UK Combined Code, the Dutch Tabaksblat Code, and the first two versions of the King Report. A newer variation on this standard, which was adopted by King III, is the so-called 'apply or explain' approach which expects companies either to apply the recommendations of the Code, or (in deviating from the recommendations) explain how they at least adhere to the overarching principles found in the Code. While still flexible in its application, it creates an additional layer of accountability whereby companies can't simply disavow the principles of the Code. (Naidoo, 2009) In the explanatory memorandum to the draft of King IV it states that the flexible approach adopted in King III should be retained, but uses a slightly more onerous "apply *and* explain" approach, assuming that companies have complied with its principles as a point of departure. (Draft King IV Report, 2016)

3. International standards and foreign implementation

It is prudent to consider international best practices, given that principles related to IT governance have been around in some manner or form for quite some time, and have since been tabulated in various international standards. The most prominent ones will be discussed briefly below, along with the positions adopted in foreign countries.

a. Control Objectives for Information and Related Technology (COBIT)

COBIT is a widely used comprehensive framework which links business risks, needs for controls and technical issues associated with IT Governance. (Naidoo, 2009) Its framework provides metrics and maturity models to assess how the above issues are managed, and also identifies the associated responsibilities of business and IT process owners. (Mingay & Bittinger, 2002; Moeler, 2008; Marnewick & Labuschagne, 2011)

The newest iteration, COBIT 5, adopts five principles, and places an increased focus on processes, enterprise goals and enablers aligned with these principles. (ISACA, 2012) Principle 1 seeks to meet stakeholder needs by maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources. Principle 2 seeks to integrate governance of enterprise IT into enterprise governance, holistically covering all IT-related functions and processes within the business from end to end. Principle 3 encourages the application of a single, integrated framework, noting that in the modern era there is a need to not only recognise but also align with other international standards. Principle 4 advocates a holistic approach to IT, noting that there are various ‘enablers’ which determine efficient and effective governance and management thereof, such as principles, policies frameworks; processes; organisational structures, corporate culture, and the skills and competencies of people within the business. Finally, Principle 5 seeks to separate governance from management, making a clear distinction between the two. In this regard, it states that: “Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.” On the other hand, it emphasises that “[m]anagement plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.” As such, it distinguishes between the holistic, steering function of a board, including independent and non-executive directors, and the more specific day-to-day running of the business, dealt with by executive directors and management committees.

It should be noted that King III is considered to be most in line with COBIT, and the general sentiments about the division between governance and management are echoed therein. In fact, the King Report expressly notes that the implementation of COBIT could help achieve adequate IT governance. (King Report, 2009; Steenkamp,

2011) However, this reference was to COBIT 4.1, which used a different method to COBIT 5. It will be considered below whether this trend is followed in the draft of King IV.

b. ISO/IEC 38500

The ISO/IEC 38500 standard provides a framework with a view to assist those at the highest levels of organisations to understand and fulfil their legal, regulatory and ethical obligations in respect of the use of IT in their business structures. To this end, it places IT at a strategic level and looks at it from a demand standpoint, focusing rather on how IT can be used by a business than how it is implemented. Crucially, it places emphasis on top management's behaviour in relation to IT governance, distinguishing clearly between the concepts of governance as a heightened and integrated degree of responsibility, and management, which is a more delegable and diluted responsibility. (ISO/IEC 38500:2015) Whereas COBIT adopts a more holistic view, this standard favours a more top-down approach. (Sylvester, 2011)

The standard prescribes three main tasks which directors should implement in governing the use of IT within their businesses, along with six overarching principles. The three tasks prescribed by ISO are the following: firstly, directors must evaluate the current and future use of IT in the company; secondly, directors must prepare and implement plans and policies to ensure that the use of IT meets the business objectives of the firm; finally, directors are to monitor the firm's conformance to policies and plans as set out by management. The six principles advocated by the standard are: ensuring that IT responsibilities are clearly established; aligning corporate and IT strategy; ensuring that IT acquisitions and investments are made properly; ensuring that IT delivers its required performance; ensuring that IT conforms to all compliance requirements; and finally ensuring that IT policies and practices take human behaviour into account. (ISO/IEC 38500:2015; Harmer, 2015) Notably, while these principles prescribe what should happen, they do not always expressly state how, when or by whom it should be implemented. COBIT 5 recognises this aspect and uses it as a point of departure in aligning itself with the ISO standard. (ISACA, 2012)

c. The Calder-Moir Toolkit

In considering IT governance holistically, Calder submits that none of the above international standards provide full and comprehensive guidance, and consequently that other remedies must be sought. It is further noted that attempting to use these frameworks concurrently is also problematic given that they at times overlap and at others are at odds with one another. When firms try to reconcile these aspects, it may cause unnecessary wastage of resources and time, and essentially detracts from the main objective, namely the governance of IT. (Calder, 2008) To this end, the so-called Calder-Moir IT Governance Framework (colloquially known as the Calder-Moir Toolkit) was developed.

The toolkit is divided into six quadrants, arranged in a cyclical manner, relating to business strategy; risk, conformance and compliance; IT Strategy; managing change; maintenance of the information and technology balance sheet and, finally, operational management. The first three deal with planning in general, covering the processes for the establishing of directions, specifying constraints and decision-making. The last three in turn cover the development of new capabilities and the management thereof as well as the use of IT to deliver business products and services. (IT Governance Ltd, 2013)

True to its arrangement, the process of applying the toolkit is also cyclical, starting with business strategy and ending with operational management. Each of these quadrants is divided into three 'layers,' the inner (denoting key issues to be dealt with by the board), middle (the executive management's responsibilities) and finally the outer layer (related to IT practitioners and delegated implementation). (Calder, 2008)

Essentially, the toolkit is a 'meta model' for the coordination of frameworks and the organisation of IT governance. While it often refers to the ISO standard, the toolkit is in itself intentionally devoid of such content in order for it to be able to be adapted to any particular strategy or corporate governance regime. (IT Governance Ltd, 2013)

d. Implementation of IT Governance in other countries

As already mentioned, most countries use some kind of hybrid system when it comes to corporate governance in general, with certain aspects covered by legislation and others by self-regulatory codes. In the United States, legislation such as Sarbanes-Oxley largely deals with financial matters, with more nuanced aspects of corporate governance for listed companies being dealt with in the listing requirements of stock exchanges. Both Section 303A of the NYSE Listed Company Manual and the NASDAQ Marketplace Rule 5600 Series, which state the corporate governance standards for their respective exchanges, are wholly silent on the issue of IT governance. However, the NYSE Corporate Governance Guide does mention that the best practices for listed companies would be to adopt COBIT (Rosenblum et al, 2014). The United Kingdom position is practically the same, with neither the 2006 Companies Act nor the 2014 Corporate Governance Code providing specific guidance. The 2015 OECD Principles are similarly silent. It is submitted that a possible reason why most country-specific codes are silent on the subject of IT governance is as a result of multinational corporations which, given that they operate globally, likely adopt international standards for such issues, rendering it somewhat moot.

The only notable country to adopt its own standard was Australia, with the publication of AS8015 in 2005. The standard's framework provides for six principles of good IT governance, namely; establish clearly understood responsibilities for ICT, plan ICT to best support the organisation, acquire ICT validly, ensure that ICT performs well, whenever required, ensure ICT conforms with formal rules and

ensure ICT respects human factors. Furthermore, the standard denotes that governance responsibility is subject to delegation to “senior managers, technical specialists, vendors and service providers.” It ultimately formed the backbone of the ISO/IEC 38500 standard, which has effectively replaced it. (Ramin Communications, 2016)

4. Comparing King III to the draft King IV Report

The principles of IT governance in King III are found in Chapter 5 and seek to highlight the most salient aspects for directors to focus on. Due to the broad and ever-evolving nature of the topic, it does not try to be the definitive text on the subject but rather to create a greater degree of awareness at board level.

King III states that pursuant to the digital nature of business conducted today and the vast automation reform of enterprise, information technology has become such an integral part of the business model in South Africa that there is a need to regulate it distinctively as it forms part of the larger corporate structure. Specific notice has been taken of how IT is and can be used as a ‘strategic asset’ to gain a competitive edge in the marketplace. One of the key aspects that King III sought to rectify is the perception that IT governance is ‘the IT department’s responsibility’ and not that of top-tier management. (Steenkamp, 2011)

Chapter 5 provides 7 overarching principles, namely that: the board should be responsible for IT governance; IT should be aligned with the performance and sustainability objectives of the company; the board should delegate to management the responsibility for the implementation of an IT governance framework; the board should monitor and evaluate significant IT investments and expenditure; IT should form an integral part of the company’s risk management; the board should ensure that information assets are managed effectively; and finally, the risk and audit committees should assist the board in carrying out its IT responsibilities. Along with these seven principles are 48 recommendations that outline how this should be enacted. Some of the notable specific recommendations include that companies should adopt an IT Charter and that a suitably qualified Chief Information Officer should be appointed.

King III speaks to IT governance in a very concise manner and has been criticised for being ambiguous at times, with specific reference to the potential uncertainty and confusion that may arise when determining whether a specific principle has been complied with. Businesses wishing to satisfy compliance have therefore sought assistance from international standards and compliance toolkits. (Etsebeth, 2010) While these aspects are mentioned in Principle 5.6, King III has been criticised for failing to sufficiently deal with aspects related to information security and information privacy. (Ragan, 2013) While this is a criticism of the Report itself, it should be noted that legislation such as the Protection of Personal Information Act, 2013 and the Promotion of Access to Information Act, 2000 may to a certain extent rectify this situation in relation to information privacy. Information security is also,

at least in part, covered by provisions in the Electronic Communications and Transactions Act, 2002.

Turning to the draft King IV Report, the text also does not pretend to be a definitive one in relation to IT governance. Nevertheless, an increased emphasis on information technology is placed in the draft's foundational concepts, describing its advent as 'the fourth industrial revolution'. Additionally, recommended practices of principles tangentially related to IT can be identified. Firstly, it is noted that organisations are to engage with stakeholders in new ways, of which digital communication platforms such as social media form a part. This is reiterated in Principle 5.1. Secondly, firms are required to adopt a 'new perspective of risk' since risks are evolving, due to globalisation and increased connectivity. Thirdly, a key aspect which is raised is the fact that more categories of jobs will be automated. The industries of robotics and artificial intelligence will thus become more prominent, forcing organisations to consider the effect of this on business, employees and larger society. Fourthly, its conception of the role of the governing body entails managing technology and information in a manner that supports the organisation's defining core purpose and setting out and achieving strategic objectives. Finally, Principle 3.4 advocates that responsibilities for functional areas including technology and information be managed with appropriate experience, be appropriately resourced and *sufficiently defined so as to create certainty*. While the phrases 'information security' and 'information privacy' are not expressly mentioned, it is submitted that, when holistically analysing the text, they are seen as priorities.

Principle 4.2 of the draft report reiterates that the governing body should govern technology and information in a way that supports the organisation in defining its core purpose and to set and achieve strategic objectives. Seven recommended practices are stated in relation to this. These practices are that: the governing body should provide strategic direction for management in respect of IT; the governing body should approve policy that articulates strategic use and direction of IT; that such policy should adopt appropriate standards to give effect to strategy; the governing body should delegate to management the responsibility of implementation of policy on IT, not only in respect of day-to-day activities, but also in relation to medium to long-term decision-making, activities and culture in general; the governing body should oversee the adequate and effective implementation of technology and information management; the governing body should oversee the management of cyber-security risk; the governing body should periodically carry out review of the adequacy and effectiveness of the organisation's technology and information function, and finally that there should be disclosure and reporting at each stage of implementation of IT policies. Essentially these principles encompass the governing body's authority to delegate, oversee and review the governance of IT in the business structure. It retains the concise and summarised nature similar to that of Chapter 5 in King III, and it is submitted that potentially the same problems in interpretation and implementation may arise.

It is submitted that what King IV seems to have done is attempt to incorporate into its text an approach similar to that of the Calder-Moir Toolkit. Seemingly it takes the most prominent best practices from each of the international standards and incorporates them in an effort to secure adequate and effective IT governance. Similar to COBIT 5, the draft King IV seemingly also makes a more pronounced distinction between aspects related to ‘governance’ and that of ‘management,’ opting for the delegation of responsibility with regard to implementing IT policies and process to management, while the governing body should be more involved in holistic policy development and the subsequent oversight of management. Whereas King III was influenced by the principles of COBIT 4.1, the drafters of the King IV appear to have placed their reliance on the provisions of COBIT 5.

Mervyn King, the former head of the King Committee, advocated that ‘a company’s board must be directly involved in IT governance’ (Steenkamp 2011). Where IT governance has been shown to be most effective is when it is governed by the board itself in line with the ISO standard and not that of COBIT. (Hardy, 2008) However, it is trite that members of the board cannot concern themselves with every single decision to be made on a day-to-day basis and as a whole may not always have the prerequisite skills and knowledge to make the right call. Milner criticises the lack of references in the draft to a Chief Information Officer or IT Steering Committee as one that could be problematic in this light. (Milner, 2016) Visser in turn argues that the importance of social media is understated, and that this should be emphasised. (Visser, 2016) Everingham also points out in his commentaries on the draft that in implementing Principle 4.2 it may prove difficult to assess return on investment in technology and information systems. As such, he notes that there should be a careful post-implementation audit of the actual delivery provided by such investment against what may have been promised. (Everingham, 2016) These *lacunae* may create a situation where organisations who are new to IT governance and do not view the Report in context with international instruments may inadvertently create inappropriate structures in comparison to what was specifically prescribed by King III. Notwithstanding these commentaries, the reaction to the draft has been largely positive. An alternative point of view to this would be that the Report shies away from using a check-list approach, rather opting to provide organisations freedom in determining how best to implement IT governance in their unique environment. It is submitted that one must take into account the nature and logistics of modern day business, to which end an amalgamated approach will be most beneficial. Seemingly, the draft King IV adopts such an amalgamated approach.

5. Conclusion

The draft of King IV recognizes IT as an integral part of nearly every aspect of corporate governance, not merely as a separate consideration placed within a standalone chapter. Also, added weight is given to the value of data and data structures, although they are not considered at length. Although King III deals with IT governance, it has been criticised as being vague and convoluted in its approach. This led organisations to consider the implementation of compliance toolkits which,

although rendering a satisfactory result, derogated from the King Code's direct utility in respect of IT governance in a South African context. To this end the drafters of King IV have seemingly attempted to incorporate the strength of compliance toolkits by taking the best of each international standard and applying it throughout King IV.

The trend in most foreign countries has been to do away with any specific principles relating to IT governance, possibly in recognition of the fact that far better specialised instruments exist, and that it is unnecessary to reinvent the wheel in this regard. It can therefore be asked why the draft features any specific recommendations at all. It is submitted that a potential answer to this is that, given the isolated nature of the South African economy and the fact that King IV seeks to apply to a variety of sectors, at least some principled guidance may initially be required. While it can be stated that the provisions of the draft are largely a step in the right direction, it is submitted that in future, more – which in this particular instance would be less – can possibly be done in order to align the South African approach to IT governance with that of the rest of the world. Kneel down to the King? Possibly not yet. However, a respectful nod seems warranted.

6. References

Books

- G20/OECD Principles of Corporate Governance* (2015), OECD, ISBN: 9789264236882
- Boar, BH (2001) *The Art of Strategic Planning for Information Technology* 2nd Edition, Wiley, ISBN 978-0-471-37655-2
- Cassim, F *et al* (2012) *Contemporary Company Law* 2nd Edition, Juta, South Africa, ISBN 9780702185656
- Enoch, C & Green JH (1997) *Banking Soundness and Monetary Policy*, IMF Publications, ISBN 978-1-55775-645-9
- ISACA (2012), *Cobit 5: A Business Framework for the Governance and Management of Enterprise IT*, ISACA, ISBN 978-1-60420-237-3
- Moeller R.R (2008) *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, COBIT and ITIL*, Wiley, DOI: 10.1002/9781119197119
- Naidoo, R *Corporate Governance: An Essential Guide for South African Companies* 2nd Edition, LexisNexis, South Africa, ISBN 9780409046052
- Rosenblum, S.A. *et al* (2014) *NYSE: Corporate Governance Guide*, White Page Ltd, ISBN: 978-0-9565842-6-7
- Wixley, T & Everingham, G (2010) *Corporate Governance* 3rd Edition, Siber Ink, South Africa, ISBN 978-1-920025-32-8

Journal Articles

- Etsebeth, V. (2005) "Governance in the information age – implications for the law", *TSAR* 274
- Etsebeth, V. (2010) "King III on IT Governance: making good, making promises or making trouble" *De Jure*
- Hardy, G. (2006) "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges." *Information Security Technical Report II*
- Hill, JG (2006) *Regulatory Responses to Global Corporate Scandals*, University of Sydney Legal Studies Research Paper No 06/35
- Koornhof, P (2013) "An overview of recent changes to Corporate Governance frameworks as

it pertains to Executive Remuneration” *Speculum Juris* 2013(1)
 Marnewick, C & Labuschagne, L. (2011) “An Investigation Into the Governance of Information Technology Projects in South Africa” *IJPM* 29:6
 Ragan, C.R. (2013) “Information Governance: It’s a duty and it’s smart business”, *RJLT* Vol. XIX:4
 Steenkamp, G. (2011) “The Applicability of using COBIT as a framework to achieve compliance with the King III Report’s requirements for good IT governance” *SA Journal for Accountability and Auditing*, Vol. 11
 Sylvester, D (2011) ‘ISO 38500 – Why Another Standard?’ *COBIT Focus* Vol 2
 Von Solms, B. & Von Solms, R. (2005) “From information security to ... business security?” *Computers & Security*, Vol. 24

Case Law

South African Broadcasting Corporation Ltd and Another v Mpfu [2009] ZAGPJHC 25

Domestic Legislation

Companies Act, 2008
 Electronic Communications and Transactions Act, 2002
 Promotion of Access to Information Act, 2000
 Protection of Personal Information Act, 2013

Foreign Legislation

Companies Act, 2006 (c46) [England]
 Sarbanes–Oxley Act of 2002 (Pub.L. 107–204) (United States of America)

Online Sources

Bettors, E. “Sony Pictures hack: Here’s everything we know about the massive attack so far” (2014) available at <http://bit.ly/28SYj12> [Accessed 14/06/2016].
 Calder, A (2008) “*Developing an IT governance framework*” available at <http://www.ncc.co.uk/article/?articleid=13371> [Accessed 21/04/2016].
 Corporate Governance Principles and Recommendations (the Third Edition) (2014), ASX Corporate Governance Council available at <http://bit.ly/1wFCjzh> [Accessed 20 June 2016]
 Draft King IV Report (2016), Institute of Directors, South Africa, available at <http://www.iodsa.co.za/?page=KingIV> (Accessed 20 June 2016)
 Everingham, G (2016) “King IV Public Commentary” available at <http://www.iodsa.co.za/resource/collection/1687791E-FCFE-4442-AABC-2C90451A6868/Geoff%20Everingham.pdf> [Accessed 20 June 2016]
 Giles, J (2016) “King IV Code and IT Governance” available at <http://www.michalsons.co.za/blog/king-iv-code-and-it-governance/18691> (Accessed 20 June 2016)
 Harmer, G. (2015) “Updated Edition of ISO 38500:2015” available at <http://www.itwnet.com/columns/updated-edition-isoiec-385002015> [Accessed 14/06/2016].
 ISO/IEC 38500:2015 “Information technology - Governance of IT for the organization” available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62816 [Accessed 20 June 2016]

- IT Governance Ltd (2013) “The Calder-Moir IT Governance Framework” available at http://www.itgovernance.co.uk/calder_moir.aspx [Accessed 20 June 2016]
- King Report on Corporate Governance in SA (2009), Institute of Directors, South Africa, available at <http://www.iodsa.co.za/?kingIII> (Accessed 20 June 2016)
- King IV Sector Supplements (2016), Institute of Directors, South Africa, available at <http://www.iodsa.co.za/page/KingIVsectorsupp> (Accessed 23 June 2016)
- Krebs, B. (2015) “Online cheating site Ashley Madison hacked” available at <http://bit.ly/1fWNcar> [Accessed 14/06/2016].
- Milner, J (2016) “King IV Public Commentary” Webber Wentzel Attorneys, available at http://www.iodsa.co.za/resource/collection/1687791E-FCFE-4442-AABC-2C90451A6868/Jean%20Milner_Webber%20Wentzel.pdf [Accessed 20 June 2016]
- Mingay, S & Bittinger, S. (2002) “Combine COBIT and ITIL for Powerful IT Governance” (2002) available at <http://gtnr.it/28V2hJN> [Accessed 20 June 2016]
- NASDAQ Marketplace Rule 5600 Series available at <http://bit.ly/28SELSM> [Accessed 20 June 2016]
- NYSE Listed Company Manual (2013) “Corporate Governance Standards” available at <http://bit.ly/292thFt> [Accessed 20 June 2016]
- Ramin Communications (2016) “AS8015: Australian Standard for Corporate Governance of Information and Communication Technology” available at www.ramin.com.au/itgovernance/as8015.html [Accessed 20 June 2016]
- Thomsen, S. (2015) “Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online” available at <http://read.bi/1HLXHUC> [Accessed 14/06/2016].
- The UK Corporate Governance Code (2014), Financial Reporting Council available at <https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-April-2016.pdf> [Accessed 20 June 2016]
- Visser, A (2016) “King IV Public Commentary” Adams & Adams available at http://www.iodsa.co.za/resource/collection/1687791E-FCFE-4442-AABC-2C90451A6868/Andre%20Visser_%20Adams%20&%20Adams%20Attorneys.pdf [Accessed 20 June 2016]

The impact of the cyber-environment on the natural environment: The case of Latest Sightings and the Kruger National Park

Woudi von Solms

Senior Lecturer: Tourism, University of Mpumalanga

E-mail: woudi.vonsolms@ump.ac.za

Abstract

The cyber-environment allows people to communicate via new platforms using the internet and devices such as mobile phones and tablets. Examples include Facebook and WhatsApp. Research has shown that an individual's online behaviour can affect their offline behaviour when humans use the cyber-environment and mobile applications to communicate. This paper considers how mobile technologies can affect behavior that impacts the natural environment. Mobile applications such as TripAdvisor, Geocaching and Latest Sightings allow tourists to post reviews of tourism destinations and attractions. Location-based technologies give exact locations of objects or sights that motivate people to travel to specific destinations. Lately, the extent to which the use of the Latest Sightings app impacts the natural environment of the Kruger National Park (KNP) has been debated by the South African National Parks board (SANParks). Latest Sightings is a cell phone application that allows users to upload the exact time and location of the sighting of specific animals within the KNP. There is thus a greater possibility that visitors will see specific animals. This paper discusses the concept of responsible tourism technologies and how location-based tourism technologies can actually increase environmental responsibility. Geocaching is another example of how location-based technology is used to encourage people to visit specific destinations and be environmentally responsible. Geocaching is an international treasure hunting game that involves the use of GPS coordinates by participants to hide treasures, or caches, at specific tourist attractions. Fellow participants download the GPS coordinates and follow clues to find the cache – a hidden container with a logbook and trinkets inside. This paper makes use of desktop research to make recommendations concerning possible protocols that must be put in place to limit negative impact on the natural environment when technology is used by tourists.

Keywords

Cyber-environment, mobile technologies, responsible tourism technologies, Geocaching, Latest Sightings, environmental responsibility, Kruger National Park

1. Introduction

Research has been done on cyber safety and cyber security and how individuals can behave responsibly in an online environment (UK Government, nd; DHS, 2016;

Cybercrime, 2016). For the purposes of this paper the “cyber-environment” or “cyber-space” references online tourism organisations that includes Latest Sightings, TripAdvisor and Geocaching. The cyber-environment changes how tourists engage with and support tourism organisations and destinations. The cyber-environment enables tourists to gain remote but up-to-date information on tourism destinations and attractions and also customise travel arrangements (Ross, 2015:87-88; Limberger, dos Anjos, de Souza Meira & dos Anjos, 2014:59; Amoral, Tiago & Tiago, 2014:137-139). The cyber-environment can also provide information on tourists’ safety at specific tourism destinations. The Geocaching and TripAdvisor websites inform visitors of responsible activities and protocols that must be followed to ensure personal safety (Geocaching, 2016; TripAdvisor, 2016). Electronic word-of-mouth (e-WOM) is the term used when tourists inform each other and exchange information relating to tourism destinations, attractions and experiences with other tourists. Such online communication is seen as more effective and immediate than traditional means of communication (Nizamuddin, 2015:70-71; Matos-Rodriguez, 2014:1-3).

2. Objective and methodology

This paper focuses on how, when tourists use the cyber-environment to gain information about sights and on the natural environment, technologies must be used responsibly in order not to lead to negative consequences for the environment. This study was sparked when Latest Sightings and the Kruger National Park were featured in the news in June 2016. News articles highlighted the characteristics of Latest Sightings and the reasons the Kruger National Park (KNP) was unhappy with the application being used within the park. These characteristic and reasons have both been considered and further desktop research has identified and investigated two other online tourism organisations to determine how the problems between Latest Sightings and the KNP can be avoided and solved.

3. Popular tourism cyber technologies

Numerous deployments of the word ‘cyber’ have been researched. Descriptions agree that ‘cyber’ is a prefix that refers to computer-related activities, the culture of using computers, future technological development and/or the use of computer networks, virtual reality and the Internet (Clark, 2010:1-4; Oxford, 2016; Merriam Webster, 2016; Cambridge, 2016). Clark (2010:1-4) agrees, but elaborates by mentioning that cyber-environments can also include the communication of information between people through electronic devices – such as cell phones or tablets. How cyberspace is used influences how people experience it and may vary depending on people’s preferences and geographic region (Clark, 2010:1-4). The cyber-environment has changed the structure of tourism (Kourtiti, Nijkamp *et al*,

2011). Cyber-tourism refers to a tourism experience that occurs within a cyber-environment only. Therefore, cyber-tourism does not involve any physical impact on the natural environment or transportation to a physical tourism destination or attraction (Ross, 2015:87-88). Cyber-communication can help to reduce or further enhance face-to-face experiences, depending on the individuals, the situation or the technology. The physical experience between tourists and the tourism destination or attractions can be mediated by information communicated in the cyber-environment (Ross, 2015:89). Electronic-Tourism (e-tourism) involves information technology being incorporated into the tourism industry and aim to make processes more efficient (Khosrow-Pour, 2015:3646). E-tourism differs from cyber-tourism. E-tourism reduces geographic differences, reduces the time spent on tourism activities and increases tourist interaction with tourism organisations and other travelers (Kourtiti, Nijkamp *et al*, 2011). Certain organisations that operate within a cyber-environment have combined the characteristics of cyber-tourism and e-tourism. Three such organisations are TripAdvisor, Latest Sightings and Geocaching. These were chosen for this research study as they are organisations that involve constantly-updated information that influences travel decisions, necessitates interaction between individuals, and involves individuals sharing trustworthy information and locations of attractions (Limberger, dos Anjos, de Souza meira *et.al.*, 2014:59-61).

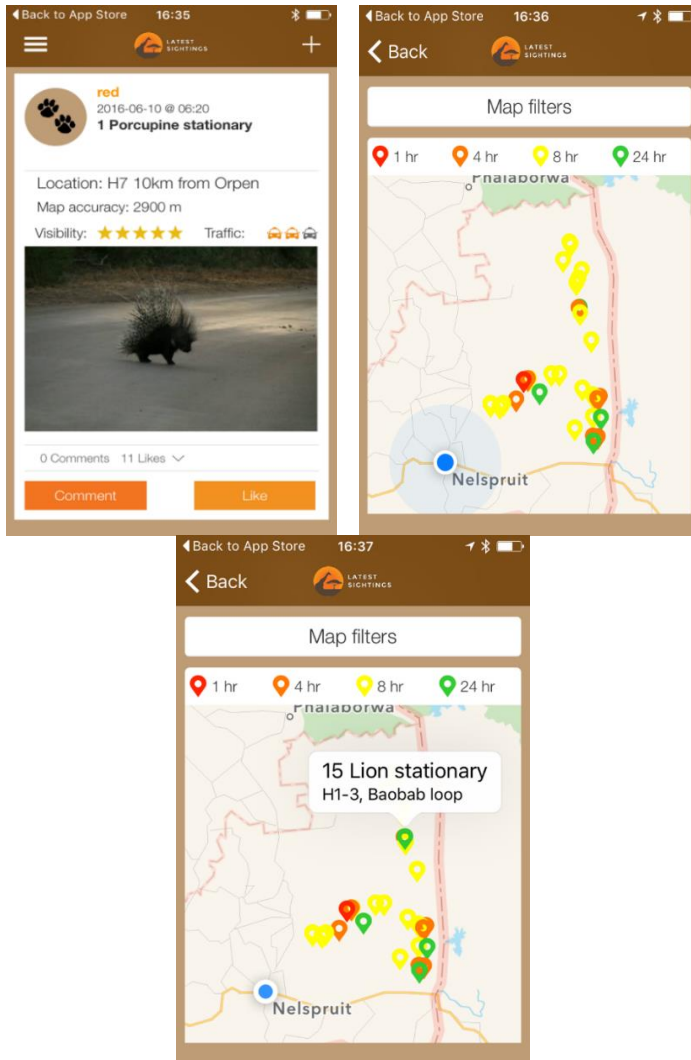
3.1 TripAdvisor

TripAdvisor was created in 2000 and mostly involves reviews from customers. The organisation is the online world leader in helping tourists to make travel decisions (Limberger, dos Anjos, de Souza Meira *et.al.*, 2014:59; Chua & Banarjee, 2013:23-25). TripAdvisor is the largest online platform that distributes tourism-related information between approximately 350 million tourists that make use of TripAdvisor to share information. Visitors to TripAdvisor create a username and password and can post comments that relate to specific tourism destinations or attractions without their real identity becoming known (TripAdvisor support, 2016; Matos-Rodriguez, 2014:1-3). The website boasts more than 170 million reviews and is visited by more than 280 million travellers (Matos-Rodriguez, 2014:1-3). On average, one comment is posted every second. Fellow tourists and tourism organisations can respond to the posts. TripAdvisor uses technology to screen the posts to ensure that the posts are family-friendly and not fraudulent. The screening process takes up to 48 hours and research has shown that reviews are reliable (Cordato, 2014:259; Chua & Banarjee, 2013:23-25). Biased or fraudulent comments as well as private or promotional content cannot be posted. Second-hand information and posts about experiences that are older than one year are also discouraged. Tourism destinations or attractions are not allowed to post comments regarding their own establishments, unless these are in response to a post by a tourist (TripAdvisor support, 2016). Tourists that post on TripAdvisor agree that the information they post is their own opinion, that they have no relationship with the organisation featured in the post and that they are not paid to make the post. If the screening process flags a post, the post is removed. Tourism organisations are also encouraged

to flag and report fake reviews (Cordato, 2014:259-260). The website allows visitors to select a location and type of organisation to see reviews from other travelers or make a booking. To view posts, the first step is to choose a destination and the type of organisation or activities that are of interest. General information on the destination can be obtained from the 'Overview' option. Alternatively, information can be obtained on hotels, flights, attractions or activities and restaurants. Upon clicking on one of these options, a new window is opened that gives information on the hotel and the reviews posted by other visitors (TripAdvisor, 2016).

3.2 Latest Sightings

Nadav Ossendryver created the Latest Sightings website and cell phone application in 2011 after he visited the Kruger National Park (KNP). The number of members soon reached 76 000 (News24, 2016b). The aim of the Latest Sightings cell phone application (L.S. app) is to encourage people to see wildlife and to collaborate with the park to protect wildlife (Sguazzin, 2016). Ossendryver said that he is willing to work with the KNP to look at the effects the L.S. app has on the KNP (BBC, 2016). The researcher downloaded the app. Upon downloading the app, you can choose an applicable national park and the types of animals you want to see. A username, real name and email address are necessary to register. Screenshots of the app are given below (Latest Sightings, 2016):



**Image 2: Latest Sighting cell phone application – post and maps
(Latest Sightings, 2016)**

The first screenshot on the left shows the posts by the L.S. app users. The post shows what animals visitors saw and how visible the animal(s) were. Regular updates also give the time, location and amount of traffic at the sighting. Other Latest Sightings users can then comment on and/or like the post. L.S. app users can access a map which informs them where and for how long ago the animals were sighted. Image two and three are examples of the map. The colour of the icon varies depending on how long ago wildlife was seen at that specific location. The type of animal and exact location are given if L.S. app users click on the map. The location of the L.S.

app user is also given (Latest Sightings, 2016.). In order to receive updates, cell phone reception is necessary but at present this is only available in certain areas within the KNP (SANParks, 2016).

6.1. 3.3 Geocaching

The United States increased GPS accuracy when they removed Selective Availability in May 2000 (Dyer, 2010:v; Peters, 2004, 6, Geocaching, 2016). In response, Dave Ulmer filled a container with books, videos and pens and hid the container in Portland. He took the GPS coordinates and posted the GPS coordinates on the Internet with a message. The message encouraged people to use the GPS coordinates to find the container and replace any item with another item that is of the same or greater value. Mike Teagan was the first to find the treasure (Dyer, 2010:3-8; Peters, 2004).

This led to a craze with an official Geocaching.com website being created in the year 2000; geocachers must now be registered to get information on geocaching and geocache locations. Participants of the game are called ‘geocachers’ and non-participants are called ‘muggles’. The containers in which trinkets are hidden are called ‘caches’ or ‘geocaches’. Over 3 million geocachers and an almost equal number of caches make geocaching the largest treasure-hunting and outdoor adventure game to date. Geocachers have found caches over 241 million times in 184 countries on all seven continents and even at the bottom of the ocean. South Africa has approximately 7900 caches (Geocaching, 2016).

Geocaching encountered problems when landowners complained that geocaching caused environmental damage to their properties. Examples of such organisations are national parks (Wilderness, 2004). The geocaching website attempts to make registered members aware of what not to do. For example, that they should not break the law. In certain areas law enforcers are aware of geocaching and are able to reprimand geocachers for unlawful actions. Premium geocaching members help to ensure that the correct procedures are followed when a new cache is hidden. Lastly, property owners must give permission for each individual cache to be hidden on their property. If these rules are not followed, Geocaching reserves the right to terminate membership or to remove a cache (Geocaching, 2016).

Geocachers hide caches in various locations. The level of difficulty in locating the caches and the kind of terrain in which the caches are hidden vary – making it more or less difficult to find a cache. To participate in the game, one can seek and/or hide caches. Members register on the website for free by giving their real name, a user name, email address and location. The website gives clear instructions on the do's and don'ts of the game. Locations of existing and new geocaches can only be found on the website or cell phone application if accessed by a registered user. The image below shows a map giving the location and types of geocaches (Geocaching, 2016).

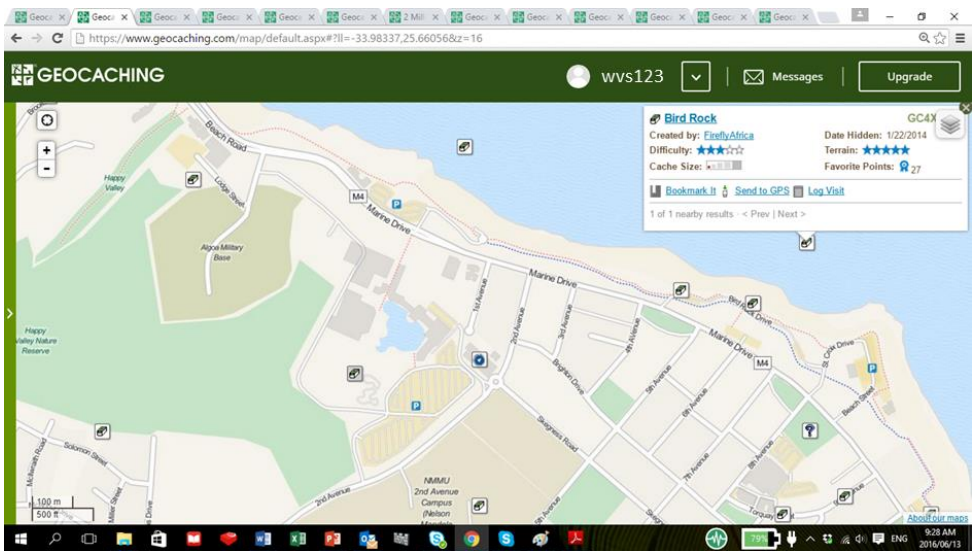


Image 2: Map of geocaches (Geocaching, 2016)

The screenshot above indicates the username of the geocacher in the top right-hand corner. The majority of the screen shows a map of the Port Elizabeth beachfront area and shows the caches in that area. Upon clicking on a cache, some information is given about the cache in a white pop-up window. The cache link on the map gives the geocacher the name of the cache next to an icon that shows the type of cache. The name of the geocacher who hid the cache, the date the cache was created, and the size of the cache are also provided. The difficulty level for this cache is three (average difficulty) and the terrain is five (very difficult to access). Geocachers who are interested in finding this cache can choose to bookmark it if they want to find it at a later stage or send the GPS coordinates straight to their GPS device if they plan to find it immediately. If the cache has already been found, the geocacher can click on the 'log find' link to gain further information. The link directs the geocacher to a clue that gives information on the specific geocache, the GPS coordinates and how difficult it is to find (Geocaching, 2016; Dyer, 2010:77-90; Cameron, 2011:11-20).

Bird Rock

A cache by [FireflyAfrica](#) [Message this owner](#) Hidden : 1/22/2014

Difficulty: ★★★★★
Terrain: ★★★★★

Size: (micro)

27 Favorites

GC4XC7G ▼

Log your visit

[View Gallery](#) (50)

[Watch](#) (5)

[Bookmark](#)

[Ignore](#)

S 33° 58.905 E 025° 40.160

UTM: 35H E 377085 N 6239069

In Eastern Cape, South Africa
► E 416.4 mi from your home location

[Print](#): [No Logs](#) [5 Logs](#) [10 Logs](#) [Driving Directions](#)

[Download](#): [Read about waypoint downloads](#)

[LOC waypoint file](#) [GPX file](#) [Send to My GPS](#)

Please note Use of geocaching.com services is subject to the terms and conditions [in our disclaimer](#).

Geocache Description:

The cache is situated on Bird Rock between Hobie Beach and Pollok Beach. Bird Rock is very much an island on the beachfront as its always surrounded by water. The rock got it's name from the fact that there are always cormorants and gulls sitting on it and most of the higher parts of the rock is covered in white "guano".

Bird Rock cache could either be attempted at low tide if you don't want to swim too far or high tide when the climb onto the rock is easier. It is best to go equipped with snorkling gear and be careful while climbing on the rock if the sea isn't flat. The cache container is a plastic tablet container wedged in a crevice on the land side of the rock towards the high point from the middle to keep it out of reach of waves as much as possible. Please wind or sun dry your hands as much as possible before taking the log sheet out so that the log sheet will stay dry. I will be checking up on the cache to make sure everybody who log it did sign the log sheet. If more than one team do it together, please sign it seperately.

Congrats to Blaster88 and Rescue33 on a FTF well done

Additional Hints ([Decrypt](#))

Fcyfv fcyfu

Decryption Key

A|B|C|D|E|F|G|H|I|J|K|L|M

N|O|P|Q|R|S|T|U|V|W|X|Y|Z

(letter above equals below, and vice versa)

[What are Attributes?](#)

[Advertising with Us](#)

58 Logged Visits

43 5 5 1 1 2

[View Logbook](#) | [View the Image Gallery of 50 images](#)

[Decrypt](#)

****Warning! Spoilers** may be included in the descriptions or links.

Current Time: 06/13/2016 00:33:02 Pacific Daylight Time (07:33 GMT)
Last Updated: 2016-06-09T14:45:27Z on 06/09/2016 07:45:27 Pacific Daylight Time (14:45 GMT)
Rendered From:Unknown
Coordinates are in the WGS84 datum

Image 3: Geocaching clue (Geocaching, 2016)

At the top of the clue, similar information is given to that which was given on the map. Directly below are driving directions, waypoints and GPS coordinates that give information on reaching the cache location. In the middle of the clue, information is given about the area and suggestions on how to approach the cache. An additional encrypted clue is given that will help geocachers find the cache upon arrival at the location. Below the description it states that 43 people have found the cache and 5

haven't. The geocacher can view five comments that relate to the find and see that the cache has been temporarily disabled once, listed and published once, and needed maintenance twice. Additional information is given on the right-hand side of the screen. It gives links to photos people have taken and allows the geocacher to ignore this particular geocache, bookmark it for later, or log it. Below these options appear the attributes of this particular cache. The attributes indicate that it is not advisable for geocachers to look for this cache at night and that it is not safe for children. There are picnic tables, public phones, restrooms and transport available at the site. Swimming, wading, scuba gear or a boat may be necessary to reach the cache. Lastly, the cache involves difficult climbing and is located in a scenically beautiful area (Geocaching, 2016; Dyer, 2010:77-90; Cameron, 2011:11-20).

Both the geocaching and L.S. apps impact the natural environment to a greater or lesser degree. The next section briefly explains responsible tourism when it comes to natural environments and how technology impacts the natural environment.

4. Tourism related cyber-technologies and the impact on responsible tourism

The Department of Tourism states that responsible tourism contributes to conservation, involves local people in decisions and offers environmental experiences that are enjoyable, meaningful and educational (Department of Tourism, 2016). Responsible tourism is seen as important by the South African government, but it is debatable how invested businesses are in promoting responsible tourism. Responsible tourism aims to improve the attractions and destinations that tourists visit and is defined as activities that aim to reduce the negative impact on the environment, while simultaneously benefitting an area in economic, social and environmental ways. Furthermore, the aim is to improve the attractions and destinations that tourists visit (Tichaawa & Samhere, 2015:402-403). The factors that are necessary to encourage responsible tourism have been widely debated (Carasuk, Becken & Hughey, 2016:23). The South African National Parks board (SANParks) suggests that responsible tourism means tourism that is integrated with the environment, takes into account the local population and economy. Responsible tourism stems from the realisation that tourists and organisations can have a negative impact on the environment and that responsible tourism practices should encourage tourists and organisations to become more aware of their actions (Tichaawa & Samhere, 2015:402-403, News24, 2016a&b). Latest Sightings has incorporated responsible tourism through projects that include the Predators Project in the Greater Kruger Park, the Wild Dog Project, the Martial Eagle Project, the Ground Hornbill Project and the Project Rhino KZN/Operation Change/Wildfest projects (News24, 2016c).

However, due to the technology involved, it is debatable whether Latest Sightings' and SANParks' definitions of responsible tourism are the same. In News24 articles of 8 to 14 June, the impact of technology on the natural environment in South African national parks is said to be so negative that SANParks is considering legal action to disallow KNP visitors to use the L.S. app. It is said that the L.S. app encourages tourists to disregard SANPark rules and policies. Accusations of irresponsible behaviour mention that the Latest Sightings app encourages tourists to ignore the speed limit in the park, causing increased congestion at wildlife sightings and increased animal deaths due to speeding.

The Latest Sightings website and cell phone application does not inform or remind tourists that it is their responsibility to follow park rules and laws when the L.S. app is used. The next section analyses TripAdvisor, Geocaching and Latest Sightings in terms of what aspects could enable these technology-based organisations to be more environmentally responsible.

5. Critical analysis of the three cyber technologies

The discussion above mentions similarities and differences between the three online organisations that are highlighted below. The first similarity is that, through technology, accurate and up-to-date information on tourist attractions and destinations is posted and shared by travelers via mobile devices connected to the Internet. The second similarity is that all three online organisations influence the behaviour of tourists. The third similarity involves environmental responsibility which is incorporated into all three online organisations to a greater or lesser degree before, during and after the use of technology. A fourth similarity is that all three online organisations are dependent on external or third-party organisations that are separate and not directly related to the online organisation.. Furthermore, the organisations have rules that must be adhered to by travellers and the organisations themselves. The differences between the three online organisations are discussed below.

All three organisations offer cell phone applications that involve location-based technologies. TripAdvisor shows the locations of tourist attractions whereas Latest Sightings and Geocaching show the location of the tourists and the attraction. The location plays an important role as it motivates tourists to travel to specific destinations TripAdvisor and Geocaching involve worldwide travel destinations, whereas Latest Sightings only involves local destinations within certain National Parks in South Africa. The attractions posted on TripAdvisor and the location of

geocaches on the geocaching website are both stationary. Thus, regardless of how long tourists take to travel to the destination, the attraction and geocache will still be at the same location. On the other hand, the wildlife posted on the L.S. app does not remain stationary. So, if a tourist takes too long to reach the location, the animal may not be at the same location anymore.

TripAdvisor does not implement policies regarding environmental responsibility. However, organisations that practice environmental responsibility receive positive reviews and recognition from tourists. Geocaching actively encourages environmental responsibility and incorporated environmental responsibility as part and parcel of the activity soon after it was established. Geocachers must follow certain rules when they hide or seek caches to ensure that the natural environment is not harmed. If the environmental responsibility portion of the game were removed, it could affect the activity as it currently exists. With Latest Sightings, environmental responsibility is also present, but it is not necessarily part of the activity when travellers use the L.S. app. Environmental responsibility takes the form of additional activities. If the environmental responsibility and conservation activities were removed, people could still use the L.S. app to locate and view wildlife.

All three organisations depend on the property of third parties. TripAdvisor and Geocaching encourage people to visit destinations internationally. If one property owner chooses not to be involved with TripAdvisor or geocaching, it will have a minimal impact on the two organisations. Latest Sightings is a South African company that can only be used in a limited geographical area. If the KNP restricts the use of the Latest Sightings cell phone application, it will have a significant impact on Latest Sightings, as it will restrict the activity in the whole park - a significant setback considering that the L.S. app is only used in a couple of National Parks within South Africa.

TripAdvisor does not publish reviews that are fraudulent and not family-friendly. Geocaching has a system in place where geocachers are reprimanded by fellow geocachers if they do not follow the rules. Latest Sightings does not seem to have repercussions for unlawfulness, such as speeding and reckless driving.

6. Conclusions and recommendations

If Latest Sightings adopts some of the approaches employed by TripAdvisor and Geocaching, the researcher believes that Latest Sighting can continue to work with SANParks; it should encourage tourists to use the L.S. app in a responsible manner

that is in line with the type of responsible tourism that SANParks aims for. The first consideration is to use location-based technologies to track the speed at which L.S. app users travel from their original locations to the wildlife sighting. This will establish whether the user drove recklessly above the speed limit to reach the destination or not. The second consideration relates to environmental responsibility that must be incorporated into the activity itself. Increased information on the rules of the property on which the tourists find themselves (such as the KNP) and the consequences of not following the rules should be communicated more directly to L.S. app users. To encourage L.S. app users to follow these rules, repercussions should be implemented and enforced. An example of a repercussion would be that L.S. app accounts are blocked and such users would thus not be able to locate wildlife through the L.S. app and speed to the sighting. Latest Sightings have stated that they want to work with SANParks so that the app can continue to be used within the KNP. The L.S. app user's name and email address can be supplied to SANParks so that SANParks can reprimand tourists for not following park rules. Furthermore, the location of animals can be shared with SANParks which will help SANParks to more closely monitor animals within the park.

The aim is not to isolate cyber-technologies from the tourism experience. Cyber-technologies should be incorporated into the tourism experience but should encourage responsible behaviour within the cyber physical and socio-economic environments. The aim is to have responsible tourism technologies that benefit tourists, organisations and the natural environment.

References.

- Amaral, F., Tiago, T. & Tiago, F. 2014. User-generated content: tourists' profiles on TripAdvisor, *International Journal on Strategic Innovative Marketing*, 1:137-147.
- BBC, 2016. National Park looks to ban animal apps – Wakefield, J. on 9 June 2016. [Online]. Available: www.bbc.com/news/technology-36489080 (Accessed 11 June 2016).
- Cambridge dictionary, 2016. 'Cyber'. [Online]. Available: www.dictionary.cambridge.org/dictionary/english/cyber (Accessed 15 June 2016)
- Cameron, L. 2011. *Geocache Handbook: The Guide for Family Friendly, High-Tech Treasure Hunting*. 2nd edition. Falcon Guides: Guilford.
- Carasu, R., Becken, S & Hughey, K.F.D. 2015. Exploring values, drivers, and barriers as antecedents of implementing responsible tourism, *Journal of Hospitality & Tourism Research*, 40(1):19-36.

Chua, A.Y.K. & Banerjee, S. 2013. Reliability of reviews on the Internet: The Case of TripAdvisor, *Proceedings of the World Congress on Engineering and Computer Science 2013*, Volume 1. San Francisco, USA.

Clark, D. 2010. Characterizing cyberspace: past, present and future, *MIT CSAIL*, 1(2):1-18.

Cordato, A.J. 2014. Can TripAdvisor reviews be trusted? *Travel Law Quarterly*, 6(3):257-263.

Cyber Crime, 2016. Local Resources on Cyber Crime. [Online]. Available: <http://cybercrime.org.za/local-resources/> (Accessed 15 June 2016).

Department of Tourism, 2016. What is responsible tourism? [Online]. Available: tkp.tourism.gov.za/rt/what/Pages/default.aspx (Accessed 11 June 2016)

DHS, 2016. Cyber Tips and Resources. [Online]. Available: <https://www.dhs.gov/stopthinkconnect> (Accessed 15 June 2016)

Dyer, M. 2010. *The Essential Guide to Geocaching: Tracking Treasures with your GPS*. Accessable Publishing Systems: Golden.

Geocaching, 2016. [Online]. Available: www.geocaching.com (Accessed 13 June 2016).

Khosrow-Pour, M. 2015. Encyclopedia of Information Science and Technology. 3rd edition. Hershey: Information Science Reference.

Kourtit, K., Nijkamp, P., Van Leeuwen, E.S. & Bruinsma, F. 2011. Evaluation of cyber-tools in cultural tourism, *International Journal of Sustainable Development*, 14(3-4).

Latest Sightings phone application. 2016 – 11 June 2016.

Limberger, P.F., dos Anjos, F.A., de Souza Meira, J.V. & dos Anjos, S.J.G. 2014. Satisfaction in hospitality on TripAdvisor.com: An analyses of the correlation between evaluation criteria and overall satisfactin, *Tourism & Management Studies*, 10(1):59-65.

Merriam Webster, 2016. 'Cyber'. [Online]. Available: www.merriam-webster.com/dictionary/cyber (Accessed 15 June 2016)

News24, 2016a. Wildlife phone apps cause chaos in Kruger – 8 June 2016. [Online]. Available: www.news24.com/Green/News/wildlife-phone-apps-cause-chaos-in-kruger-20160608 (Accessed 10 June 2016)

News24, 2016b. SANParks to 'curtail use of wildlife apps' such as Latest Sightings – 9 June 2016. [Online]. Available: <http://traveller24.news24.com/Explore/Bush/sanparks-to-curtail-use-of-wildlife-apps-such-as-latest-sightings-20160609> (Accessed 10 June 2016)

News24, 2016c. Wildlife sightings app restrictions to rely on 'sensible consideration' from visitors - SANParks – 10 June 2016. [Online]. Available: <http://traveller24.news24.com/Explore/Bush/wildlife-sightings-ap-restrictions-to-rely-on-sensible-consideration-from-visitors-sanparks-20160610> (Accessed 11 June 2016)

Nizamuddin, S.K., 2015. Marketing utility of TripAdvisor for Hotels: An importance-performance analyses, *Journal of Tourism*, 16(1):69-75.

Oxford dictionary, 2016. 'Cyber'. [Online]. Available: www.oxforddictionaries.com/definition/english/cyber (Accessed 15 June 2016)

Peters, J.W. 2004. *The complete idiots guide to geocaching*. New York: USA Penguin Group

Ross, G.F. 2015. Cyber-tourism and Social Capital: Ethics, Trust and Sociability, *Tourism Recreation Research*, 30(3):87-95

SANParks, 2016. [Online]. Available: www.sanparks.org. (Accessed 11 June 2016)

SANparks, 2016a. [Online]. Available: www.sanparks.org/about/responsible_tourism.php (Accessed 11 June 2016)

Sguazzin, A. 2016. Latest Sightings Disputes Claim Apps Are Harming Wildlife. [Online]. Available: www.bloomberg.com/news/articles/2016-06-10/latest-sightings-disputes-claim-apps-are-harming-wildlife (Accessed 11 June 2016)

Shop Geocaching, 2016. [Online]. Available: <http://shop.geocaching.com/default/international-retailers/> (Accessed 13 June 2016)

Tichaawa, T.M. & Samhere, S. 2015. Responsible tourism: Analysing implementation and challenges in East London using the stakeholder approach, *African Journal for Physical Health Education, Recreation and Dance*, 21(1:2):401-414.

UK Government, nd. Guidance: 10 Steps: Summary. [Online]. Available: <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary> (Accessed 25 May 2016).

Van der Merwe, P. & Saayman, M. 2008. Travel motivation of tourists visiting Kruger National Park, *Koedoe*, 50(1):154-159.

Wilderness, 2004. Geocaching Proposal: Implementing Regulations to prohibit Geocaching in National Forest Wilderness Areas. [Online]. Available: <http://www.wilderness.net/toolboxes/documents/geocaching/FS%20Geocaching%20Policy%20Paper%20DRAFT.pdf> (Accessed 13 June 2016).

WHAT TYPE OF INFORMATION ARE SOUTH AFRICANS REALLY LOOKING FOR ON FACEBOOK BRAND FAN PAGES?

K.L. Viljoen¹, B.K. Gavaza² and L. Dube³

Department of Business Management, University of Fort Hare, East London, South Africa, Eastern Cape, South Africa, 5241

E-mail: kviljoen@ufh.ac.za; bkgavaza@gmail.com and langadubs@gmail.com

Abstract

Social media has transformed the way marketers and consumers communicate with each other. Facebook has become the most popular social networking site in the world thus presenting organisations with opportunities to convey relevant information to consumers. Brand fan pages allow consumers to fully engage with a brand in their own time and according to their specific needs. This study recognises the importance of Facebook brand fan pages and their current and intended use in the marketing domain. It examines the effects of consumer's exploratory buying behaviour and the resulting influence of this behaviour on the intentions of consumers to visit Facebook brand fan pages. The theory of planned behaviour provides the primary underpinning theory in the study alongside that of the consumer decision making process.

This study employed a descriptive research design alongside a positivistic paradigm and quantitative approach. A survey was conducted amongst 384 respondents located in the towns of East London, Bhisho and Alice in the Eastern Cape Province of South Africa (SA). Convenience sampling was used to select respondents and these respondents were aged between 18 and 64 years. Various statistical tests were used to establish reliability and validity of the measurement instrument as the well as the significance of the hypotheses posed.

The study established that exploratory information seeking is significantly related to consumers' intentions to visit Facebook brand fan pages whilst on the other hand exploratory acquisition of products is not related to consumers' intentions to visit Facebook brand fan pages. Findings indicate that South African consumers visit Facebook brand fan pages to confirm their views regarding the brands they already buy, and not necessarily to find information about new brands.

Keywords

Social media, Facebook, brand fan pages, exploratory buying behaviour, brand loyalty

1. Introduction

Facebook, a social media site founded by Mark Zuckerberg in 2004, has changed the definition of socialisation (Darvell, Walsh & White, 2011). Marketers have inherently followed consumers to these social platforms for various marketing

reasons (Malmivaara, 2011). Facebook brand fan pages have found vitality in consumer engagement with marketers strategically tapping into Facebook (Tsai & Men, 2013). A brand fan page is a profile created by business or marketing managers who communicate brand-related information to its users (Chow & Shi, 2015). Beyond the primary objective of engagement between marketers and consumers, the latter are also observably relying on each other's opinions on these pages and engaging with each other in discussions around their most preferred brands. Accurately quantifying reasons for such visits has been proven to be difficult based on diversity in consumer behaviour (Wallace, Buil, de Chernatony & Hogan, 2014). However, it is believed that fans of a brand who visit Facebook brand fan pages have the same primary goal of a unified identity (Tsai & Men, 2013).

2. Research Problem

Marketers are interested in every consumer who visits their brand fan pages and identifying the factors that influence these visits would provide them with valuable information regarding their customers' behaviour (Hanzaee, 2011). Few studies currently exist which explain consumers' intentions to visit Facebook brand fan pages especially in SA. Further, a lack of understanding and evidence of how liking Facebook brand fan pages impacts on consumers' current and future visits also exists (De Vries, Gensler & Leeftang, 2012). This study sought to explore whether buying behaviour determines intentions to visit Facebook brand fan pages. The study further determined whether exploratory acquisition of products and exploratory information seeking behaviour influence intentions to visit Facebook brand fan pages. Understanding the factors that influence consumers to visit Facebook brand fan pages will help to create and develop better electronic marketing strategies.

2.1 Research Objectives

The research study's primary objective is to examine the extent to which exploratory buying behaviour influences consumer's intention to visit Facebook brand fan pages.

2.1.1 Secondary Objectives

- To determine if exploratory acquisition of products behaviour is related to consumer's intentions to visit Facebook brand fan pages.
- To determine if exploratory information seeking behaviour is related to consumer's intentions to visit Facebook brand fan pages.

3. Literature Review

Facebook is an internet application created for social connectivity and is used as a panel of interaction between individuals and organisations through texts, pictures and videos (Kaplan & Haenlein, 2010; Mansfield, 2012). Its emergence as a dominant global social networking tool has been observed across businesses and industries at large. Facebook brand fan pages' use has increased consumer opportunities for collecting brand information by including comments that enable sharing of advice between friends (Park, Wang, Yao & Kang, 2011). Consumers are increasingly using brand fan pages to interrelate with other brand customers, thus widening and supporting the importance of electronic word of mouth.

Facebook brand fan pages therefore have become an essential form of electronic word of mouth for marketers (De Vries et al., 2012). Word of mouth, in-person and electronically, is considered to be one of the most effortless yet valuable marketing communication methods that grows brand recognition and in turn improves business profits. In spite of Facebook's commercial potential, few studies have been conducted, specifically in SA, to understand what influences consumers to visit Facebook brand fan pages.

3.1 Theory of planned behaviour

The theory of planned behaviour defines consumer's intentions that result in observable actions undertaken (Ajzen & Fishbein, 1980). Summarised by the three antecedents of attitude towards behaviour, perceived behavioural control and subjectivity, an understanding of Facebook users' behaviour can be assessed through this theory (Ajzen, 1991; Cameron 2010). The theory suggests that where there is intention, there is action which allows for an assumption of a significant relationship between intentions to visit Facebook brand fan pages and actual behaviour (Ajzen & Fishbein, 1980).

3.2 Exploratory buying behaviour

Exploratory buying behaviour is explained as part of the consumer decision making process whereby consumers engage in activities to obtain stimulating experiences, brand variation and change, and to obtain information about products and brands (Hanzaee, 2011). Time constraints have a solid impact on exploratory buying behaviour as it influences consumers' intentions as well as their decisions (Malmivaara, 2011; Shin, 2014). Facebook fan pages have become a rich source of information, allowing consumers to quickly and easily explore many different brand

and product options and make a satisfactory comparison with other like-minded consumers (Huttunen, 2013).

Consumers visit social media sites such as Facebook brand fan pages to fulfil their pre-purchase information needs (Mir, 2014). The more consumers browse a Facebook brand fan page, the more likely they are to be exposed to brand information that aids in decision making. The concept of exploratory buying behaviour can be sub-divided into two elements, namely, exploratory acquisition of a product and exploratory information seeking.

3.2.1 Exploratory acquisition of products behaviour

When visiting a Facebook brand fan page, consumers are exposed to sensory stimulation through posted brand content and new ideas which will assist them in making brand and product choices (Malmivaara, 2011; Park, Kee & Valenzuela, 2009). Consequently, consumers who score high on the exploratory acquisition of products scale would enjoy unfamiliar brands and seek variety in their purchases (Huttunen, 2013). Pre-purchase information gathering helps consumers in reducing the perceived risk involved in a purchase and also to make sensible brand choices (Muntinga, Moorman & Smit, 2011). The pre-purchase search is the primary consumer motivation for using Facebook brand fan pages and it is as a result of a consumer's desire to make a quality brand purchase decision (Mir, 2014). It is likely that the search for new ideas and more variety would lead these consumers to visit more Facebook fan pages and thus be exposed to many more customers' views.

This study examines the concept of exploratory acquisition of products from both a brand loyalty and brand switching perspective. It measures the extent to which consumer's brand loyalty and brand switching is relative to their intentions to visit Facebook brand fan pages. Thus, consumers who are prone to brand loyalty will not actively seek out new and novel brands and businesses on Facebook. The formulated hypothesis is therefore:

H₁: Exploratory acquisition of products behaviour is significantly related to consumer's intention to visit Facebook brand fan pages.

3.2.2 Exploratory information seeking behaviour

Exploratory information seeking arises when consumers realise the inadequacy of the information currently held necessary to make purchase decisions (Legoh, Dauc & Ranchhold, 2009; Hanzae, 2011). Consumers will then engage in a sense-making

process that equips them with the detailed brand information they require to reduce any uncertainty they may experience. Exploratory information seeking deals with the consumers' need for cognitive stimulation through the acquisition of relevant brand knowledge (Legoh et al., 2009).

Consumers with a high need for exploratory information show enthusiasm for brand knowledge and are motivated to obtain first-hand information through engaging with others on Facebook brand fan pages (Huttunen, 2011). Due to the interactive nature of Facebook, fans of some brand fan pages establish relationships with brand experts and with other consumers, which allows for co-construction of information and engagement on the brand rather than being mere recipients of brand information, hence creating brand value (De Valck, van Bruggen & Wierenga, 2009). Based on this literature, the second hypothesis for this study is stated as follows:

H₂: Exploratory information seeking behaviour is significantly related to consumer's intention to visit Facebook brand fan pages.

4. Research Methodology

Research methodology refers to ways used by researchers to obtain, organise and analyse data (Tadić & Mamić, 2011). A paradigm is a broad view or perspective of something which explains the patterns of beliefs and practices that standardise inquiry within a discipline by providing lenses, frames and processes through which investigation is fulfilled (Crowther & Lancaster, 2008). A positivist approach was adopted for the purposes of this study which facilitated the adoption of quantitative methods to measure the extent to which consumers' intentions to visit Facebook brand fan pages is influenced by their exploratory buying behaviour. Primary data for the study was collected through a survey using a probability convenience sampling strategy. The 384 respondents who participated in the study were students and staff from the University of Fort Hare's campuses in East London, Alice and Bhisho. Students are considered to be highly technologically efficient thus they formed the majority of the sample. This data collection and sampling approach was considered to be the most time and cost effective methods for the study. The size, composition and locations of the sampling population allows for greater generalisation to a broader South African context.

The questionnaire used in the survey was constructed using existing scales from other studies. The scales include exploratory acquisition of product (EAP) items and exploratory information seeking (EIS) items developed by Baumgartner and Steenkamp (1996). These scales were used by Legoh et al. (2009) and were found to

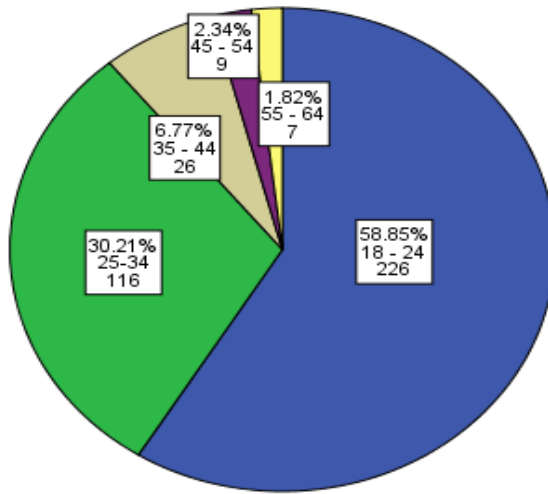
be both reliable and valid. In addition to these scales, this study also used Intention to visit (ITV) scale which was used by Shin (2014) and found to be reliable and valid. EAP and EIS were regarded as the independent variables in the study with ITV being the dependent variable. Data analysis conducted included descriptive statistics, reliability tests (Cronbach's alphas), validity tests (factor analysis) and correlation analyses.

5. Results

5.1 Biographical analysis of respondents

A total of 384 respondents were sampled with 198 being female and 186 male. The participants of the study ranged from the ages of 18 to 64. The findings, as indicated in Figure 1, showed that most of the participants ranged between 18 and 34 years old. More specifically, the majority of the sample (226 or 58.8%) were between the ages of 18 to 24; followed by 116 (30.2%) respondents between the ages of 25 to 34 years old; 26 respondents (6.7%) were between the ages of 35 to 44, and the remaining respondents (16 or 4.1%) were aged between 45 and 64.

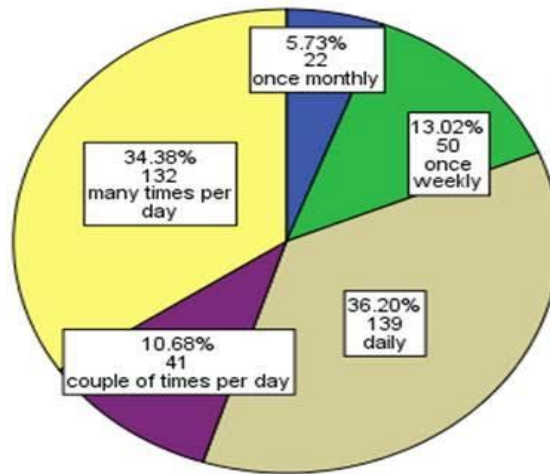
Figure 1: Age of respondents



5.2 Facebook usage of respondents

It was essential for the study to determine if respondents were in fact Facebook users as well as the extent to which the respondents engage in Facebook activities. Figure 2 indicates the level of Facebook usage that was recorded amongst respondents. Of the 384 respondents sampled, 36.2% (139) indicated that they visit Facebook daily with 45% (173) visiting the page two or more times per day. At least 13% logged in once a week with 5.7% using Facebook only once a month. These findings reveal the level of importance that Facebook has within the respondents lives and the potential influence it has on users.

Figure 2: Facebook Usage of respondents



5.3 Reliability and validity analysis

As discussed, the three scales used in this study originally all achieved acceptable levels of reliability ranging from 0.816 for the intention to visit scale; 0.709 for the EAP scale and 0.633 for EIS scale respectively. These results were above the required 0.600 Cronbach's alpha, as stated by Babbie, (2013) which means the measures were consistent and reliable.

With respect to validity, several modifications and iterations had to be conducted via factor analysis. The EAP scale, which originally consisted of 10 items, required adjustments in order for it to be validated, thus, EAP4, EAP5, EAP8 and EAP10 were removed. EAP4 and EAP5 referred to variety in selecting goods in 'a shop' and 'restaurant' settings respectively thus were not deemed relevant to this context. Statements for EAP8 and EAP10 appeared to be vague and respondents did not seem to understand them clearly which impacted on the factor loadings. Further, the remaining six items of the scale splintered into two dimensions consisting of three items each. The first dimension, consisting of items EAP1, EAP 2 and EAP3, related to statements testing consumer's levels of brand loyalty, for example, 'I think of myself as a brand loyal consumer' and 'I would rather stick with a brand I usually buy than try something I am not sure of'. The second dimension comprised of items EAP6, EAP7 and EAP9, these statements questioned consumers on their brand switching behaviour, for example, 'If I like a brand, I rarely switch from it to try

something different'. The factor loadings for the EAP brand loyalty dimension ranged between .674 and .756 and between .638 and .705 for the EAP brand switching component of the scale.

In terms of the validity of the EIS scale, items EIS1, EIS3, EIS5, EIS7 and EIS9 were reverse stated, thus were removed in order to achieve validity for the scale. The five items eliminated all alluded to consumers not being interested in product or brand information whereas the five items retained (EIS2, EIS4, EIS6, EIS8 and EIS10) related to consumers who actively seek out information on products and brands. Principal component analysis produced factor loadings of between .466 and .710 for the retained items.

Reliability of the modified independent constructs was then re-tested. Re-test reliability is a test used to determine or measure the consistency of a construct after some alterations on the scale items or over a period. It confirms that there is no change in the quality of constructs. It can also be perceived as the degree to which a score is steady and consistent when measured at different times in different ways or with different items within the same scale (Zikmund & Babin, 2013). Alpha's for re-test reliability were all over .600 thus a careful balance between reliability and validity was attained.

5.4 Correlations analysis

A Pearson correlation analysis was used to determine if a relationship exists between EAP brand loyalty, EAP brand switching behaviour, EIS and the ITV Facebook brand fan pages. As illustrated in Table 1, the two dimensions of EAP (brand loyalty and brand switching), although significantly related to each other at .570, both showed no significant relationships to intention to visit Facebook brand fan pages. Correlations results for EAPloy and EAPswit in relation to ITV were .089 and .025 respectively. Therefore, neither EAP brand loyalty nor brand switching behaviour is related to a consumer's intention to visit Facebook brand fan pages. The EIS construct shows a correlation of .289** with the dependent variable, which indicates that EIS is related to the consumer's action when intending to visit a business's Facebook brand fan page.

Table 1: Correlations of variables

Constructs	EAPloy	EAPswit	ITV	EIS
EAPloy Correlation	1	.570**	.089	.214
Sig. (2-tailed)		.000	.81	.000
N	383	383	381	383
EAPswit Correlation	.570**	1	.025	.142**
Sig. (2-tailed)	.000		.622	.005
N	383	383	381	383
ITV Correlations	.089	.025	1	.289**
Sig. (2-tailed)	.081	.622		.000
N	381	381	382	382
EIS Correlation	.214**	.142**	.289**	1
Sig. (2-tailed)	.000	.005	.000	
N	383	383	382	384

****.** Correlation is significant at the 0.01 level

5.5 Hypotheses testing

The P-values for the correlation results of the EAP dimensions (brand loyalty and brand switching) in relation to ITV were .081 and .622 respectively. The P-value scores confirmed that EAP overall does not influence consumers' intention to visit Facebook brand fan pages. The P-value of .000 proved that EIS is significantly correlated to intention to visit Facebook brand fan pages. When consumers are anxious to obtain product or service knowledge of a certain brand, they are bound to engage in what is called exploratory information seeking to increase their knowledge. This search mode results in consumers visiting various information sources, among which are Facebook brand fan pages. These findings are consistent with previous studies showing that that consumers' need for brand knowledge and information leads to engagement with Facebook brand fan pages (Huttunen, 2013; Chen, 2012 and Hanzaee, 2011). Moreover, the combination of these hypotheses

results, indicate that consumers who search for information on Facebook brand pages do not necessarily do so with the intention to switch brands, they do so for brand and product confirmatory reasons.

6. Discussion

The findings conclude that although consumers seek information about products and brands on Facebook brand fan pages, they are doing so for confirmatory reasons. This means that they do not actively search Facebook for new brands and products but instead opt to reinforce what they know about the current brands and products that they are aware of and/or use. Facebook brand fan pages thus have a large role to play in reducing consumer cognitive dissonance in the purchase decision making process as opposed to playing roles in the idea generation and information gathering stages as has been previously believed. It is important to note that a possible explanation for this finding is that consumers are not prepared to 'like' an unknown brand or business on Facebook, preferring to engage with those brands and businesses which they are familiar with. In addition, this finding could be related to Facebook brand fan pages acting as a medium or referral platform for consumers. Notwithstanding these explanations, the final result that consumers visiting Facebook brand fan pages can be construed as brand loyal customers is an important aspect for marketers to consider.

Based on these findings, it is recommended that marketers and business managers need to ensure that they display a vast array of product or service related information on Facebook brand fan pages to aid consumers in both pre and post decision-making. Furthermore, businesses must make use of customer loyalty strategies on Facebook brand fan pages in order to reward loyal customers thus differentiating their brands position in the marketplace. It is also recommended that marketing managers to try to match consumers needs with brand information they are searching for and to develop personalised marketing communications strategies, alongside loyalty strategies, to meet these needs. Further, they should be taking note of what other consumers are saying about their brand and/or business and allow more opportunities for engaging with customers leading to the co-creation of brand knowledge and the further enforcement of brand loyalty.

7. Conclusion

The study's aim was to establish if exploratory buying behaviour influences consumers' intentions to visit Facebook brand fan pages. Evidence from literature and this study indicated that there is a relationship between exploratory buying behaviour and consumers' intention to visit Facebook brand fan pages. This study

revealed that exploratory acquisition of products is not related to consumer's intentions to visit Facebook brand fan pages, whilst exploratory information seeking is positively related to consumer's intentions to visit Facebook brand fan pages. Thus Facebook brand fan pages need to be equipped with a rich variety of brand information to support existing brands in the marketplace and should not ideally be used as a communication medium for new brands. The findings of this study will assist organisations to streamline and categorise the information provided on Facebook brand fan pages in order to attract a larger and more specifically targeted audience.

8. References

- Ajzen, I. (1991) The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes* 50, 179-211.
- Ajzen, I. and Fishbein, M. (1980) *Understanding attitudes and predicting social behaviour*. Upper Saddle River: Prentice-Hall.
- Alleyne, P. and Broome, T. (2011) Using the Theory of Planned Behaviour and Risk Propensity to Measure Investment Intentions among Future Investors. *Journal of Eastern Caribbean Studies*, 36(1) 1–20.
- Babbie, E. (2010) *The Practice of Social Research*. (12th ed.). Belmont: Cengage.
- Baumgartner, H. & Steenkamp, J.B.E.M. (1996) Exploratory consumer behaviour: Conceptualization and Measurement. *International Journal of Marketing*, 13(2), 121-137.
- Cameron, R. R. (2010) *Ajzen's Theory of Planned Behaviour Applied to The Use of Social Networking By College Students*, 1–34. Retrieved from <https://digital.library.txstate.edu/bitstream/handle/10877/3298/fulltext.pdf>. (Accessed on 1 April 2015).
- Chen, H. (2012) *Relationship between Motivation and Behaviour of SNS User*. *Journal of Software*, 7(6), 1265-1272.
- Chow, W. S. and Shi, S. I. (2015) Investigating customers' satisfaction with brand pages in social networks sites, *Journal of Computer Information Systems*, 55(2), 48-58.
- Crowther, D. and Lancaster, G. (2008) *Research Methods: A Concise Introduction to Research in Management and Business Consultancy*. Butterworth-Heinemann.
- Darvell, M. J., Walsh, S. P. and White, K. M. (2011) Facebook Tells Me So : Applying the Theory of Planned Behaviour to Understand Partner-Monitoring Behaviour on Facebook. *Cyber psychology, Behaviour and Social Networking*, 14(12), 717-722.
- De Valck, K., van Bruggen, G.H. and Wierenga, B. (2009) "Virtual communities: A marketing perspective". *Decision Support Systems*, 47(3), 185–203.

- De Vries, L., Gensler, S. and Leeflang, P. S. (2012) Popularity of brand posts on brand fan pages: an investigation of the effects of social media marketing, *Journal of Interactive Marketing*, 26(2), 83-91.
- Hanzaee, K. H. (2011) Pre-Purchase Intentions of Consumers: based on Flow Theory and Navigational Characteristics of Websites. *Interdisciplinary Journal of Research in Business*, 1(4), 83–93.
- Huttunen, E. (2013) *Associations between life satisfaction, time use and exploratory buying behaviour - Quantitative exploratory study among Finnish business students*. Master's thesis. Department of Marketing Aalto University School of Business.
- Kaplan, A.M. and Haenlain, M. (2010) Users of the world, unite: The challenges and opportunities of social media. *Business Horizons*, 53(1), 59-68.
- Legoh, P., Dauc, B. and Ranchhold, A. (2009) Culture, Time Orientation, and Exploratory Buying Behavior, *Journal of International Consumer Marketing*, 21: 93–107.
- Lehohla, P. (2011) Census 2011 results are accurate. South African government news agency. Retrieved from <http://www.sanews.gov.za/south-africa/census-2011-results-are-accurate-lehohla>. (Accessed on the 15th of September 2015).
- Lin, K and Lu, H, (2011) Intention to Continue Using Facebook Fan Pages from the Perspective of Social Capital Theory. *Cyberpsychology, behaviour, and social networking*, 14(10), 565-570.
- Malmivaara, T. (2011) *Motivations behind liking: Implications of Facebook brand community behaviour on purchase intentions*. Master's thesis. Department of Marketing Aalto University School of Economics.
- Mansfield, H. (2012). *Social Media for Social Good: A How-To Guide for Non-profits*. (7th ed.). New York: McGraw Hill.
- Mir, I. A. (2014) Effects of Pre-Purchase Search Motivation on User Attitudes toward Online Social Network Advertising: A Case of University Students. *Journal of Competitiveness*, 6(2), 42–55.
- Muntinga, D.G., Moorman, M. and Smit, E.G. (2011) Introducing COBRAs: Exploring Motivations for Brand-related Social Media Use. *International Journal of Advertising*, 30(1), 13-46.
- Nelson-Field, K., Riebe, E. and Sharp, B. (2012) What's not to "like?" can a Facebook fan base give a brand the advertising reach it needs? *Journal of Advertising Research*, 52(2), 262–269.
- Park, C., Wang, Y., Yao, Y. and Kang, Y. R, (2011) Factors influencing eWOM Effects: Using Experience, Credibility and Susceptibility. *International Journal of Social Science and Humanity*, 1(1), 74-79.
- Park, N., Kee, K.F., & Valenzuela, S. (2009) Being Immersed In Social Networking Environment: Facebook Groups, Uses and Gratifications, and Social Outcomes. *Cyber psychology & Behaviour*, 12(6), 729–33.

Tadić, D. P. and Mamić, M. D. (2011) Market Research in Function of Business Process Management. *International Journal of Management Cases*, 13(4), 279–285.

Tsai, W.-H.S. and Men, L. R. (2013) Motivations and antecedents of consumer engagement with brand pages on social networking sites. *Journal of Interactive Advertising*, 13(2), 76–87.

Shin, II, S. (2014) Examining social networking community users' perception of company fan page use, behavioural intention, and actual visiting behaviours. *Journal of Consumer Behaviour*, 44(2), 1–141.

Wallace, E., Buil, I., de Chernatony, L. and Hogan, M. (2014) Who “likes” you...and why? A typology of Facebook fans: From “fan”-atics and self- expressive to utilitarian and authentic. *Journal of Advertising Research*, 54(1), 92–109.

Zikmund, W. G. & Babin, B.J. (2013) *Essentials of Marketing Research*. Australia: Cengage.

Me, my cell and I: Selfhood in the Digital Age

Jessica Oosthuizen
Associate Professor Kevin Thomas
Associate Professor Elelwani Ramugondo

University of Cape Town
jess.oosthuizen@uct.ac.za

Abstract

There is growing interest in understanding the pervasive role that cellphones play in young people's lives, and in how these devices impact psychological development and wellbeing. Recent research shows that many young people prefer socialising online, rather than interacting face-to-face. These devices have become normalised within their peer groups. They are an integral part of how young people relate to the world, each other, and importantly themselves. This paper aims to contribute to a crucial question: How do we enable young people to draw on inner resources to develop healthy relationships with their cellphones in order to support, rather than undermine, psychosocial development. Much of the available research in this field focuses on evaluating heavy cellphone or Internet use in the framework of an addiction. Although there is a mounting body of evidence suggesting that cellphone use has negative effects on young people's psychosocial development, framing this behaviour as an "addiction" might not be beneficial to young users or to society. Specifically, the addiction rhetoric denies young people's potential to realise their agency in social situations, both on- and offline. An alternative focus for research on the psychosocial effects of young peoples' cellphone use is, therefore, on the self. An important focus of cyberpsychology research should be investigating ways to enable young people to recognise and exercise their agency in on- and offline social situations. Among the mechanisms of agency, none is more central or pervasive than people's beliefs about their capabilities to exercise control over their own level of functioning. However, the current literature has not clearly defined the role of self-belief in the relationship that young people have with their cellphones (and, in turn, with their on- and offline social behaviour). This paper explores the possibility that an assessment of self-processes that stimulate a positive self-view might bring researchers closer to understanding the deep attachment that young people have to their cellphones. Furthermore, this paper questions whether evaluating self-view through the often-used construct "self-esteem" perpetuates notions of conditional self-worth. I propose that self-compassion (i.e., compassion turned inward) could make an important contribution to this field of study. Emerging research shows that self-compassion predicts more stable feelings of self worth than self-esteem, and may promote resilience. Furthermore, self-compassion may be an important avenue to explore in promoting young South Africans psychosocial development, and thus empowering them to exercise their agency both on- and offline.

Keywords

Cellphones, Cyberpsychology, Self-compassion

The financial assistance of the National Institute for the Humanities and Social Sciences (NIHSS) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NIHSS.

Introduction

The pervasive presence of cellphones in young people's lives, and the subsequent preoccupation of those young people with using these devices and engaging with each other online, has introduced a new field of psychological enquiry: Cyberpsychology. One primary focus of inquiry driving this field is to find out how these devices influence the wellbeing and social development of young people.

Growth in Internet users has been steady during the last decade; with a net increase of 200 to 300 million people every year (Facebook, 2016). Most cyberpsychological research is conducted in the global north, where most of the population in developed countries has Internet access (Facebook, 2016). The need for more South African cyberpsychological research is illustrated by the fact that the total number of mobile (cellphone) Internet subscribers in this country is predicted to increase from 19.5 million in 2014 to 38.0 million (or 70% of the population) in 2019 (PricewaterhouseCoopers, 2015). Furthermore, two of the very few local cyberpsychological research papers describe how the negative impact of cellphone use in African schools is becoming increasingly apparent (Porter et al., 2016; Swanepoel & Thomas, 2012).

This paper presents a targeted narrative review of cyberpsychology literature that aims to reveal the deep attachment that young people have towards their cellphones. However, rather than contributing towards the literature that regards the nature of the relationship as an "addiction", this paper proposes an alternative way of understanding this relationship, where the focus is not on user behaviour but on the self. In short, I propose that the construct of self-belief could play an important role in helping researchers, clinicians, teachers, and parents to understand the nature of the relationship that young people have with their cellphones.

If one argues (quite reasonably) that young people possess the potential agency to manage their online behaviour, then discussions about cellphone use should focus on exploring ways in which they can develop their personal agency. As Porter et al. (2016) argue, in order for young people to become competent and confident digital citizens they need to be empowered to develop their own agency and to receive the necessary support to acquire these skills.

Digital natives

Today's young people represent the first generation that has grown up surrounded by and immersed in digital technologies. Internet-enabled cellphones have made it possible for most young people to access social media platforms anywhere and at any time. This level of access has given rise to a generation of young people with expectations of being always online and of being always connected (Subrahmanyam & Smahel, 2010; Turkle, 2011). Hence, the term *digital natives* has been coined to describe them (Prensky, 2001).

Emerging research reports that many young people prefer to relate to each other using cellphones, rather than via face-to-face interactions (Casale, Tella, & Fioravanti, 2013; Pierce, 2009; Walsh, White, Cox, & Young, 2011). Perhaps this situation arises because young people cannot recall what life was like without cellphones. Regardless, this device has become so embedded in the daily lives of young people that the term *nomophobia* (*no-mobile-phobia*) has been coined to describe the fear of being without your cellphone (Bivin, Mathew, Thulasi, & Philip, 2013; King et al., 2013). Certainly, using these devices has become normalised within their peer groups, and they have become an integral part of how young people relate to the world, each other, and themselves (Carbonell, Oberst, & Beranuy, 2013; Carter, 2015; Turkle, 2011). As Baker and White (2010, p. 1591) state, social networking sites are “emerging as a primary tool for adolescent socialisation”.

Clearly, the role of cellphones in young people’s lives extends beyond that of a communication device. It also extends beyond serving the social function of connecting the user to others. Cellphones function as a companion, and in many instances become embedded with notions of self. In previous research, I found that young people described their cellphone as “a part of [me]”, and stated that the experience of using feels “natural” and is “like blinking” (Oosthuizen & Young, 2015). Otherwise stated, young people experience their cellphones as being inseparable from themselves.

The view that there is co-dependency between society and technology is not new (Berthon, DesAutels, & Butaney, 2010). Since the introduction of the printing press, people’s involvement with technology and its impact on their lives has been contested and debated. However, the digital age has brought with it the potential for technology to become embodied within our identity and infused with notions of self.

Digital technologies have only existed for a relatively short time, and so it is difficult to clearly define their long-term impact on our lives. It is possible that our relationship to smartphones has the potential to shift the way we relate to ourselves by replacing our traditional understanding of self-processes – the way in which a person relates to himself or herself – with a combination of cellphone-mediated-self-processes. It is not yet known whether the role of a cellphone supports or undermines self-processes. Conducting research to investigate how cellphones affect psychosocial development is crucial.

Effects of excessive cellphone and Internet use on psychosocial development

Among digital natives, socialising online seems to hold more appeal than interacting offline. Because young people spend less and less time offline in favour of spending time online, part of the appeal of socialising online might be because they are unfamiliar with socialising offline. It is possible that this is a vicious cycle: Fears of interacting offline could encourage young people to use their cellphones as a prop,

which results in them having less opportunity for social practice, or for gathering information that would disconfirm the fear.

Social interactions play a central role in a young person's social development (Bandura, 1990, 1999b; Erikson, 1968). In particular, adolescence represents a unique developmental period during which young people need to master how to navigate complex social situations (Dahl, 2004). Thus, there is a vibrant research literature investigating how young people's potentially excessive involvement with these digital technologies might influence their overall social development.

A growing body of research reports on the negative impact that excessive cellphone use has on young people's social development and well-being (LaRose, Connolly, Lee, Li, & Hales, 2014; Rosen, Cheever, & Carrier, 2012; Uhls et al., 2014). Many researchers express concern over the capacity of children and adolescents to learn key social skills through online interactions. These researchers argue, for instance, that habitual cellphone and Internet use interferes with young people's ability to develop autonomy (Baym, 2015; Davis, 2012). If this is true, young people might be missing out of critical opportunities through which to exercise and develop agency by not engaging in enough offline socialising. Here *agency* refers to an individual's ability to recognise their goals, the value associated with these, and the ability to follow-through with pursuing them (Deneulin & Shahani, 2009).

The role of interpersonal skills in supporting a young person's development is also important to consider. Brown argues that a true sense of "interpersonal nuance can only be achieved by a child who is engaging all five senses by playing in the three-dimensional world" (as cited in Henig, 2008). This outlook cautions against socialising on a cellphone because these types of interactions take place in a two-dimensional, or on-screen, world. Furthermore, onscreen engagement predominantly involves text-based communication. This is particularly true in countries such as South Africa, where data costs limit or prevent young users from communicating using data-heavy platforms like Skype. As a result, young people establish and nurture relationships without physically engaging with their peers. Even though these text-based or online interactions are taking in real-time, which mimics the sensation of physical proximity, they lack an element of non-verbal communication, which is a crucial component in face-to-face communication. In their study on the effect of non-verbal cues on relationship formations, Kotlyar and Ariely (2013, p. 545) argue that the "limited capacity of text-based communication to convey nonverbal cues may lead to an impoverished personal interaction".

The addiction rhetoric

Clearly, much of the literature on the negative impact of cellphone and social media use refers to compulsive and excessive cellphone use. Such use is often described as "an addiction" (e.g., Byun et al., 2009; Huang & Leung, 2009; Young, 2009). Although "addiction" might be a necessary diagnosis for some people, using this term as a blanket definition for an entire generation of young people who use their

cellphones frequently is problematic. Ahn and Jung (2014) argue that framing frequent cellphone use in this way focuses on the negative outcomes of such use, and neglects to consider the users' perspective on their 'addiction'. For example, taking the young users' perspective into consideration involves recognising that the way in which they use their cellphones is normal to them because they don't have a personal reference for socialising with each other without the presence of this device.

Documenting young people's experience of using their cellphones was the focus of my previous research (Oosthuizen & Young, 2015). Central to the design of this particular study is a "social media detox" for which the participants agreed to restrict their social media/cellphone use. Through their experience of participating in the detox the respondents had the opportunity to critically reflect on the nature of their relationship with this device, which enabled them to become more aware of their agency in social situations. I propose that a young person's capacity to recognise and exercise their agency in social situations foreshadows whether that person will use the Internet in a way that is beneficial or problematic to their overall wellbeing. This view is shared by Boyd (2014, p. 83) who deems the "addiction rhetoric" as positioning cellphones "as devilish and teenagers as constitutionally incapable of having agency in response to the temptations that surround them".

The process of enabling young people to recognise their agency in social situations should consider how different personalities respond to on- and offline situations. Several studies argue that problematic Internet use is associated with personality type, such as introversion or extraversion (van der Aa et al., 2009; Kraut et al., 2002). However, these studies do not discuss the potential role of agency in supporting a young person's capacity – regardless of personality type – to utilise and develop the skills necessary to effectively self-regulate their on- and offline social behaviour. Here, the perspective that problematic Internet use is attributed to a particular personality type might have the unintended consequence of disempowering a young person's potential to exercise their agency if, for example, they regard themselves as introverted and therefore incapable of feeling competent in offline social situations.

Ultimately, the way in which young people use social media sites will determine whether its influence on their lives is likely to be positive or negative (Burke, Kraut, & Marlow, 2011; Shields & Kane, 2011). Rather than focusing on so-called addictive behaviour, or on the personality of the user, the social skills model of generalised problematic Internet use predicts that young people who perceive themselves as having low levels of social competency are vulnerable to developing a preference for online social interactions (Caplan, 2005; Casale et al., 2013). This argument highlights the potential for young people to learn skills to improve their level of social competency in order to manage the time they spend online and the types of interactions they engage in. If one considers that the amount of Internet consumed matters much less than the degree of self-control that users exercise over it, an alternative focus for research on the psychosocial effects of young peoples' cellphone use is, therefore, on the self, and the processes and mechanisms involved

in empowering the self (LaRose et al., 2014).

Selfhood in the age of cellphones

To better understand the impact that socialising on social media platforms has on young people's lives, it is important to examine factors, such as stronger self-concept (Kalpidou, Costin, & Morris, 2011). More research is needed to understand the complex dynamic of how young people's self-concept influences their relationship with their cellphones and how notions of self are perpetuated through the use of this device.

Human agency is inseparable from and enmeshed within self theory (Bandura, 1999, p. 21). The impact of most environmental influences on human motivation, affect, and action is heavily mediated through self processes (Bandura, 1993, p. 118). Ultimately, developing personal agency involves recognising and forging a relationship with self.

Self-concept is multi-dimensional, and hence various models exist for measuring the construct (Adamson & Lyxell, 1996; Benjamin, Rothweiler, & Critchfield, 2006; Ybrandt, 2008). In broad terms, self-concept is a person's perception of him/herself (Shavelson, Hubner, & Stanton, 1976). Because self-concept is created through interpersonal interactions (Benjamin, 1996), it is important to explore how social interactions taking place online inform the development of a young person's self-concept. Additionally, it is necessary to investigate whether this process of identity development online enables or disables the young person's ability to develop and exercise personal agency.

The interaction patterns of many young people have evolved beyond dichotomous online and offline social worlds into an integration of both (Ellison et al. 2011). However, the separation of these two contexts enables researchers to evaluate how the "online self" compares to the "offline self" and provides important information for understanding identity development in the digital age. There are varying perspectives on how cellphone and social media use might influence this process of developing a sense of self. Some researchers argue that socialising online – specifically via Facebook – facilitates the development of an *optimal self* (Gonzales & Hancock, 2011). Other researchers, however, argue that a *pre-corrected self* (Turkle, 2011) or *shallow self* (Suler, 2015) emerges as a result of socialising online.

Even though many young people might shift between socialising on- and offline without being aware that they switching between these two contexts, research suggests that the expression of self in each context is different. Unlike with socialising face-to-face, socialising online enables us to maintain control over how close we get to each other. Turkle (2012) refers to this phenomenon as 'the Goldilocks effect': these platforms allow us to keep people not too close, and not too far, but just right. Where the young user might consider this level of perceived control as advantageous in his/her social interactions, from a developmental

perspective Suler (2015) questions whether this way of relating to each other produces a *shallow self*. According to this author, communicating online “enables us to bypass conflict and sidestep true intimacy” (p. 91). This raises an important concern about whether or not socialising online provides young people with the opportunity to develop true intimacy through their interactions with their peers – and how this might, as a consequence, impact on their ability to relate to themselves as individuals.

Research on identity development in the digital age needs to consider the role of the cellphone as an object in young people’s lives – such as their attachment to the device itself. In addition, it is important to consider how socialising with this device facilitates online social behaviour and how these interactions also impact on a young person’s identity development. Webb and Widseth (2012) question whether the experience of engaging in constant online contact with their peers leads young people to lose their internal connection with themselves because they seldom experience solitude. Other researchers focus on the impact of the cellphone as an object. For example, Davis (2012) questions whether the constant presence of cellphones in young people’s lives interferes with their capacity to develop an autonomous sense of self. This author observes that young people will use their cellphone to deflect boredom and in doing so it discourages them from tapping into their inner resources as a means to dealing with it.

In summary, it seems plausible that socialising online more than offline might be fundamentally shifting the way in which young people come to know themselves, and might be shaping their identity development. The challenge is to find out what kind of self and relationships are created and perpetuated online (Belk, 2013).

The self and wellbeing

It is widely understood and accepted that wellbeing is an important indicator and contributing factor towards a young person’s psychosocial development. However, the impact of using cellphones on our wellbeing has not yet been clearly defined in the literature. It is crucial to approach this field of study from many different perspectives and disciplines in order to identify how to support young people to invest in their wellbeing in both on- and offline contexts.

This paper draws on Bandura’s theories about the importance of developing personal agency through social interactions. Furthermore, in order to exercise their personal agency, young people need to possess self-belief (Bandura, 1993). Many social scientists like Bandura preceded the Digital Age. With this in mind, it is important to consider how young people develop and exercise their personal agency in on- and offline social contexts. Self-belief is also a well-established predictor of future behaviours in health and education (Błachnio & Przepiorka, 2016; Strauss, Rodzilsky, Burack, & Colin, 2001). Thus, evaluating a young person’s level of self-

belief could be an important starting point for understanding their behaviour in online and offline contexts, and how these different contexts either undermine or support a young person's well-being.

In addition to self-belief, young people benefit from having a positive self-concept. A positive self-concept is a critical foundation for optimal mental health and positive development during adolescence. Individuals who acquire positive self-concept may demonstrate resilience in the face of a range of challenges (Olsson, Bond, Burns, Vella-Brodrick, & Sawyer, 2003; Sebastian, Burnett, & Blakemore, 2008). The importance of resilience is echoed by Burton (2015) who argues that we need to enable young people to develop resilience in order to successfully deal with online risks.

Many different factors contribute towards the overall wellbeing of an individual – such as self-belief, self-concept and self-worth. One of the dominant constructs that psychologists and researchers frequently use to measure wellbeing is self-esteem. According to Neff and McGehee (2010), psychologists and educators in the global north have mostly focused on enhancing self-esteem as a response to adolescents' negative self-evaluations. This outlook is evident in many cyberpsychology studies that evaluate how Internet or cellphone use impacts on self-esteem (e.g., Ehrenberg, Juckes, White, & Walsh, 2008; Gonzales, 2014; Gonzales & Hancock, 2011; Mehdizadeh, 2010; Steinfield, Ellison, & Lampe, 2008). Interestingly, these studies yield mixed results. For example, Gonzales (2014) reports that text-based communication is more beneficial for self-esteem than face-to-face communication or talking on a cellphone. In contrast, Mehdizadeh (2010) found that high Facebook activity is correlated with high scores in narcissism and low self-esteem scores. This paper proposes that it might be useful to evaluate a young person's social behaviour – both online and offline – using alternative wellness measures. This view is shared by other research that highlights the value of testing alternative means of measuring self-view (Crocker & Knight, 2005; Karanika & Hogg, 2016; Krieger, Hermann, Zimmermann, & grosse Holtforth, 2015; Marshall et al., 2015).

Moving away from focusing exclusively on self-esteem, Błachnio and Przepiorka (2016) claim that theirs is the first study examining the construct of positive orientation – having a positive perception of oneself, positive evaluation of one's life, and expecting positive things in the future – in the context of the Internet. In their study, positive orientation consists of three self-belief dimensions: self-esteem, optimism, and satisfaction with life. These authors found that the respondents who have a problem with excessive Internet use exhibited a low level of positive orientation – meaning that they have a low level of self-esteem, optimism, and satisfaction with life. This research highlights the importance of utilising multiple constructs to assess wellbeing in relation to Internet use.

More research is required in order to understand whether frequent cellphone use undermines or improves a young person's sense of self and in turn their wellbeing. In a study of 2,187 individuals, Neff and Vonk (2009) report that self-compassion

predicted more steady feelings of self-worth than self-esteem. In light of this, self-compassion might provide a useful avenue through which to understand the nature of the relationship that young people have with their cellphones and themselves.

What is self-compassion?

Three interacting components comprise self-compassion: self-kindness versus self-judgment, a sense of common humanity versus isolation, and mindfulness versus over-identification when confronting painful self-relevant thoughts and emotions (Neff & Germer, 2013). Self-compassion offers a secure and non-judgmental context to confront negative aspects of the self (Breines & Chen, 2012). Karanika and Hogg (2016) argue that self-compassion represents a healthy form of self-acceptance and plays an important role in how people cope with problems. In contrast, self-esteem refers to a way of relating to self in which “self-worth is conditional on (perceived) personal competence, performance, and attainment of desired states and ideals” (Karanika & Hogg, 2016, p.760).

The importance of self-acceptance is supported by an experimental study which revealed – rather paradoxically – that a self-accepting response to personal failure may actually motivate people to improve themselves (Breines & Chen, 2012). Emerging research highlights the potential for self-compassion to promote healthy behaviour (Sirois, 2015). Furthermore, self-compassion can be increased through relatively easy-to-administer exercises and training (Neff & Germer, 2013; Sirois, 2015).

Despite the positive benefits of self-compassion, its application in cyberpsychology research is novel. To my knowledge, only one published cyberpsychology study explores the role of self-compassion in determining outcomes of Internet use. In a study involving 261 university students, Iskender and Akin (2011) presented Internet addiction as an indicator of psychological maladjustment and self-compassion as an indicator of psychological adjustment. Results suggested that students high in self-judgment, isolation, and over-identification (i.e., those who were low in self-compassion) were more likely to be vulnerable to Internet addiction than those with high levels of self-kindness and mindfulness. The authors therefore concluded that enhancing self-compassion might be one way to diminish Internet addiction.

Conclusion

Ultimately, the process of switching between online and offline realms will quite likely be an evolutionary step forward in human identity development (Suler, 2015, p. 94). This perspective highlights the importance of finding out how to enable young people to develop the relevant competencies to achieve this evolutionary step forward.

This paper positions “self” as central to discussions about the way in which young people conduct their lives online. Because social media use has the potential to both

skill and deskill (Keegan, 2012), understanding the self-processes that inform online and cellphone user behaviour are crucial. From this perspective, research investigating the factors that determine how, and how much, and why young people engage in online behaviour should focus on understanding how to empower young users to use devices as tools that leverage, rather than undermine, their social development. Specifically, I argue that self-compassion is a potential avenue through which to explore identity development online. If a *healthy self* – as Suler (2015) refers to it – both incorporates and juggles online and offline living, then self-compassion might provide a potential avenue to explore to achieve this *healthy self*.

References

- van der Aa, N., Overbeek, G., Engels, R.C.M.E., Scholte, R.H.J., Meerkerk, G.-J. and Van den Eijnden, R.J.J.M. (2009), “Daily and Compulsive Internet Use and Well-Being in Adolescence: A Diathesis-Stress Model Based on Big Five Personality Traits”, *Journal of Youth and Adolescence*, Vol. 38 No. 6, pp. 765–776.
- Adamson, L. and Lyxell, B. (1996), “Self-concept and questions of life: identity development during late adolescence”, *Journal of Adolescence*, Vol. 19 No. 6, pp. 569–582.]
- Ahn, J. and Jung, Y. (2014), “The common sense of dependence on smartphone: A comparison between digital natives and digital immigrants”, *New Media & Society*, p. 1461444814554902.
- Baker, R.K. and White, K.M. (2010), “Predicting adolescents’ use of social networking sites from an extended theory of planned behaviour perspective”, *Computers in Human Behavior*, Vol. 26 No. 6, pp. 1591–1597.
- Bandura, A. (1990), “Perceived self-efficacy in the exercise of personal agency”, *Journal of Applied Sport Psychology*, Vol. 2 No. 2, pp. 128–163.
- Bandura, A. (1993), “Perceived Self-Efficacy in Cognitive Development and Functioning”, *Educational Psychologist*, Vol. 28 No. 2, pp. 117–148.
- Bandura, A. (1999), “A Sociocognitive Analysis of Substance Abuse: An Agentic Perspective”, *Psychological Science*, Vol. 10 No. 3, pp. 214–217.
- Bandura, A. (2006), “Toward a Psychology of Human Agency”, *Perspectives on Psychological Science*, Vol. 1 No. 2, pp. 164–180.
- Baym, N.K. (2015), *Personal Connections in the Digital Age*, John Wiley & Sons.
- Belk, R.W. (2013), “Extended Self in a Digital World”, *Journal of Consumer Research*, Vol. 40 No. 3, pp. 477–500.
- Benjamin, L.S. (1996), *Interpersonal Diagnosis and Treatment of Personality Disorders (2nd Ed.)*, Vol. xvi, Guilford Press, New York, NY, US.
- Benjamin, L.S., Rothweiler, J.C. and Critchfield, K.L. (2006), “The Use of Structural Analysis of Social Behavior (SASB) as an Assessment Tool”, *Annual Review of Clinical Psychology*,

Vol. 2 No. 1, pp. 83–109.

Berthon, P., DesAutels, P.A. and Butaney, G.T. (2010), “Created creates creator”, Orlando, Florida.

Bivin, J., Mathew, P., Thulasi, P. and Philip, J. (2013), “Nomophobia-Do we really need to worry about?”, *Reviews of Progress*, Vol. 1 No. 1.

Błachnio, A. and Przepiorka, A. (2016), “Personality and positive orientation in Internet and Facebook addiction. An empirical report from Poland”, *Computers in Human Behavior*, Vol. 59, pp. 230–236.

Breines, J.G. and Chen, S. (2012), “Self-Compassion Increases Self-Improvement Motivation”, *Personality and Social Psychology Bulletin*, Vol. 38 No. 9, pp. 1133–1143.

Burke, M., Kraut, R. and Marlow, C. (2011), “Social capital on facebook: differentiating uses and users”, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, New York, NY, USA, pp. 571–580.

Burton, P. (2015). "Risky Business? Emerging Policy and Young People's Agency in Online Safety: From Risk to Harm in the South African Context". In S. Cortesi & U. Gasser (Eds.), *Digitally connected: Global perspectives on youth and digital media* (pp. 97-99). Retrieved from <http://ssrn.com/abstract=2585686>

Byun, S., Ruffini, C., Mills, J.E., Douglas, A.C., Niang, M., Stepchenkova, S., Lee, S.K., et al. (2009), “Internet Addiction: Metasynthesis of 1996–2006 Quantitative Research”, *CyberPsychology & Behavior*, Vol. 12 No. 2, pp. 203–207.

Caplan, S.E. (2003), “Preference for Online Social Interaction A Theory of Problematic Internet Use and Psychosocial Well-Being”, *Communication Research*, Vol. 30 No. 6, pp. 625–648.

Caplan, S.E. (2005), “A Social Skill Account of Problematic Internet Use”, *Journal of Communication*, Vol. 55 No. 4, pp. 721–736.

Carbonell, X., Oberst, U. and Beranuy, M. (2013), “Chapter 91 - The Cell Phone in the Twenty-First Century: A Risk for Addiction or a Necessary Tool? A2 - Miller, Peter M.”, *Principles of Addiction*, Academic Press, San Diego, pp. 901–909.

Carter, M. (2015), “Me, My Self, and I(t): Conceptualizing Information Technology Identity and Its Implications”, *MIS Quarterly*, Vol. 39 No. 4, pp. 931–957.

Casale, S., Tella, L. and Fioravanti, G. (2013), “Preference for online social interactions among young people: Direct and indirect effects of emotional intelligence”, *Personality and Individual Differences*, Vol. 54 No. 4, pp. 524–529.

Crocker, J. and Knight, K.M. (2005), “Contingencies of Self-Worth”, *Current Directions in Psychological Science*, Vol. 14 No. 4, pp. 200–203.

Dahl, R.E. (2004), “Adolescent Brain Development: A Period of Vulnerabilities and Opportunities. Keynote Address”, *Annals of the New York Academy of Sciences*, Vol. 1021 No. 1, pp. 1–22.

- Davis, K. (2012), "Friendship 2.0: Adolescents' experiences of belonging and self-disclosure online", *Journal of Adolescence*, Vol. 35 No. 6, pp. 1527–1536.
- Deneulin, S. and Shahani, L. (2009), *An Introduction to the Human Development and Capability Approach: Freedom and Agency*, Earthscan.
- Ehrenberg, A., Juckes, S., White, K.M. and Walsh, S.P. (2008), "Personality and Self-Esteem as Predictors of Young People's Technology Use", *CyberPsychology & Behavior*, Vol. 11 No. 6, pp. 739–741.
- Ellison, N.B., Steinfield, C. and Lampe, C. (2011), "Connection Strategies: Social Capital Implications of Facebook-Enabled Communication Practices", *New Media & Society*, Vol. 13 No. 6, pp. 873–892.
- Erikson, E.H. (1968), *Identity: Youth and Crisis*, W. W. Norton.
- Facebook. (2016), *State of Connectivity 2015: A Report on Global Internet Access*, Annual, available at: <https://fbnewsroomus.files.wordpress.com/2016/02/state-of-connectivity-2015-2016-02-21-final.pdf>
- Gonzales, A.L. (2014), "Text-based communication influences self-esteem more than face-to-face or cellphone communication", *Computers in Human Behavior*, Vol. 39, pp. 197–203.
- Gonzales, A.L. and Hancock, J.T. (2011), "Mirror, Mirror on my Facebook Wall: Effects of Exposure to Facebook on Self-Esteem", *Cyberpsychology, Behavior, and Social Networking*, Vol. 14 No. 1-2, pp. 79–83.
- Henig, R.M. (2008), "Taking Play Seriously", *The New York Times*, 17 February, available at: <http://www.nytimes.com/2008/02/17/magazine/17play.html> (accessed 8 June 2012).
- Huang, H. and Leung, L. (2009), "Instant Messaging Addiction among Teenagers in China: Shyness, Alienation, and Academic Performance Decrement", *CyberPsychology & Behavior*, Vol. 12 No. 6, pp. 675–679.
- Iskender, M. and Akin, A. (2011), "Self-Compassion and Internet Addiction", *Turkish Online Journal of Educational Technology - TOJET*, Vol. 10 No. 3, pp. 215–221.
- Kalpidou, M., Costin, D. and Morris, J. (2011), "The Relationship Between Facebook and the Well-Being of Undergraduate College Students", *Cyberpsychology, Behavior, and Social Networking*, Vol. 14 No. 4, pp. 183–189.
- Karanika, K. and Hogg, M.K. (2016), "Being kind to ourselves: Self-compassion, coping, and consumption", *Journal of Business Research*, Vol. 69 No. 2, pp. 760–769.
- Keegan, S. (2012), "Digital technologies are re-shaping our brains: What are the implications for society and the research industry?", *Qualitative Market Research: An International Journal*, Vol. 15 No. 3, pp. 328–346.
- King, A.L.S., Valença, A.M., Silva, A.C.O., Baczynski, T., Carvalho, M.R. and Nardi, A.E. (2013), "Nomophobia: Dependency on virtual environments or social phobia?", *Computers in Human Behavior*, Vol. 29 No. 1, pp. 140–144.

- Kotlyar, I. and Ariely, D. (2013), "The effect of nonverbal cues on relationship formation", *Computers in Human Behavior*, Vol. 29 No. 3, pp. 544–551.
- Kraut, R., Kiesler, S., Boneva, B., Cummings, J., Helgeson, V. and Crawford, A. (2002), "Internet Paradox Revisited", *Journal of Social Issues*, Vol. 58 No. 1, pp. 49–74.
- Krieger, T., Hermann, H., Zimmermann, J. and grosse Holtforth, M. (2015), "Associations of self-compassion and global self-esteem with positive and negative affect and stress reactivity in daily life: Findings from a smart phone study", *Personality and Individual Differences*, Vol. 87, pp. 288–292.
- LaRose, R., Connolly, R., Lee, H., Li, K. and Hales, K.D. (2014), "Connection Overload? A Cross Cultural Study of the Consequences of Social Media Connection", *Information Systems Management*, Vol. 31 No. 1, pp. 59–73.
- Marshall, S.L., Parker, P.D., Ciarrochi, J., Sahdra, B., Jackson, C.J. and Heaven, P.C.L. (2015), "Reprint of 'Self-compassion protects against the negative effects of low self-esteem: A longitudinal study in a large adolescent sample'", *Personality and Individual Differences*, Vol. 81, pp. 201–206.
- Mehdizadeh, S. (2010), "Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook", *Cyberpsychology, Behavior, and Social Networking*, Vol. 13 No. 4, pp. 357–364.
- Neff, K.D. and Germer, C.K. (2013), "A Pilot Study and Randomized Controlled Trial of the Mindful Self-Compassion Program", *Journal of Clinical Psychology*, Vol. 69 No. 1, pp. 28–44.
- Neff, K.D. and McGehee, P. (2010), "Self-compassion and Psychological Resilience Among Adolescents and Young Adults", *Self and Identity*, Vol. 9 No. 3, pp. 225–240.
- Neff, K.D. and Vonk, R. (2009), "Self-Compassion Versus Global Self-Esteem: Two Different Ways of Relating to Oneself", *Journal of Personality*, Vol. 77 No. 1, pp. 23–50.
- Olsson, C.A., Bond, L., Burns, J.M., Vella-Brodrick, D.A. and Sawyer, S.M. (2003), "Adolescent resilience: a concept analysis", *Journal of Adolescence*, Vol. 26 No. 1, pp. 1–11.
- Oosthuizen, J. and Young, C. (2015), "How students' relationships with their cellphones inform their experience of socialising online and offline", presented at the African Cyber Citizenship Conference 2015, Nelson Mandela Metropolitan University, Port Elizabeth, available at: <http://accconference.nmmu.ac.za>.
- Pierce, T. (2009), "Social anxiety and technology: Face-to-face communication versus technological communication among teens", *Computers in Human Behavior*, Vol. 25 No. 6, pp. 1367–1372.
- Porter, G., Hampshire, K., Milner, J., Munthali, A., Robson, E., de Lannoy, A., Bango, A., et al. (2016), "Mobile Phones and Education in Sub-Saharan Africa: From Youth Practice to Public Policy", *Journal of International Development*, Vol. 28 No. 1, pp. 22–39.
- Prensky, M. (2001), "Digital Natives, Digital Immigrants Part 1", *On the Horizon*, Vol. 9 No. 5, pp. 1–6.

PricewaterhouseCoopers. (2015), *Entertainment and Media Outlook: 2015–2019 (South Africa–Nigeria–Kenya)*, Annual, available at: www.pwc.co.za/en/assets/pdf/entertainment-and-media-outlook-2015-2019.pdf.

Rosen, L.D., Cheever, N.A. and Carrier, L.M. (2012), *iDisorder: Understanding Our Obsession with Technology and Overcoming Its Hold on Us*, Palgrave Macmillan, New York.

Sebastian, C., Burnett, S. and Blakemore, S.-J. (2008), “Development of the self-concept during adolescence”, *Trends in Cognitive Sciences*, Vol. 12 No. 11, pp. 441–446.

Shavelson, R.J., Hubner, J.J. and Stanton, G.C. (1976), “Self-Concept: Validation of Construct Interpretations”, *Review of Educational Research*, Vol. 46 No. 3, pp. 407–441.

Sirois, F.M. (2015), “A self-regulation resource model of self-compassion and health behavior intentions in emerging adults”, *Preventive Medicine Reports*, Vol. 2, pp. 218–222.

Steinfeld, C., Ellison, N. and Lampe, C. (2008), “Social capital, self-esteem, and use of online social network sites: A longitudinal analysis”, *Journal of Applied Developmental Psychology*, Vol. 29 No. 6, pp. 434–445.

Strauss, R.S., Rodzilsky, D., Burack, G. and Colin, M. (2001), “Psychosocial Correlates of Physical Activity in Healthy Children”, *Archives of Pediatrics & Adolescent Medicine*, Vol. 155 No. 8, pp. 897–902.

Subrahmanyam, K. and Smahel, D. (2010), *Digital Youth: The Role of Media in Development*, Springer.

Suler, J.R. (2015), *Psychology of the Digital Age: Humans Become Electric*, Cambridge University Press.

Swanepoel, T.L. and Thomas, K.G. (2012), “Malicious MXit? South African adolescents’ use of mobile-based communication applications”, *Journal of Child & Adolescent Mental Health*, Vol. 24 No. 2, pp. 117–132.

Turkle, S. (2011), *Alone Together: Why We Expect More from Technology and Less from Each Other (Large Print 16pt)*, Basic Books, New York, NY, USA.

Turkle, S. (2012), “The flight from conversation”, *The New York Times* (accessed 26 March 2016).

Uhls, Y.T., Michikyan, M., Morris, J., Garcia, D., Small, G.W., Zgourou, E. and Greenfield, P.M. (2014), “Five days at outdoor education camp without screens improves preteen skills with nonverbal emotion cues”, *Computers in Human Behavior*, Vol. 39, pp. 387–392.

Walsh, S.P., White, K.M., Cox, S. and Young, R.M. (2011), “Keeping in constant touch: The predictors of young Australians’ mobile phone involvement”, *Computers in Human Behavior*, Vol. 27 No. 1, pp. 333–342.

Webb, R.E. and Widseth, J.C. (2012), “The Erosion of Aloneness”, *Journal of College Student Psychotherapy*, Vol. 26 No. 3, pp. 165–167.

Ybrandt, H. (2008), "The relation between self-concept and social functioning in adolescence", *Journal of Adolescence*, Vol. 31 No. 1, pp. 1–16.

Young, K. (2009), "Internet Addiction: Diagnosis and Treatment Considerations", *Journal of Contemporary Psychotherapy*, Vol. 39 No. 4, pp. 241–246.

Students' Perceptions & Experiences of Flaming on Social Networking Sites: An Exploratory Study

Pearl Maseko & Willie Chinyamurindi

University of Fort Hare, Alice, South Africa

email: wchinyamurindi@ufh.ac.za

Abstract

In this exploratory study, we investigate how students perceive and experience the notion of flaming when using social networking sites such as Facebook. Flaming is defined as the display of any hostile behaviour to cover insults, swearing or the use of offensive language. We used a focus group technique with 20 randomly selected students incorporating interviews to understand the perception and experience of flaming on social networking sites. Thematic analysis was used as a technique to analyse the transcribed interview data. Three main findings emerged. First, flaming was found to be a multi-faceted construct to the lived experiences of students, online and offline. Second, flaming appears to be prevalent due to the online realm allowing for anonymity and lack of policing. Finally, victims of flaming narrated a sense of helplessness due to their perpetrators being around their physical community spaces, and this has subsequently affected their online behaviour. Conclusions were made based on the findings of this study to inform not only etiquette around online behaviour but also implications for those who work within a campus setting.

Keywords: Flaming, Perceptions, Experiences, Social Networking Sites, Students

1. Introduction

The concept of online flaming is one that is gaining currency, empirically, as is the behaviour. The growing interest can be alluded to the popularity and ease of access individuals have of platforms of expression around them (Li, Yang, Song & Lu, 2012) especially Social Networking Sites (SNS) (Sahlin, 2015). Within the student population, it can be expected that flaming could be a popular concept given that young people in this population value interaction, especially online (Skiba, 2014) and can belong to a number of online communities (Chen & Katz, 2009).

Researchers have made calls for studies that give further focus into understanding flaming in various contexts (e.g. Moor, Heuvelman & Verleur, 2010; Wu, Lirn & Dong, 2014). Flaming is defined as consisting of abusive comments that can be made (Kim & Raja, 1991) and believed to be evident, especially online (Arendholz, 2013). Others (e.g. Hardaker, 2013) view flaming to be linked to behaviours such as hating (harsh commentary) and trolling (deliberately angering others) - all of these with the ultimate aim of being provocative (Yee, 2006). A bold claim is made that behaviours such as flaming are just part of community behaviour where conflict and such practices are seen to be unavoidable (Pagliai, 2010).

However, not all authors seem to view flaming as dysfunctional. Lunt and Stenner (2005) argue for behaviours such as flaming as giving society an opportunity to see and understand those issues which may be covert. This can be a useful platform for generating “discussion” and enforcement, especially around “online communicative rights and privileges” (Lange, 2014: 53). This is an irony because on one side is a view that behaviours such as flaming can cause a great deal of emotional trauma for the individual and close friends (Garcés-Conejos Blitvich, 2010). Conversely, while there is such trauma, behaviours such as flaming allow for an opportunity to understand human behaviour better and generating public discourse (Buckingham, 2009).

This paper seeks to extend the knowledge around the issue of flaming through studying experiences and perceptions of this behaviour. The paper has two main aims. First, given popularity in the usage of SNS platforms, especially amongst the student population, research is needed into the experiences and perceptions with regard to flaming on such platforms (Moor et al., 2010). Second, we note with interest few studies in South Africa paying attention specifically to the concept of flaming amongst the student cohort. Empirical attention has been given towards understanding issues such as mobile phone usage amongst students (Shava, Chinyamurindi & Somdyala, 2016) and the acceptance of technology for teaching instruction (Chinyamurindi & Shava, 2015). We seek to advance an understanding of the concept of flaming, especially within the student population group. The findings of the study have important implications for educators, communication researchers, technology experts and counsellors involved in working with the student market, their communication patterns and online behaviours.

The rest of the paper is organised in the following manner: first we give a brief discussion of the literature, and this flows into the research aims and questions of this study. Thereafter, the research methodology, results, discussion and implication of the study, as well as limitations, are discussed. The last sections focus on areas for future research and the study’s conclusion.

2. Literature Review

2.1. Theoretical literature

As a theoretical lens, the Uses and Gratification Theory (UGT) (Lin, 1998) is a useful theory to explain psychological and behavioural tendencies in computer mediated communication (Nazareth, 2011). There are three underlying assumptions here (Katz, Blumler & Gurevitch, 1974). First, the audience must be considered to be active media users. Second, this audience is goal-directed in their behaviour and finally, an awareness of individual needs in media usage, including the gratification thereof, must exist. Thus, at play, when flaming occurs and espoused in the UGT is the personality (Alonzo & Aiken, 2004) and how the experience of using an online platform relates to the gratification of needs and the responses that may emerge from this (Nazareth, 2011). In essence, using the flaming motives model of Alonzo and Aiken (2004) that borrow tenets from the UGT, four flaming categories exist and linked to this: a) passing time; b) escape; c) relaxation; d) entertainment and finally, e) status-enhancement.

Further, lack of direct individual contact is attributed to causing flaming to be widespread (Alonzo & Aiken, 2004). This has led to the de-individuation theory in which individuals or members of a group do not see other individuals as individuals (Kayany, 1998) and making it easy to vent out at others without sympathy or consideration (Aiken & Waller, 2000). In essence, there is acknowledgement by Moor et al. (2010) that more research is needed on flaming, especially on SNS to even test the veracity of such theories covered in this section.

2.2 Empirical literature

Research has been conducted and found flaming to be prevalent in a number of online platforms such as email (Turnage, 1997); electronic classrooms (Aiken & Waller, 2000) and video sharing platforms such as Youtube (Moor et al., 2010). Flaming is manifested through the use of text (O' Sullivan & Flanagan, 2003), making it one of the most recognised phenomena within computer mediated communication (Moor et al., 2010). In relation to this, researchers have found a number of behaviour experiences that characterise the phenomena of flaming. Common to this are aspects of hostility and harsh opinion over others online (Kayany, 1998) with the purpose to offend (Aiken & Waller, 2000). Moor et al. (2010) add that often, flaming experiences entail the use of insults and offensive language.

The experiences of users online with regard to flaming can be mixed. Research conducted has found that in some cases, what is deemed offensive to one individual can be considered entertaining by another one (Kushin & Kitchener, 2009). Further, lack of physical contact amongst users can make flaming to be more prominent, especially given that the channel of communication is virtual (Moor et al., 2010). Others (Lapidot-Leffler & Barak, 2012) argue that flaming becomes prevalent because of anonymity. Individuals can create false profiles and be able to vent out at others given this aspect of anonymity and a sense of a lack of accountability (Kushin & Kitchener, 2009). Based on the coverage of the theoretical and empirical literature, the research sought to investigate the perceptions and experiences of students towards flaming, especially on SNS. This is done with the intent of being exploratory to better understand a concept cited in literature to require more investigation in various contexts. Thus, the specific research questions are: *what are the perceptions and experiences of students on SNS?*

3. Method

A qualitative research approach using the exploratory research design was adopted for this study based on two main arguments from literature. First, this approach and research design are argued, within literature, as useful, especially when seeking an “understanding” of issues that affect humans such as “perceptions, attitudes and experiences” (Sheard, 2011, p. 623). Second, lived experiences, including the complexity that accompany them can be better understood through the qualitative paradigm an argument made especially in countries such as South Africa with apparent inequality (Chinyamurindi, 2016a, b, c). This can be a useful pre-cursor not only to interventions that help individuals but also a contribution towards emerging sense-making around an issue (Chinyamurindi, 2012). This then becomes a platform to generate meaning and understanding (Sparkes & Smith, 2012). The research technique adopted in this study was the focus group technique, used in previous studies within the information systems discipline in understanding phenomena (Chetty & Mearns, 2012). This was also done using interviews within a large group setting and breaking the group into two smaller groups seeking to understand how individuals make sense of phenomena around them (Silverman, 2013).

3.1 Participants

A total of 20 student participants took part in the study. The sample consisted of an even split between males and females. Participants were aged between 22 and 29 years, with an average age of 25 years. The study was conducted at

a rural university in the Eastern Cape Province of South Africa. Given that the university is a historically black university, all the participants were Black Africans. A convenience sampling approach relying on those participants who were most ‘accessible and available’ (Cohen, Manion, & Morrison, 2007, p. 114) was used. An invite was made to a Media and Communication class for students who were interested to avail themselves for the study. Participants had to be registered students with the University of South Africa. The focus group discussions, including interviews, were conducted at the university, and potential participants were first informed of the study, including their rights. Upon agreeing to be part of the study, participants had to sign an informed consent form. Ethical clearance was applied for and granted to the university research ethics committee where the students were based.

3.2 Procedure

A focus group session that ran for a period of an hour and a half was conducted and split into four sessions. The first session was meant to be an introduction with ice-breaker exercises meant to put participants at ease. The second session was meant to gauge participants’ understanding of the concept of flaming through a group discussion with all the 20 participants, prompted by the question: “have you ever heard of the term *flaming*, if so, what do you understand by this term?” Further, participants were asked to be free and open in their expression for as long as this was done in a manner that respected other individuals and for the purpose of order. The third session entailed splitting participants into two groups where discussions within these sub-groups were on relating with actual experiences and perceptions around flaming. To prompt discussions, participants were shown screen shots of online occurrences of flaming and asked to relate with this. A scribe was nominated to write the experiences and perceptions of participants with the view of presenting to the larger group in the fourth session. The final session was split into two, a report back session (with discussion allowed) and a concluding session where participants based on the third session suggested solutions to the issues raised in the breakaway groups. Sub-group discussions were all recorded, and the entire focus group discussion was video-taped with permission from participants. All the interviews were then transcribed verbatim, including the notes made by the researchers.

3.3 Strategies to ensure data integrity

To ensure data quality, three steps were taken. First, the researchers pre-tested the questions used in the discussion components of the four sessions with a sample of 10 non-participating students. Second, a process of content and face validity was conducted on the questions asked in the study by consulting a) an industrial psychologist; b) technology educationist and finally, c) a qualitative research expert. Third, to ensure credible data, all the discussions were recorded through audio and video means with the purpose of transcription within twenty-four hours.

4. Data analysis

The transcribed interviews were exported into QSR International's NVivo 9, a data analysis and management software package for the purpose of data analysis useful when dealing with a lot of text, graphic, audio, and video data (Bazeley & Jackson, 2013; Reuben & Bobat, 2014). Chinyamurindi (2016c) makes the argument that software such as NVivo only serves the purpose of organising data. There is need for further researcher on some form of analysis based on this organised data. Thematic analysis, which is a commonly used method of analysis in qualitative research, was used to reduce texts to codes that represented themes or concepts in order to capture the complex meanings within a textual data set (Guest, MacQueen & Namey, 2012). Further, thematic analysis offered a means of not only analysing but also organising large volumes of data into themes (Rohleder & Lyons, 2014). This can be a basis for developing conclusions from the data analysis (Sotiriadou, Brouwers & Le, 2014). As consistent with working with qualitative research, especially using thematic analysis, themes and quotes based on consistencies across participant views were used (Rhodes, 2000).

5. Results

In reporting the findings around the perceptions and experiences of flaming amongst students, three questions based on structural analysis (Labov, 1972) guided the questions we sought to investigate. Notably: a) *how does flaming begin*; b) *what is involved* and c) *what happens next*?

5.1 How does flaming begin?

Participants narrated flaming to be prevalent around them. However, two interesting issues emerged here as to how flaming begins. First, flaming was expressed by participants to be a multi-faceted construct. This meant that in the various spheres of influence and experiences characterising the lived experience of students flaming appears to be prevalent. Second, the online platform appears to be a nuanced extension of battles happening in these spheres. Consequently, students narrated the boldness that the online platform created (allowing for flaming to occur) to issues happening in the non-virtual realm. For instance, one female participant narrated how flaming manifests due to campus political organisations:

“It happens also even on our university Facebook page where you see, especially student political groupings attacking each other so much and being harsh based on the diversity of opinions. I think it even starts before people are online.” Angie (Pseudonym)

Another male participant seems to support the views of Angie and revealed how flaming is not only a multifaceted construct but also a mere continuation of attacks that happen within the university community such as the residences. The virtual platform is an extension of these battles from outside:

“The fight actually begins before people go online. The only difference being that when it goes online, it gets intense. For instance, I have seen people threatened with death. Brian (Pseudonym)

A female participant who took part in the study framed flaming as having linkages to her aesthetic persona and how she was attacked online for wearing a weave. Once again, it appears that some of the issues of her being flamed online appear due to issues happening outside the online platform of expression:

“I love my weaves and get the sense that some people may not like weaves judging by comments I get walking on campus. So I once posted a picture on Facebook, I was wearing a weave, some people started even attacking me accusing me of having a blesser who is paying for the weave. The thinking is that as a student, I can’t afford to wear Brazilian hair. Earlier on campus someone had told me I am un-African. So the attack just

continued from my campus walk to my Facebook page.”
Musa (Pseudonym)

5.2 What is involved?

As researchers, we also sought to understand what is involved within the context where flaming occurs as part of a lived experience amongst students. Students narrated two main issues involved here. First, there was the boldness of being anonymous. One female participant narrated this succinctly:

“Flaming is fuelled by anonymity, and this creates some form of boldness. You can create a fake account and just spew all the attacks you can. You know why? Because no one knows you. Sivuyile (Pseudonym)

This issue of being anonymous was a telling confession by a student who admitted being part of the flaming culture. In this confession, the male student admitted that for as long as he remained anonymous, he would continue the habit:

“Look, there must be someone that is honest to tell it like it is. Call it flaming, but I call it the bitter truth that society does not want to hear. I guess until a time we are ready to hear this, I continue what I do anonymously. Steve (Pseudonym)

Second, an issue at play with flaming appears to be the lack of policing, especially on social networking sites. This lack of policing makes the practice to be prevalent and can be linked to the first sub-theme presented previously of anonymity. For instance, one female participant also narrated an attack that happened to her online:

“For us as women, the attacks are on our persona. For instance, you get attacks on issues around wearing mini-skirts, the makeup you put on, the size of your body....I actually think I am better than my outside and really people need to get to know the inner me. The absence of someone to protect us online makes us suffer while our perpetrators prosper.” Mary (Pseudonym)

Another participant berated those involved in flaming stating that the absence of punishment accompanying the behaviour makes it continue:

“On campus, if you are caught stealing you can be punished. If you fight, you will be punished. However, there is no traceable case I know of anyone that has been punished for attacking others online. Surely the lack of such punishment and monitoring makes people continue the bad behaviour. Don (Pseudonym)

5.3 What happens next?

A final perception and experience of students was the resultant effect of what happens after the incident of flaming. Participants narrated a sense of helplessness, and it appears to be business as usual. Given this state of helplessness, some participants narrated a sense of detachment from using social networking sites in fear of being flamed. This was espoused by one participant:

“I am scared of posting pictures because of the potential abuse I can suffer.” Faith (Pseudonym)

Some participants went to describe the psychological trauma that accompanies being a victim of flaming. Due to this trauma, participants narrated how this limited their usage of social networking sites:

“It’s also a psychological thing, I put you down so I can benefit from your misery as this will make me feel better. Sadly, I don’t feel better at all and have limited use of platforms such as Facebook fearing attacks” Xola (Pseudonym)

Finally, other participants narrated the trauma, at times, of seeing those people involved in flaming around the campus.

“Everyone knows who flames online, they live with us and walk amongst us. At times, we avoid these people in our community spaces and it’s just not a nice feeling.” Vuyo (Pseudonym)

“I see him around campus, the guy who wrote nasty things about me. Just seeing him makes me angry and yet powerless.” Zandi (Pseudonym)

6. Discussion

The findings of this work, through identified themes, confirm the existence of flaming found in previous work (Sahlin, 2015). Our work shows how this happens, especially within a campus setting, confirming also how this behaviour affects interaction and usage of online platforms (Chen & Katz, 2009; Skiba, 2014). Notably, our work illustrates the linkage between what happens in the community spaces students belong to and how these issues transfer towards the online platform. In this regard, we note with interest how flaming could be an extension of wider endemic issues happening outside online platforms. It would appear that the online platform serves an easy playground for attacks to happen due to lack of policing wherein individuals can remain anonymous. Thus, our work further highlights how not only flaming exists but also the complexity impeding advancing from previous studies (Lapidot-Lefler & Barak, 2009; Kushin & Kitchener, 2009; Moor et al., 2010).

Further, our work gives cadence to the UGT. The UGT, as illustrated in this study, has relevance in that it explicates more on the communication behaviours that happen, especially on social media platforms such as Facebook. In a rather negative way, the study illustrates the needs and motivations (Katz et al., 1974) including communication behaviours, especially on online platforms such as social networking sites. It would appear that those who are involved in the habit of flaming exhibit an information role in pursuit of gratifications and a possible explanation why they are engaged in the practice. It would also appear that the application of the UGT is given cadence as in previous studies (e.g. Alonzo & Aiken, 2004) to the perceived anonymity of being online; hence encouraging dis-inhibition which results in behaviours such as flaming.

7. Contribution

This work makes a contribution in three ways. First, this work advances literature calling for more studies on behaviours such as flaming in various contexts (Morr et al., 2010; Wu et al., 2014). In our case, we not only posit flaming to be abusive (Kim & Raja, 1991) but also to be multifaceted in how it is framed within a campus setting. Second, as advised by Buckingham (2009), we hope that our work creates a platform where public discourse can be generated around behaviours such as flaming. To us, the perceptions and experiences of flaming espoused in this paper are not only useful in understanding flaming but also in creating some psycho-social support for victims and help for rehabilitation for perpetrators. Finally, we push

towards the necessity for more campus monitoring, especially concerning online usage. There is a need to be able to identify and offer support to at-risk students on campus who may have been or are targets of flaming. Such support can only happen when some form of monitoring and report mechanisms are available on campus. Second, through monitoring, individuals who practise flaming can be reported anonymously and necessary investigations conducted. These are all views suggested by Lange (2014). However, as found and illustrated in this paper, there is need for a collaborative effort between monitoring online and offline behaviours as they have linkages.

8. Limitation and Future Research

A limitation exists with the current research. The results of this research are not generalisable to the entire population of students in South African universities. Caution should be exercised when interpreting and making implications based on this. Further, the study relied on a small sample size for the purpose of understanding further the concept of flaming. This is also a notable limitation of this work. Despite the limitation that exists within the current research, future research can be suggested to improve on such. Furthermore, a quantitative study would aid in understanding underlying motivations and behaviours around flaming amongst students. This could aid in testing relationships between constructs. Further, future research could unpack further, the negotiation that happens amongst students between tensions in their offline and online spaces with regards to dealing with perpetrators in both spaces. Finally, as part of phase 2 of the project, we wish to utilise the same sample of students to propose a framework and policy guidelines around etiquette and policy on online policing.

9. Conclusion

The compelling theme that emerged from this study which is *flaming* is much alive within the campus setting. It would appear that flaming as an online behaviour is not receiving much focus with limited interventions as compared to more physical abuse incidents prevalent on campus. The study argues for more attention to be given to flaming to assist both victims and perpetrators. This becomes a priority in making safe student usage of social networking sites while respecting other users.

10. References

- Aiken, M., and Waller, B. (2000), Flaming among first-time group support system users. *Information & Management*, Volume 37, 95-100.
- Alonzo, M., and Aiken, M. (2004), Flaming in electronic communication. *Decision Support Systems*, Volume 36, Number 3, 205–213.
- Arendholz, J. (2013), *(In) Appropriate Online Behavior: A pragmatic Analysis of Message Board Relations*. Amsterdam: John Benjamins.
- Bazeley, B.V., and Jackson, K. (2013), *Qualitative Data Analysis with NVivo*. London: Sage Publications.
- Buckingham, D. (2009), *Speaking back? In search of the citizen journalist*. In: Buckingham, D., Willett, R. (Eds.), *Video Cultures: Media, Technology and Everyday Creativity*. Palgrave Macmillan, London, pp. 93–114.
- Chetty, L. and Mearns, M., (2012), “Using communities of practice towards the next level of knowledge management maturity”, *South African Journal of Information Management*, Volume 14, Number 1, 1-9.
- Chinyamurindi, W.T. (2016a), “A narrative investigation into the meaning and experience of career success: Perspectives from women participants”, *South African Journal of Human Resource Management*, Volume 14, Number 1, 1-11.
- Chinyamurindi, W.T. (2016b), “Using narrative analysis to understand factors influencing career choice in a sample of distance learning students in South Africa”, *South African Journal of Psychology*, 1-11.
- Chinyamurindi, W.T. (2016c), “Middle manager role & contribution towards the competitive intelligence process: A case of Irish subsidiaries”, *South African Journal of Information Management*, 18(2), 1-7.
- Chinyamurindi, W.T. (2012), “An investigation of career change using a narrative and story-telling inquiry”, *South African Journal of Human Resource Management*, Volume 10, Number 2, 1–11.
- Chinyamurindi, W. and Shava, H., (2015), “An investigation into e-learning acceptance and gender amongst final year students”, *South African Journal of Information Management*, Volume 17, Number 1, 1-9.
- Chen, Y.F. and Katz, J.E., (2009), “Extending family to school life: College students’ use of the mobile phone”, *International Journal of Human-Computer Studies*, Volume 67, Number 2, 179-191.
- Cohen, L., Manion, L., and Morrison, K. (2007), *Research methods in education* (6th ed.). London, England: Routledge-Falmer.
- Garcés-Conejos, P. and Blitvich, P. (2010), A genre approach to the study of impoliteness. *International Review of Pragmatics*, Volume 2, 46-94.
- Hardaker, C. (2013), “Uh. . . not to be nitpicky,,,,,but. . .the past tense of drag is dragged, not drug: an overview of trolling strategies”, *Journal of Language Aggression and Conflict*, Volume 1, Number 1, 57-85.

- Katz, E., Blumler, J., & Gurevitch, M. (1974), *Utilization of mass communication by the individual*. In J. Blumler & E. Katz (Eds.), *The uses of mass communication: Current perspectives on gratifications research* (pp. 19–34). Beverly Hills, CA: Sage.
- Kayany, J. M. (1998), Contexts of uninhibited online behavior: *flaming in social newsgroups on Usenet*. *Journal of the American Society for Information Science*, Volume 49, Number 12, 1135–1141.
- Kushin, M., and Kitchener, K. (2009), “Getting political on social network sites: Exploring online political discourse on Facebook”, *First Monday*, Volume 14, Number 11, 1–16.
- Labov, W. (1972), *Sociolinguistic patterns*. Philadelphia: University of Pennsylvania Press.
- Lange, P.G. (2014), Commenting on YouTube rants: Perceptions of inappropriateness or civic engagement? *Journal of Pragmatics*, Volume, 73, 53–65.
- Lapidot-Lefler, N. and Barak, A. (2012), “Effects of anonymity, invisibility and lack of eye-contact on toxic online disinhibition”, *Computers in Human Behavior*, Volume 28, Number 2, 434–443.
- Li, B., Yang, J., Song, X. and Lu, B. (2012), ‘Survey on disposal behaviour and awareness of mobile phones in Chinese university students’, *Procedia Environmental Sciences*, Volume, 16, 469–476.
- Lin, C.A. (1998), Exploring personal computer adoption dynamics. *Journal of Broadcasting & Electronic Media*, 42, 95–112.
- Lunt, P., and Stenner, P. (2005), “The Jerry Springer Show as an emotional public sphere”, *Media, Culture & Society*, Volume 27, 59–82.
- Moor, P.J., Heuvelman, A., and Verleur, R. (2010), “Flaming on YouTube”, *Computers in Human Behavior*, Volume 26, Number 6, 1536–1546.
- Nazareth, D.S. (2011), *Revising the Flaming model: Examining personality traits as predictors of flaming motives in online forums*. Retrieved from <http://essay.utwente.nl/61258/>.
- O’Sullivan, P., and Flanagan, A. (2003), Re-conceptualizing “flaming” and other problematic messages. *New Media & Society*, Volume 5, Number 1, 69–94.
- Pagliai, V. (2010), “Introduction: performing disputes”, *Journal of Linguistic Anthropology*, Volume 20, Number 1, 63–71
- Reuben, S., and Bobat, S. (2014), “Constructing racial hierarchies of skill-experiencing affirmative action in a South African organisation: A qualitative review”, *South African Journal of Industrial Psychology*, Volume 40, Number 1, 1–12.
- Rhodes, H. (2000), *Mid-life career change to home-based self-employment in a group of women* (Unpublished master’s thesis). Simon Fraser University, Burnaby, British Columbia, Canada.
- Rohleder, P., & Lyons, A. (Eds.) (2014), *Qualitative research in clinical and health psychology*. Basingstoke: Palgrave Macmillan.

Sahlin, J.P. (2015), *Social Media and the Transformation of Interaction in Society*. USA: Information Science Reference.

Shava, H., Chinyamurindi, W.T. and Somdyala, A. (2016), An investigation into the usage of mobile phones amongst a sample of TVET students in South Africa. *South African Journal of Information Management*, Accepted for Publication.

Sheard, L. (2011), Anything could have happened: Women, the night-time economy, alcohol and drink spiking. *Sociology*, Volume 49, 619–633.

Silverman, D. (2013), What counts as qualitative research? Some cautionary comments. *Qualitative Sociology Review*, Volume 9, Number 2, 48–55.

Skiba, D.J., (2014), “The connected age: Mobile apps and consumer engagement”, *Nursing Education Perspectives*, Volume 35, Number 3, 199–201.

Sotiriadou, P., Brouwers, J. and Le, T. (2014), Choosing a qualitative data analysis tool: A comparison of NVivo and Leximancer. *Annals of Leisure Research*, Volume 17, Number 2, 218-234.

Sparkes, A., and Smith, B. (2012), “Embodied research methodologies and seeking the senses in sport and physical culture: A fleshing out of problems and possibilities”, *Qualitative Research on Sport and Physical Culture Research in the Sociology of Sport*, Volume 6, 167–190.

Turnage, A.K. (2007), Email flaming behaviors and organizational conflict. *Journal of Computer-Mediated Communication*, Volume 13, Number 1, 43-59.

Guest, G., MacQueen, K.M., and Namey, E.E. (2012), *Applied thematic analysis*. Los Angeles: Sage Publications.

Wu, Y.C.J., Lirn, T.C., and Dong, T.P. (2014), “What can we learn from advertisements of logistics firms on YouTube? A cross cultural perspective”, *Computers in Human Behavior*, Volume 30, 542-549.

Yee, N. (2006), “The demographics, motivations, and derived experiences of users of massively-multiuser online graphical environments”, *Presence Tele-operators and Virtual Environments*, Volume 15, Number 3, 309-329.

Using personas to understand city residents' information needs and evaluate city information services

Judy Backhouse and Shado Masilela

University of the Witwatersrand, Johannesburg, South Africa
judy.backhouse@wits.ac.za

Abstract

In increasingly complex cities, residents have information needs relating to accommodation, utilities, healthcare, public safety, transport, training and employment. These information needs are met by different providers, including city governments. To be effective, such information services must be inclusive and provide for the specific needs of residents. So providers of information services need tools for understanding the information needs of diverse city dwellers and designing effective information services.

Personas are one such tool, used in software design. A persona is a hypothetical archetype, constructed through a rigorous process, based on empirical induction. Personas are used to assist software designers to envision users, as a communication tool, and to evaluate the design of software. This research investigates the process of using a grounded theory approach to construct personas representing different kinds of city residents and reflects on the potential for personas to lead to better designed city information services.

Interviews were conducted with purposely selected participants at two sites in Johannesburg and these were used to construct five personas with different information needs. These personas were then used to evaluate online municipal services provided by the City of Johannesburg and to make recommendations for improvements. The paper reflects on the process of constructing the personas, as well as the value of using personas to understand the information needs of city residents and evaluate the effectiveness of information services.

Keywords

Persona, Smart City, Information Need, Information Service, Grounded Theory

7. Introduction

Life in cities is complex as individuals negotiate securing shelter and services, finding work and other resources, and identifying and affiliating to appropriate groups for work, social and leisure activities. Residents have to navigate a wide range of different systems and to do this, they need information. The complexities of city life are reflected in the complex information needs of city dwellers (Cole, 2011). Understanding information needs, and how residents go about meeting them, makes it possible for the providers of information to design better services, with the ultimate goal of making it easier to live in the city.

The process of understanding information needs and the best ways to meet them has been the subject of information systems requirements gathering research and practice

for some time (Cheng and Atlee, 2007). This work originated in the design of information systems for organisations, where information needs could be defined in terms of the organisation's purpose and processes. However, as more widely used information systems have emerged, particularly those that are embedded in consumer products, new tools for understanding information needs have been developed. Among these is the use of personas as an analytical device (Aoyama, 2005, 2007; Pruitt and Grudin, 2003; Faily and Flechais, 2010, 2011).

As the task of providing for the information needs of city residents is in some ways similar to that of providing for a diverse set of customers, personas may be useful tools for designing information-based services for smart cities. This research investigates the use of personas in understanding the information needs of city residents and evaluating the services that provide for these needs.

8. The role of information in city living

City residents make use of a wide range of different types of information (Lee and Lee, 2014). This may be information relating to finding accommodation, about services such as water, electricity and refuse collection, about learning and employment opportunities, or about political issues that impact their lives in the city. It might also be information related to transportation, healthcare, or to leisure activities. A so-called smart city takes advantage of information technologies to provide such information in ways that are easy to access and immediately relevant to the individual (Hollands, 2008; Komninou, 2002, Lee and Lee, 2014). Such technologies also enable providers to collect information about residents and the uses they are making of the information provided in making choices about their lives in the city. The information collected as residents go about their daily lives can in turn be used to improve the services offered and to provide better information.

City information services are provided by the city itself, but also by consultants to the city, private companies, research groups, NGOs and individuals. Providing effective information services depends on having a good understanding of the information needs of the people that will use the services, but this is difficult in most cities because city residents are very diverse. Without a comprehensive understanding of the information needs of all residents, information services may be offered that address the needs of only a subset of people in the city.

9. Personas

A persona is defined as a "hypothetical archetype of an actual user" (Cooper, 1999). A persona includes descriptive information about an imagined individual such as a typical day in their life, their job description and work activities, their home and leisure activities, their goals, fears and aspirations, and preferred ways of communicating. Personas might also include information about the individual's attitude towards and ability to use technologies as well as information about the size and influence of the market segment that this persona represents (Pruitt and Grudin,

2003) or, in the provision of city information services, the extent of the population represented by each persona.

Personas do not exist in isolation. Designers of information services are interested in how personas behave in specific scenarios which support their individual end goals (Pruitt & Grudin, 2003). The scenario is the contextualised setting of the interaction between the person and the information source (such as a web site, a software application or a printed notice on a notice board) (Aoyama, 2005). For example, a resident who wishes to buy a house has a need for information about houses for sale and this results in the scenario of conducting an online search for houses to buy.

Using personas in the design of information systems has a number of benefits. Personas result in better designs because they help designers to envision an actual user of the system, thus preventing the design from being biased to the designers' conveniences, purposes and preferences (Aoyama, 2007; Pruitt and Grudin, 2003, Faily and Flechais, 2011). Personas serve as a communication tool, within the team designing and developing an information system, and between the team and the commissioning client. They have been known to generate empathy, among designers and developers, towards users (Faily and Flechais, 2010). Personas can also be used to guide the design of marketing materials for informing different potential users about the system (Pruitt and Grudin, 2003) and to guide the evaluation of information systems (Aoyama, 2007).

Personas have been criticised as being open to being challenged and changed arbitrarily, and in response well-defined procedures have been developed for basing personas on evidence and empirical induction (Aoyama, 2005, 2007; Faily and Flechais, 2010, 2011). Our approach echoes that of Faily and Flechais (2010, 2011).

10. Purpose of the research

The purpose of this research was to test the process of creating personas in the context of city residents using city information services and to construct a preliminary set of personas for the City of Johannesburg that could be used, with some refinement, in future smart cities research. The research objectives were as follows:

1. To construct personas representing the information needs and preferences of residents of Johannesburg.
2. To compare the information needs and preferences of the constructed personas to the information services offered on the City of Johannesburg website, in order to evaluate the effectiveness of the City of Johannesburg website.
3. To reflect on the feasibility of using personas in understanding and developing city information services.

The scope of the study was limited to residents of Johannesburg, with information needs that could be met by the City of Johannesburg. The study did not include the information needs of tourists or potential investors in the city.

11. Data and analysis

The personas were constructed from data gathered through semi-structured interviews with city residents. Interview questions were based on the items in persona templates described by Aoyama (2007) and Pruitt and Grudin (2003). Questions were included about personal characteristics, interests and circumstances; skills in, attitudes towards and access to information technologies; engagement and attitudes towards government services; past and present information needs and the sources of information used. Interviews were conducted at Thuso House Customer Service Centre as well as the Johannesburg City Library. These two sites were selected because they attract large numbers of residents from a range of suburbs, including different income groups and demographics, hence providing access to a variety of residents.

Respondents were purposely selected in order to obtain appropriate variety, as well as commonality that would form patterns and ground the findings reliably. Potential respondents were invited to participate based on perceived gender, ethnicity and age, as well as who they were with (for example parents, children or other partners) from which we inferred family circumstances or social circles. Although the library did attract large numbers of residents, few library patrons were over the age of eighteen and this limited the number of respondents interviewed at the library. Respondents were interviewed in English, in the public spaces, and interviews were recorded with their permission.




Sixteen interviews were conducted with people between 18 and 70 years of age; four were unemployed, five were employed, six were self-employed and one was employed part-time. Eight of the respondents were African, four Caucasian, one coloured and three of Indian descent; nine were men and seven were women. Although the sample is not representative of the city's residents, it did give a sufficiently rich mix of residents for our purposes.

Personas are documented using persona templates (Aoyama, 2007), foundation documents (Pruitt and Grudin, 2003) and narrative descriptions (Faily and Fléchais, 2010). We made use of a persona template with attributes selected as discussed below. Using a grounded theory approach (Corbin and Strauss, 2008; Faily and Fléchais, 2010, 2011) and Atlas.ti software, the interview data was analysed using closed and open coding. Closed codes were used to identify some of the template attributes (for example the personal characteristics and circumstances) while open coding was used to understand others (like attitudes and information needs). As patterns in the template attributes emerged, personas were identified with specific themes and named.

In constructing the personas, information gathered from individuals is combined and decomposed so that a persona may combine attributes from several individuals and the attributes of one individual may inform more than one persona (Aoyama, 2005). The attributes selected are often demographic, but must relate to the scenarios of interest. In our case, we are interested in residents' information needs and the ways in which they satisfy these needs. So we included in the template personal characteristics (age, gender and marital status), life circumstances (employment and economic situation), attitudes (towards the city, information and technology) and hobbies. These characteristics were inferred from the collected data which typified each persona. A name and an image were added to personalise each persona and aid in envisaging an actual resident.

12. Five personas and their information needs

Five distinct personas emerged from the data: the techno-stressed old lady, the unemployed homeowner, the self-sufficient business woman, the community hero and the young and connected hustler. The characteristics of these personas are summarised in Table 1. This set of personas is not comprehensive because it is based on a limited set of data. However, the personas are well grounded in the data (Faily and Flechais, 2010) and serve to illustrate and reflect on the processes of creating and using personas.

Name and description	Personal characteristics	Personal circumstances	Attitudes	Hobbies	Profile picture
Elisabeth van de Baker, the techno-stressed old lady	Caucasian woman of 65, married	Retired former bookkeeper, owns a car, doesn't need "all the things that young people need"	Values neatness and order; using technology is stressful; you can't trust the internet	Reading and visiting friends	
Chennons Williams, the unemployed home owner	Coloured man of 33, with a wife and 2-year-old son	Unemployed; worked at a printing store; owns a house; uses public transport	Patriotic and optimistic; positive about interactions with the city	Watching and playing soccer, socialising	
Kuyelwa Mbonani, the self-sufficient business woman	African woman of 47, married	self-employed financial consultant; owns a car	Wants simplicity and minimal services that are efficient and effective	Reading, playing tennis, walking and running	



Name and description	Personal characteristics	Personal circumstances	Attitudes	Hobbies	Profile picture
Poupa Chandrapal, the community hero	Man of Indian descent, 39, with a wife and two children	Police officer, owns a car and uses public transport	Loves his city and people; community-minded; enthusiastic about the city's plans	Watches soccer, active in his religious community, and loves reading	
Perseverance Mtimora, the young and connected hustler	African bachelor of 24	Self-employed business owner and student; driven, with many interests	Young, ambitious and tech-savvy; connected and well-informed	Plays piano and drums, socialises with family and friends, runs to stay fit	

Table 1: Characteristics of the five personas

The information needs identified by the respondents are shown in Table 2 in descending order of frequency. It is not surprising that information about service tariffs was frequently sought because people come to the customer service centre to resolve queries with their services accounts. Community-specific information included planned power and water outages, the identity of meter readers and safety. Respondents showed interest in the city's plans and initiatives for development, and were seeking information about jobs, public transport, leisure and cultural pursuits, as well as housing.

Information about	# of references	% of references
Service tariffs	17	31
Community-specific information	7	13
Jobs and job opportunities	6	11
Public transport information	6	11
City development plans	5	9
Leisure and cultural pursuits	5	9
Housing information	4	7
Other	5	10
TOTAL:	55	100

Table 2: Information needs identified by the respondents

The sources that residents rely on for information include general internet searches (26% of references in the interviews), or the online information provided by the city (19%). But many also rely on the physical service centres (23%), as well as family and friends (16%). Several respondents reported that they first tried the City's web site but did not find the information they needed and so had to go into the service

centre. Other information sources mentioned were traditional media (newspapers, magazines, radio and television) as well as observing others.

Table 3 below reports the information needs of each persona and how they meet those needs. In order to understand how each persona engages with online information, the table also lists technology devices that each persona is able to use when seeking information, the activities that they use the internet for, and the number of hours they spend online each day.

Name and description	Information needs	Information sources	Devices	Online activities	Hours per day
Elisabeth van de Baker, the technostressed old lady	To log an account query. To check the status of a query. Information that is neat and indexed.	Customer service centre, friends and family, media outlets, general internet	Personal computer (phone is hard for her to see)	Online banking and general searching	0 – 1 hours
Chennons Williams, the unemployed home owner	Utility account query. Proof of unemployment for debtors. Government job vacancy information. Service outages in his suburb	Media outlets, general internet	Mobile phone (used to use a computer at work)	Job hunting and general searching	0 – 1.5 hours
Kuyelwa Mbonani, the self-sufficient business woman	Feedback on her services account. Information related to her community and neighbourhood. Queries over Skype.	Customer service centre, general internet	Personal computer at home and mobile phone	Online banking, email, research for her business	0 – 4 hours
Poupa Chandrapal, the community hero	Services account queries. Community information. City success stories, like park renovations. City development plans.	Media outlets, general internet, city website, customer service centre	Mainly his phone, also his laptop	Reading, research and general searching	3 – 6 hours
Perseverance Mtimora, the young and connected hustler	Identity of meter readers in his suburb. Crime stats and housing options. Wants to upload own meter readings and make online payments. Community notices and updates. City development plans.	General internet, City of Johannesburg website, customer service centre	Personal laptop and smart-phone	Online banking, email, research for study/business, general searching, entertainment	6-10 hours

Table 3: Persona information needs and behaviours

The information needs of the personas were compared with the information provided on the City of Johannesburg's web site by completing a walk-through of selected information-seeking scenarios associated with specific personas. The scenarios examined were: to query a water and electricity account, to look for job opportunities, to identify planned service outages, to learn about city development plans, and to identify the meter readers for an area. The walk-throughs were performed using the devices available to the personas and took account of the experiences and outcomes that respondents reported in the interviews. The results are summarised in Table 4.

Scenario	Personas	Experience	Outcome
Billing query on a personal computer	Aged technostressed lady; Self-sufficient business woman	Tries following menu options, but gets "page not found" errors. Tries the quick help and gets a list of FAQs, but can't find the question she wants to ask. Finally uses the search option. The search term "query" returns 682 results. One says Accounts and following this link gives information about logging a query by phone and in person, but not online.	Information need not met
Billing query on mobile phone	Unemployed homeowner; Community hero	Navigates to the site's home page. Tries a number of tabs and links that appear to relate to billing information, but cannot find the information he needs.	Information need not met
Look for job opportunities on mobile phone	Unemployed homeowner	Navigates to the site's home page. Cannot find any links that relate to employment information.	Information need not met
Find service outage times on a personal computer	Self-sufficient business woman	Navigates to the site's home page. Identified "service alerts" link which gives details of planned outages. Her suburb is listed and the information is available.	Information need met
Find service outage times on mobile phone	Unemployed homeowner; Community hero	Navigates to the site's home page. Identified "service alerts" link which gives details of planned outages. Suburb is not listed. It is not clear if this is an omission or whether there are no planned outages for his area.	Information need partially met
Identify the meter readers for an area on a personal computer	The young, connected hustler	Navigates to the site's home page. Types "meter reading" in the search field. The system returns 511 results. The first result is a link to the Electricity page which lists the meter readers for each area.	Information need met

Table 4: Scenarios evaluated and outcomes

From this analysis it is clear that many information needs of residents are not being met by the City's web site and consequently, residents are turning to other information sources. Respondents reported that coming into the service centre was inconvenient, but that it had the capacity to address their information needs because

the service centre is interactive; they get direct feedback from an individual. By contrast, the web site was not interactive.

13. Reflecting on the use of personas

The personas revealed new ways of thinking about city residents. For example, while the needs of homeowners are clearly present in the smart city, as are the needs of the unemployed, the intersection of these two groups, the unemployed homeowner, was unexpected and presents a new set of information needs. So it appears that the use of personas will give a more inclusive view of the city's residents and a more comprehensive understanding of their information needs.

The process of constructing personas using interviews created well-grounded archetypes of the city's residents. The interviews allowed the respondents to express themselves and resulted in a more in-depth understanding of the interviewed residents. However, to create a comprehensive cast of personas, representing all the residents of the city, using this method would be time consuming. Some authors have used surveys to collect data for constructing personas (for example Ayoma, 2005), but this approach lacks the richness of interviews. Some combination of data based on surveys and interviews will probably yield the best results.

Aoyama (2005) cautions that the practice of naming the personas may make the personification too "strong" and this has been reflected in practice (Faily and Flechais, 2010). We opted to use a name (e.g. Kuyelwa Mbonani) and a descriptive title (e.g. "the self-sufficient business woman") for each persona. In working with the personas, the descriptive title seems to encapsulate the persona without the strong personification and we recommend this practice.

The personas assist in understanding the ways in which different people interact with information services. For example, it helped in doing the web site evaluations to think of the approaches that each persona might use. This would be even more effective if the city set up resident panels, like the persona user panels of Pruitt and Grudin (2003), of representative people who could assist in such evaluations.

One of the challenges in Johannesburg is ensuring that the information needs of residents are addressed equitably. Often the information needs of wealthier, more powerful residents are better provided for because private companies and individuals see business opportunities in doing so. Such residents are also more vocal and better able to lobby for their needs to be met. In South Africa, where there are deep inequalities and the need to provide redress for past inequities, equity of information provision is important. A comprehensive cast of city resident personas would bring the needs of a wider range of residents to the attention of those designing information services, highlight those who have pressing needs that are not being met.

This study was limited in the data collection with data being collected from only two locations in the city and only 16 interviews being conducted, and so the personas

reflect the types of people who make use of those locations. Future research might expand the cast of personas for the City of Johannesburg; construct personas for other information services; critique other information services used by city residents, and examine the use of these personas in the design of information services.

14. Conclusion

The construction of a comprehensive cast of city resident personas is feasible, although the process of arriving at such personas may need to be refined. Having a set of resident personas would facilitate user centred design and make it more likely that the information services provided in the city match the information needs of the residents. In addition, the personas could give a “voice to the voiceless”, raising awareness of the information needs of residents who lack the capacity and influence to demand that their needs are met.

15. Acknowledgement

This research was supported by the South African National Research Foundation (NRF) through the Information Systems for Smart Cities in Africa research grant.

16. References

- Aoyama, M. (2005), “Persona-and-Scenario Based Requirements Engineering for Software Embedded in Digital Consumer Products”, in *Proceedings of the Requirements Engineering Conference, 2005 (RE '05)*, Aug-Sep 2005, Paris, pp85-94.
- Aoyama, M. (2007), “Persona-scenario-goal methodology for user-centered requirements engineering”, in *Proceedings of the Requirements Engineering Conference, 2007, (RE'07)*, Oct 2007, Delhi, pp185-194.
- Cheng, B.H.C. and Atlee, J.M. (2007), “Research directions in requirements engineering”, in *Proceedings of the Future of Software Engineering Conference (FOSE'07)*, May 2007, Minneapolis, MN, pp285 – 303.
- Cole, C. (2011), “A theory of information need for information retrieval that connects information to knowledge”, *Journal of the American Society for Information Science and Technology*, 62(7), pp1216-1231.
- Cooper, A. (1999), *The inmates are running the asylum*, 1st edition, Sams, ISBN 978-0672326141.
- Corbin, J.M. and Strauss, A.L. (2014), *Basics of qualitative research: techniques and procedures for developing grounded theory*, 4th edition, Sage Publications, ISBN 978-1412997461.
- Faily, S. and Fléchain, I. (2010), “Barry is not the weakest link: Eliciting Secure System Requirements with Personas”, in *Proceedings of the 24th British HCI Group Annual*

Conference on People and Computers: Play is a Serious Business (BCS-HCI '10), British Computer Society, pp113–120.

Faily, S. and Flechais, I. (2011), “Persona cases: a technique for grounding personas”, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp2267-2270.

Hollands, R.G. (2008), “Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?” *City*, Vol.12, No.3, pp303-320.

Komninos, N. (2002), *Intelligent Cities: Innovation, Knowledge Systems and Digital Spaces*, Routledge, ISBN 978-0415277174.

Lee, J., & Lee, H., (2014), “Developing and validating a citizen-centric typology for smart city services”, *Government Information Quarterly*, Vol.31, Suppl.1, ppS93-S105.

Pruitt, J. and Grudin, J. (2003), “Personas: practice and theory”, in *Proceedings of the 2003 conference on Designing for user experiences*, ACM, pp1-15.